DIGITAL NATIONS

A Comprehensive Guide to Web3

Tory Green

About This Book

Web3 is the biggest opportunity of our generation. Investments in the space have the potential to yield **100x to 1,000x returns** and, *if you know where to look,* you can make tens to hundreds of millions (or more).

Unfortunately, **most people don't understand the full potential of Web3**. They think it's simply the next version of the internet, when the truth is that it's so much more than that…

Web3 is combining seemingly unrelated technologies such as cryptocurrencies, NFTs, smart contracts, DAOs and DeFi to create truly autonomous online economies and – by extension – **the world's first digital nations**. Those who help build and invest in these new nations will be the Rockefellers and Carnegies of the 21st century.

This book intends to **help you understand Web3 better than 99.9% of the population**. It provides a holistic overview of every major aspect of the space and – more importantly – will show you how all the pieces tie together to create an entirely new paradigm that can overthrow centuries of economic oppression.

In particular, you'll learn:

- How Web3 is combining cryptocurrencies, DeFi, NFTs, DAOs and smart contract platforms to create the first digital nations
- Why our current economic system is flawed and how Web3 will fix it
- Easy to understand descriptions of how decentralized economic systems work – in particular, how technologies such as blockchains, digital key cryptography, consensus mining and smart contracts combine to form decentralized "world computers"
- A deep understanding of cryptocurrencies, DeFi, NFTs, DAOs, smart contract platforms and the metaverse, and how all of these concepts will combine to form the world's first truly autonomous digital nations
- The technical architecture of the Web3 ecosystem and the key "picks and shovels" protocols that support the network (such as wallets, decentralized ISPs, node providers, decentralized storage, oracles and virtual worlds)
- The often-overlooked challenges that plague Web3 and how we are working to fix them
- Why Web3 could easily be a $100+ trillion investment opportunity

The book **also includes a free "Web3 University" section that highlights the best resources** I've come across for learning more about the space, including books, articles, videos, podcasts, news sources, data repositories and twitter accounts.

I hope that you find this book helpful and, if you like it, please don't hesitate to share and follow me on Twitter for updates on developing trends!

- Tory Green

P.S. Please check out the book's companion website: www.digitalnations.xyz

Note: This content is for informational purposes only, you should not construe any such information or other material as legal, tax, investment, financial, or other advice.

Table of Contents

Table of Contents

Table of Contents

Part 4: Non-Fungible Tokens

Table of Contents

Table of Contents

Table of Contents

Part 8: Challenges Facing Web3

Part 9: Why Web3 Will Eat the World…

Table of Contents

Part 10: Web3 University

Part 1: Introduction to Web3

_____

Chapter 1: What is Web3?

Few people truly understand the potential of Web3.

It's not – as most people think – simply the "next version of the internet". Instead, it's creating the world's **first autonomous digital nations**.

Seemingly disparate verticals such as cryptocurrencies, DeFi, NFTs, smart contract platforms and DAOs will combine to form the building blocks of "borderless" economies that **operate outside of the purview of the existing financial, legal and political ecosystem**.   These new organizations can eliminate many of the costs, restrictions and regulations that hamper us today, and may also help overturn centuries of inequality and economic oppression.

To understand why this is so relevant now, consider the fact that we are becoming a digital species.

Over 5 billion people use the Internet and **the average American spends more than 8 hours online everyday** (over 50% of our waking hours!). The technology has revolutionized information sharing, communication and connectivity, becoming arguably the most efficient system for organizing people that has ever existed.

<u>5+ Billion People Use the Internet, Spending an Average of 8 Hours Online per Day</u>
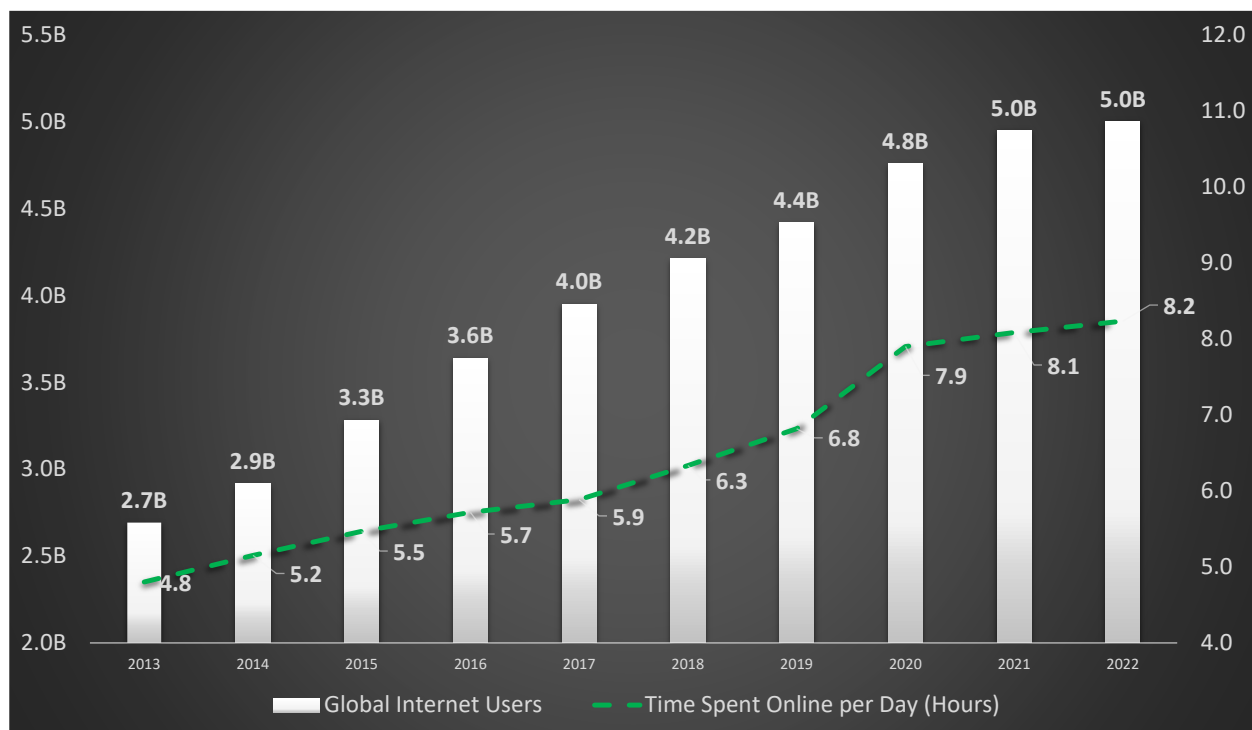
Source: Hootsuite and Statista

Despite all this, the internet is still a vassal to legacy economic systems. It is almost entirely controlled by third parties – we make transactions in national currencies such as the US Dollar, digital goods are created and controlled by companies such as Google, Amazon, Facebook and

_____

_____

Apple and the space is subject to a patchwork of local laws and regulations – such as the European Union's GDPR or China's Great Firewall.

The technology behind Web3 changes all of this, and allows us – for the first time in history – to create fully sovereign, self-sufficient online economies with their own:

- **Money**: Cryptocurrencies will replace national, fiat currencies as the new nation's money

- **Financial System**: DeFi will replace banks as the native financial system

- **Native Goods**: NFTs – assets which are entirely created, used and owned online – will become the native goods of this new economy

- **Laws**: Smart Contract Platforms will replace local administrations and legacy legal systems as the governing law

- **Corporations**: DAOs will replace corporations as the primary economic entities

This makes the opportunity in Web3 much bigger than anyone is projecting, as liberating the nearly **$100 trillion in value created by the internet** into its own sovereign entities could change the world in ways we can't even imagine.

<u>Web3 Has the Potential to Be a $100 Trillion Opportunity</u>

_____

_____
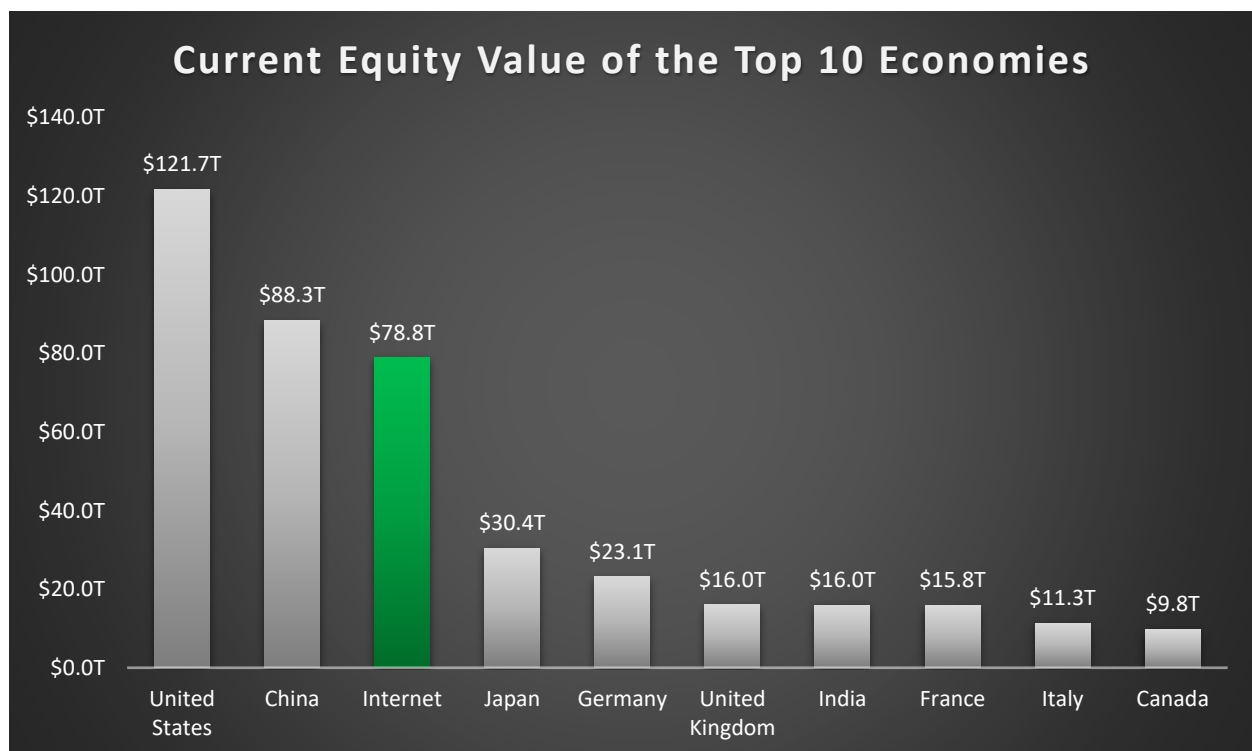
Chapter 2: The Problem with Centralized Economies

Our current political-legal-economic infrastructure is highly centralized and still relatively autocratic.

National governments are the only entity with the power to create laws and issue currencies, banks control the money supply and flow of capital and large corporations have a near monopoly on the production and sale of most goods and services.

Governments, Banks and Corporations Have a Monopoly on the Economy
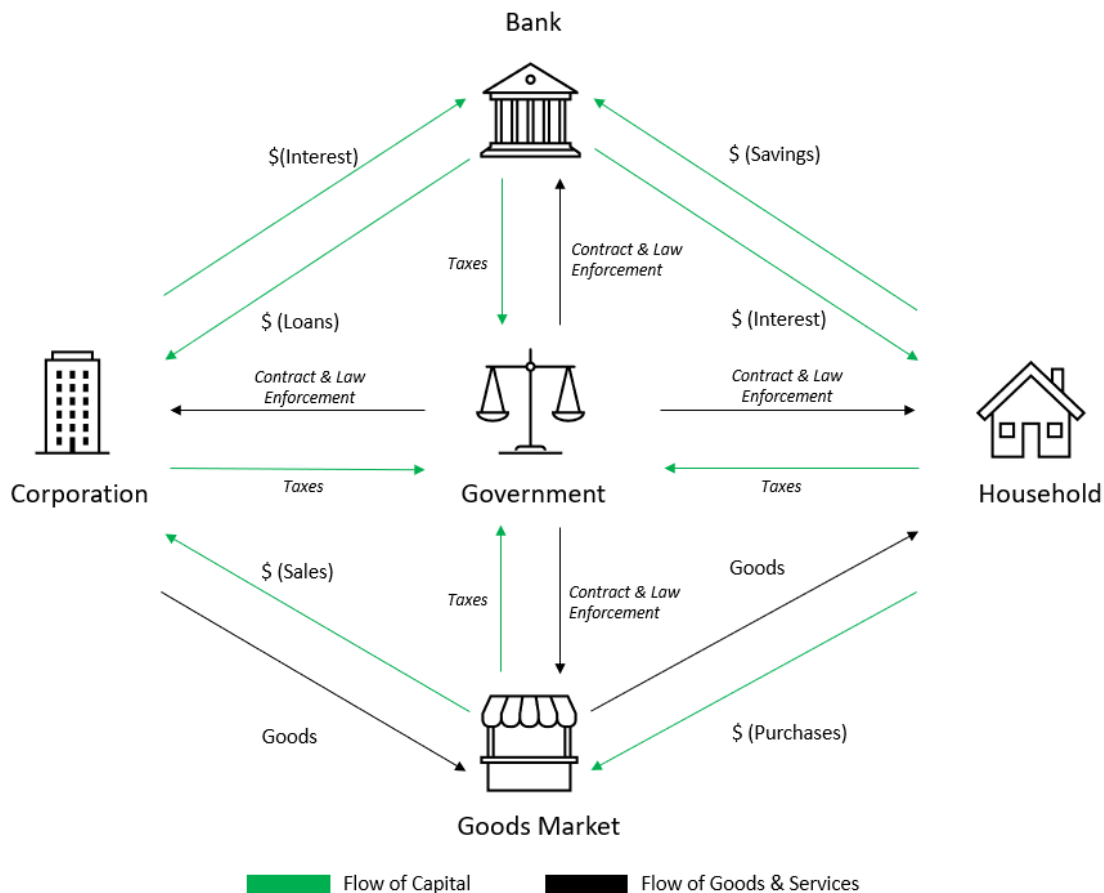
Unlike many in the crypto space, I don't hate this system. In fact, I think that it has served us remarkably well and has undoubtedly been a key driver of prosperity over the few centuries. Governments provide security and help establish trust through laws and regulation, the international financial sector facilitates growth via trade and the international flow of investment capital and corporations help coordinate the production and distribution of goods and services.

But, like any centralized system, our current infrastructure has its issues. It's bloated, byzantine and draconian and – worst of all – it consolidates power in the hands of the few. This leads to numerous problems including:

_____

_____

- **Expensive and Inefficient:** Governments, banks and large corporations are highly inefficient. Hierarchical layers slow communication and new ideas must often pass-through multiple rounds of approval before being implemented. To make matters worse, armies of bankers, lawyers, accountants, executives and bureaucrats are required to maintain the system, costing an estimated $7 trillion a year in the US ([or 35% of GDP](#))

- **Potential for Corruption:** Even the best centralized economies are notoriously opaque. We aren't privy to many of the internal decisions of our government, corporations are only required to share certain types of information on an intermittent basis and – as the financial crisis of 2008 proved – even the banks and regulators had little idea what was sitting on the balance sheets of our largest financial institutions. At best, this opacity is a recipe for negligence, at worst, it is a breeding ground for corruption

- **Seizure:** In our current system, it's debatable whether you really own your assets. Many governments can arbitrarily revoke citizenship, corporations can take your digital goods and banks can freeze and even seize your assets at will. While this may seem far-fetched, consider that in 2013, the Government of Cyprus seized 47.5% of all bank accounts over €100,000 to bail-out its failing banking system

- **Limited Access:** The economic agents of nation-states are the ultimate gatekeepers. Gaining citizenship to many countries is often impossible and banks can decide whether they want you as a customer. While the latter is generally not a problem in the developed world, this is a huge issue in growing economies. Today, nearly 1.7 billion people remain unbanked simply because they aren't profitable enough to be considered by global financial institutions

- **Limited Privacy:** Our current system offers citizens very little privacy. Governments require extensive documentation, banks must collect detailed personal information to adhere to KYC, AML and CFT regulations and companies such as Facebook own all the data you post. While in some cases this produces comical effects (such as a man learning from Facebook that he was going to be a father before his wife told him), it has also produced dystopian ones (such as Facebook illegally sharing user vast amounts of private user data with third parties in the Cambridge Analytica scandal)

- **Censorship:** While many modern democracies have codified freedom of speech, this unfortunately doesn't always apply to private institutions.   Companies such as Twitter have full discretion over who can access its site and whom they can ban. To date, they have banned hundreds of thousands of people, including several high-profile users. This problem also isn't limited to social media, as Apple recently banned Epic Games, the creator of the multi-billion dollar game Fortnite, from its App Store after a revenue dispute

- **Hidden Taxes:** In addition to the taxes we pay to the federal government, citizens of many developed nation states are also subject to a variety of "hidden taxes". Banks often charge enormous fees on credit card transactions and international money transfers, and "Big

_____

_____

Tech" often takes a large cut of revenues earned by artists and entrepreneurs. For example, Spotify garners 30% of the revenues from a song, and Apple often charges a 30% "tax" on every sale made through their App Store

- **Lack of Interoperability**: Many players in the economic ecosystem of modern nation-states operate as "walled gardens", limiting the interoperability between financial institutions and technology companies (i.e. an app built for Apple's App Store will rarely work on Google). This makes it difficult to even transfer assets between entities let alone share and collaborate on new technologies and products

Together, these concerns represent a major problem. Not only do they limit growth, but they also continue to drive inequality.

So why do we tolerate these inefficiencies? Well, we don't really have a choice due to what is known as the Byzantine General's Problem. While I'm oversimplifying a bit, this concept basically states that large groups of humans can't trust one another or coordinate across vast distances without using centralized third parties (such as governments, banks or corporations) to establish trust. For example, when a stranger sends you money online, you must rely on your bank to ensure that 1) they are whom they say they are and 2) they have the money they say they have and 3) they actually send it.

_____

_____

Chapter 3: The Benefits of Decentralized Economies

This all changed in 2009 when Satoshi Nakamoto invented Bitcoin, solving the Byzantine General's Problem and setting off a chain of events that made the concept of "decentralization" possible.

While the mechanics of this invention will be discussed more throughout the book, the key thing to remember is that he (or she) created a new technology known as a **decentralized ledger** (or more commonly, but somewhat erroneously, a "blockchain") that could autonomously authenticate economic actors, verify their funds and guarantee the completion of a transaction.

This made it possible, for the first time in history, to create **an economy that doesn't rely on third parties such as corporations, banks, governments or courts to function**.

<u>Digital Nations don't Require Banks, Governments, Courts or Corporations to Function</u>

	Nation States			Digital Nations		
Money						
		Fiat			Cryptocurrencies	
Financial System						
		International Banks			DeFi	
Goods						
		Digital			NFTs	
Law						
		Governments			Smart Contract Platform	
Economic Entities						
		Limited Liability Corporations			DAOs	

The effect of this cannot be overstated and requires a bit of *tabula rasa* thinking. Imagine for a bit, how you would design an economy if you no longer needed intermediaries:

- After all, what's the point of relying on central banks and treasury departments if you can issue your own money and control the supply?

_____

_____

- What's the point of banks if you can safely hold your own assets, raise your own funds and orchestrate your own lending and borrowing protocols?

- Why do we need Big Tech if we can create and own our own digital goods?

- Why do we need to rely on local governments and courts if we can enforce our own laws through smart contracts?

If you're like me, you're probably envisioning something much simpler and more elegant than what we have today…

In short, an economy without unnecessary middlemen.

This, my friends, is Web3. And it may allow us to reap all the benefits of a traditional economy – namely trust, security and growth – while removing most of the downsides. Indeed, Web3 is:

- **Fast and Efficient**: Web3 operates almost entirely via computer programs which automate the execution of all transactions. As such, there's no need for intermediaries such as bankers, regulators, lawyers, accountants, executives or government bureaucrats – making the system much faster and cheaper

- **Transparency**: Every transaction in Web3 is broadcast to the public allowing for real-time monitoring and maximum transparency. In addition, protocols are built with open-source code allowing any user to audit them, greatly reducing the threat of corruption and serving as a safeguard against negligence

- **Seizure-Proof**: In Web3, you control your assets. Instead of relying on banks, governments and corporations, you hold your funds, identity and digital goods in your own digital wallet. As such, there's no one to seize your assets, limit withdrawals or tell you where you can and can't spend your money

- **Permission-Less**: No one can stop you from accessing Web3. Anyone with an internet connection can participate in markets that are open 24 hours a day, 7 days a week and 365 days a year

- **Borderless:** Web3 has no borders. Users can store millions (or more) on a thumb drive or online wallet (not recommended) and go anywhere they please. They can send money to relatives living abroad, perform cross-border transactions and invest in foreign companies without having to pay outrageous fees or navigate a labyrinth of international laws

- **Private**: Web3 is designed so that users have complete ownership of their data – in fact, it's completely possible (and often preferred) to navigate Web3 in a completely anonymous fashion

_____

_____

- **Eliminates Censorship**: No one in Web3 can censor you. Anyone is free to upload any content, no matter how controversial, to any platform they so choose

- **Permanence**: Because a decentralized internet is hosted on thousands of devices across the world, it's very resistant to failures and almost impossible to shut down (unlike traditional nations, digital states can't be conquered with tanks, bombs or guns)

- **More Money for Artists:** Artists, musicians, game developers and entrepreneurs could increase their profits by an order of magnitude when we remove the current gatekeepers of the web. In fact, we are already seeing this take shape, as some Web3 services such as Audius (a decentralized version of Spotify) increase a musician's share from 12% to 90%!

- **More Money for Consumers**: Users will be able to choose whether they want to be paid for creating content or sharing their data and they will also have the right to sell the virtual goods that they earn online. We already saw this happen last year in the Philippines, where many citizens made more money selling the digital assets they earned playing the blockchain-based game Axie Infinity than they would have from working full-time as a teacher, construction workers or office assistant

- **Interoperability**: Web3 protocols are built to be composable, that is, they can be programmed to work with one another allowing users to build increasingly complex and novel products

I know this is a lot to take in. Crypto is so unique, so transformative, so unintuitive that I've been studying it for seven years now and sometimes I feel like I only partially get it.

But to help you understand more about how Web3 can transform the world, let's go a bit deeper down the rabbit hole and learn how it works on a technical level…

_____

_____

Chapter 4: How do Decentralized Economies Work?

As discussed, centralized systems exist because of the need to create trust. We trust banks to hold and transfer our money, governments to enforce contracts and laws and corporations to establish the legitimacy and ownership of digital goods.

Decentralized systems are so innovative because they allow us to do all of these functions without the aforementioned "middlemen".

<u>Decentralized Systems Provide the Money, Goods and Law of a Digital Nation</u>
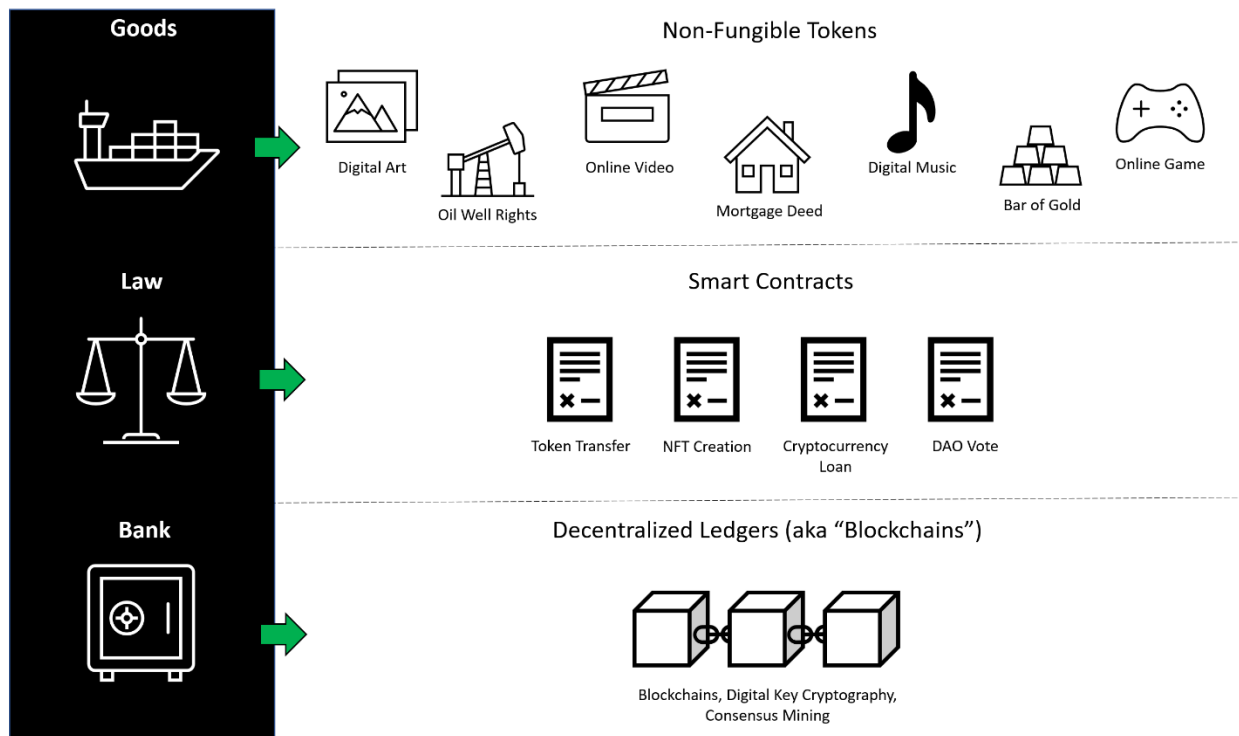
They do this by combining three separate innovations – decentralized ledgers, smart contracts and NFTs:

- **Decentralized Ledgers:** Decentralized ledgers, often referred to as "blockchains", serve as the "bank" of a digital nation. They are immutable, distributed and decentralized databases that allow users to **create, store and transfer money without using a government or traditional bank**

  The mechanics of decentralized ledgers are covered more in Chapter 10 ("How do Cryptocurrencies Work?")

- **Smart Contracts:** Smart contracts codify and enforce the "laws" of a digital nation. They are digital agreements that execute _automatically_ when pre-determined conditions are met.

_____

_____

This removes the need for lawyers and courts and allows for the creation of economies that can **operate outside of the purview of the existing financial and legal ecosystem**

The mechanics of smart contracts (and smart contract *platforms* – the decentralized computers that operate them) are covered more in Chapter 16 ("How do Smart Contract Platforms Work?")

- **NFTs:** Non-fungible tokens are the "goods" of a decentralized economy. They are digital "certificates of ownership" that are recorded on a blockchain. NFTs can represent almost anything – virtual goods such as digital art or computer-generated land, physical resources such as oil or gold or intangible assets such as voting rights or ownership stakes. Because they don't rely on "Big Tech" to verify their legitimacy, **NFTs allow consumers to truly own their digital goods**

  The mechanics of NFTs are covered more in Chapter 25 ("How do NFTs work?").

I know there's a lot to take in here – these are all very unique technologies that have the potential to radically restructure society. As such, it can take a while to get your head around them. So instead of getting too deep into the technical aspects now, we're going to build them up piece-by-piece in the coming chapters.

For now, however, the key takeaway is to remember that **a set of technologies has been invented in the last 15 years that allow us to run an entire economy without needing traditional intermediaries such as governments, banks and corporations**.

_____

_____

Chapter 5: The Web3 Ecosystem

As discussed, Web3 uses blockchain technology to create fully autonomous digital nations that can operate outside of the purview of the existing financial, legal and even political ecosystems.

Each of these nations have their own:

- **Money:** Cryptocurrencies are the native currency of a digital nation. They are a form of money that is created, distributed and owned directly by the public (as opposed to the government).

  To paraphrase Abraham Lincoln, they are the currency "of the people, by the people and for the people" as they can't be seized, restricted or regulated by the government.

- **Financial Systems:** Decentralized Finance ("DeFi") forms the financial system of a digital nation. The term refers to a global, peer-to-peer network that allows users to transact directly with other users to borrow, lend, earn interest and buy insurance without ever using traditional intermediaries such as banks, brokers, exchanges, lawyers and / or regulators.

  Decentralized banks can't appropriate your assets, restrict or regulate your transactions, block you from becoming a customer, force you to share private data or charge outrageous fees.

- **Goods:** NFTs are the native goods of a digital nation. They are digital "certificates of ownership" that are recorded on a blockchain. Almost any asset can be represented by an NFT: a piece of art, a photograph, a song, a concert ticket, a passport or the deed to your house.

  NFTs are the first and only virtual asset that can be truly owned by a consumer – Big Tech can't confiscate your NFTs, dictate how you use them or charge you exorbitant prices for selling them.

- **Laws:** Smart contract platforms coordinate the economic activity of a digital nation and enforce its laws. They are decentralized computers that can host almost any type of application or business (e.g. financial, entertainment, eCommerce, social networking).

  Unlike traditional computers, smart contract platforms i) can't be shut down, ii) aren't controlled by any one entity and iii) anyone can use them.

- **Corporations:** DAOs are the "corporations" of a digital nation. They are blockchain-based organizations that are owned and operated by members who make decisions democratically (much like a modern-day cooperative).

  Unlike a traditional corporation, no single person or group owns or controls a DAO and they largely operate outside of the purview of the existing financial and legal ecosystem.

  The next five parts of this book will explore each of these verticals in detail.

_____

Part 2: Cryptocurrencies

_____

Chapter 6: What is a Cryptocurrency?

To paraphrase Abraham Lincoln, a cryptocurrency is the money "of the people, by the people and for the people."

Contrary to popular belief, you don't really own your money. Traditional currencies – such as the U.S. Dollar, Euro or RMB – are **owned and controlled** by the government and **leased** to the public to use as payments for goods and services. While this model has its benefits, it also gives the State the power to seize your funds, restrict access to your accounts or impose limitations on usage any time they see fit.

Cryptocurrencies, on the other hand, are created, distributed and, most importantly, **owned directly by the people**. This removes the need for governments and banks and gives consumers full control over their funds – allowing them to store their own assets without fear of seizure, transact directly with other users without regulation, and freely move their funds anywhere in the world.

"Cryptocurrencies are the money of the people, by the people and for the people."

- Abraham Lincoln
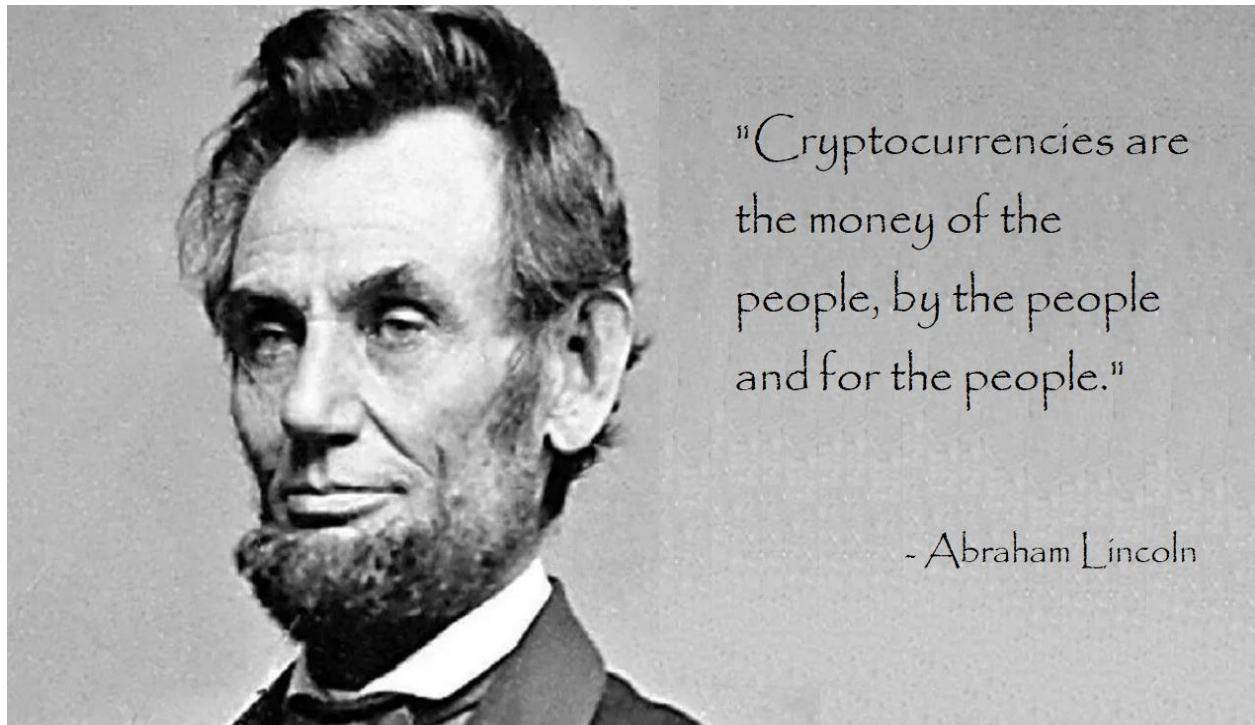
Proponents assert that cryptocurrencies are superior to traditional government-backed (or "fiat") currencies because they retain all the benefits of conventional money with the added benefits of being cheaper, faster, less restrictive, more accessible and highly transparent. Critics argue that they represent an existential threat to the global financial system, a serious danger to the community and must be regulated at all costs.

Whatever side of the argument one falls on, the popularity of cryptocurrencies is undeniable. The market has grown nearly 5x in the last three years to a total value of nearly $1 trillion (and reached a peak of almost $3 trillion in late 2021).

_____

The Total Market Cap of Cryptocurrencies is Nearly $1 Trillion

Total Market Cap of All Cryptocurrencies

$3.5T	
$3.0T	
$2.5T	
$2.0T	
$1.5T	
$1.0T	
$0.5T	
$0.0T	

2/19/2016   2/19/2017   2/19/2018   2/19/2019   2/19/2020   2/19/2021   2/19/2022
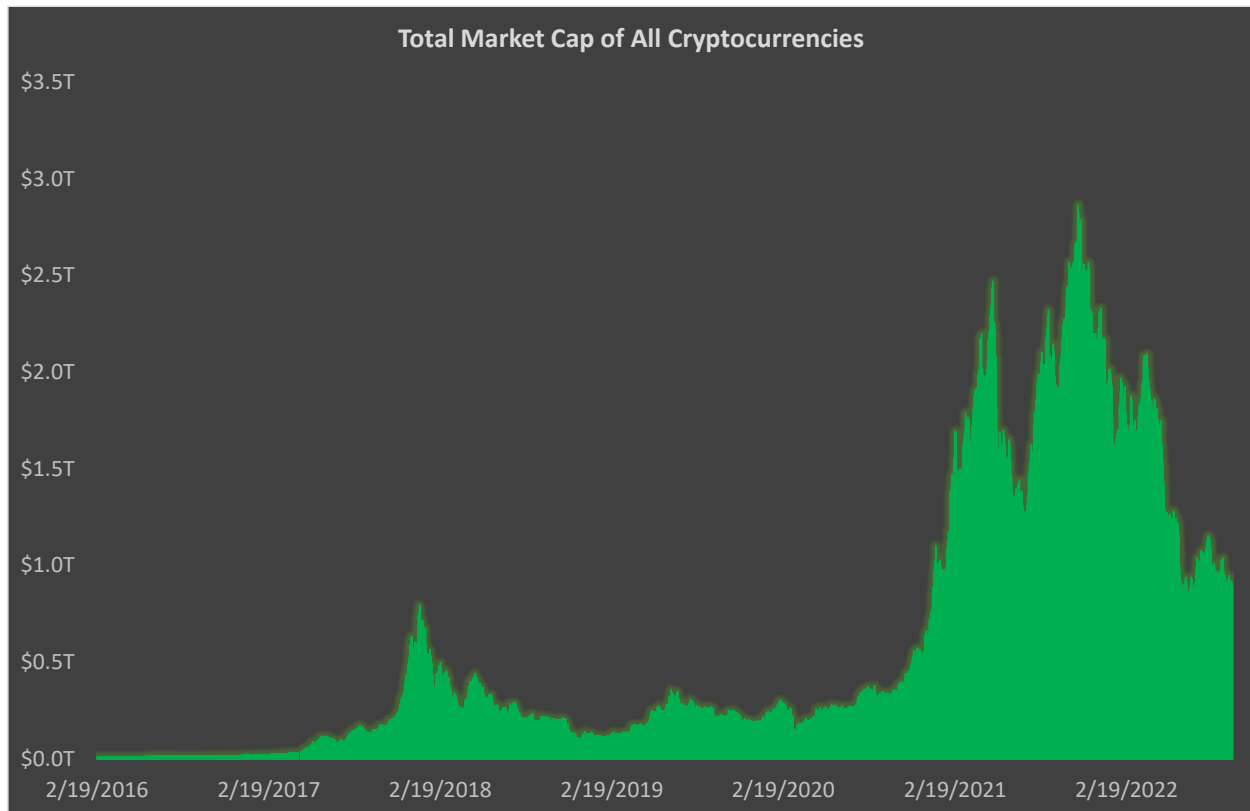
Source: Coinmarketcap.com as of 10.2.22

What is driving this popularity? Let's dig a little deeper…

Chapter 7: What is Money?

To understand the importance of cryptocurrencies, we first need to understand money.

The history of money is, in many ways, the history of civilization itself. For thousands of years, human beings have utilized various forms of currency to build economies and facilitate trade.

Indeed, money serves three important functions in our economy. It is used as a:

- **Store of value**: Money can be saved and used for later
- **Unit of account**:   It serves as a common base for prices
- **Medium of exchange**: Currency is used to buy goods and services

Ideally, money is durable, portable, divisible, uniform, accepted everywhere and has a limited supply.

<u>The Ideal Properties of Money</u>

<u>Cows vs. $20 Bills</u>

1. **Durability.** A cow is fairly durable, but a long trip to market runs the risk of sickness or death for the cow and can severely reduce its value. Twenty-dollar bills are fairly durable and can be easily replaced if they become worn.

2. **Portability.** While the cow is difficult to transport to the store, the currency can be easily put in my pocket.

3. **Divisibility.** A 20-dollar bill can be exchanged for other denominations, say a 10, a 5, four 1s, and 4 quarters. A cow, on the other hand, is not very divisible.

4. **Uniformity.** Cows come in many sizes and shapes and each has a different value; cows are not a very uniform form of money. Twenty-dollar bills are all the same size and shape and value; they are very uniform.

5. **Limited supply.** In order to maintain its value, money must have a limited supply. While the supply of cows is fairly limited, if they were used as money, you can bet ranchers would do their best to increase the supply of cows.

6. **Acceptability.** Even though cows have intrinsic value, some people may not accept cattle as money. In contrast, people are more than willing to accept 20-dollar bills.

Source: St. Louis Federal Reserve

Money has taken many forms over the years – it started with the barter of goods, progressed to trinkets such as seashells then to precious metals, and finally to paper money, plastic cards and electric money.

Today, over 90% of currency is electronic, meaning that it has no physical backing and exists only in computers owned by large banks.

_____

Chapter 8: The Problems with Centralized Money

While the earliest forms of money – such as seashells, precious metals and gold – were owned and controlled by individuals, money today is controlled almost exclusively by governments and banks.

In the United States, the system is dominated by three entities:

- **Treasury:** The Department of the Treasury is responsible for printing physical currency (i.e. notes and coins) and distributing it to Federal Reserve banks and branches

- **Federal Reserve:** The Fed is the "bank of banks" – it controls the overall money supply and distributes money to commercial banks

- **Commercial Banks:** Institutions such as Bank of America, Chase and Wells Fargo put currency into circulation by lending directly to consumers

<u>The Federal Reserve and Banking System</u>

Source: Coursehero.com

_____

_____
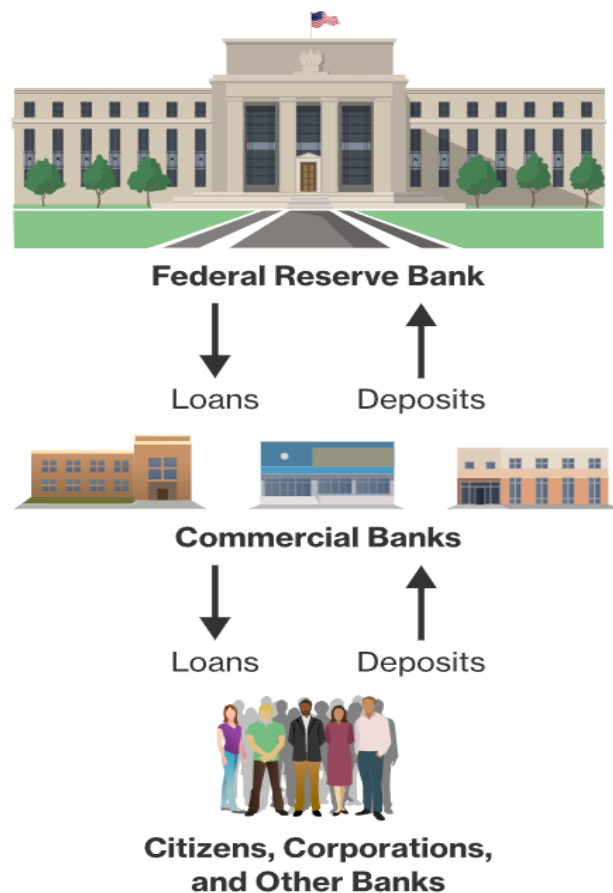
This centralized ownership presents five major problems:

- **Third-Party Custody**: In the current financial system, you don't really hold your funds – the banks do. This means that they can freeze and even seize your assets at will. While this may seem far-fetched, consider that in 2013, the Government of Cyprus seized 47.5% of all bank accounts over €100,000 to bail-out its failing banking system.

- **Limited Access:** Banks can decide whether they want you as a customer. While generally not a problem in the developed world, this is a huge issue in growing economies. Today, nearly 1.7 billion people remain unbanked simply because they aren't profitable enough to be considered by global financial institutions

- **No Privacy**: Banks must collect detailed personal information to adhere to KYC, AML and CFT regulations and transactions

- **Expensive and Inefficient:** The current financial system is rife with inefficiencies and unnecessary expenses. Payment networks charge up to 3% on credit card fees, cross-border remittance payments can take up to a week and cost 10%, and even in developed nations, users are faced with long transfer times and bloated fees

- **Restrictions of Transfer:** Several countries restrict or even ban the transfer of large amounts of cash internationally

So why do we tolerate these inefficiencies? Well, we don't really have a choice due to what is known as the Byzantine General's Problem. We discussed this earlier in Chapter 2, but as a refresher it basically states that large groups of humans can't trust one another or coordinate across vast distances without using third parties (such as banks) to establish trust. For example, when a stranger sends you money online, you must rely on your bank to ensure that 1) they are whom they say they are and 2) they have the money they say they have and 3) they actually send it.

In short, while some may call the banking system "evil", up until now it has been a "necessary evil".

_____

_____

Chapter 9: The Benefits of Decentralized Money

This all changed in 2009 when a person (or persons) using the name "Satoshi Nakamoto" invented Bitcoin – the world's first cryptocurrency – solving the Byzantine General's Problem and setting off a chain of events which made the concept of "decentralization" possible.

For the first time in history, Bitcoin made it possible to perform **direct, peer-to-peer transactions without relying on third parties to establish trust**.

The effect of this cannot be overstated and requires a bit of "tabula rasa" thinking. Imagine for a bit how you would design a financial system if you no longer needed intermediaries. After all, what's the point of banks if you can safely hold your own assets? What's the point of a federal reserve if you control the money supply? What's the point of a Treasury Department if you can issue your own money?

If you're like me, you're probably envisioning a form of money that is much simpler and more elegant than what we have today…

<u>Evolution of Money: From Cows to Crypto</u>
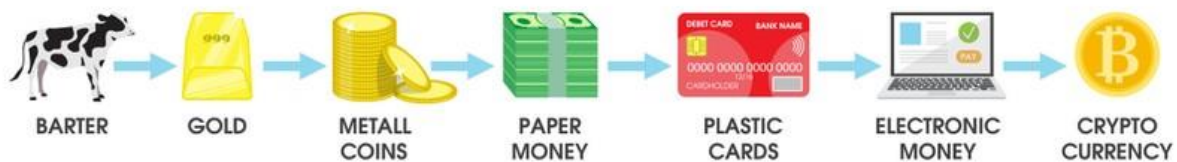
Source: Shutterstock

That's the promise of cryptocurrencies, and they may allow us to reap all the benefits of traditional money – namely trust, security and growth – while removing most of the downsides. Indeed, cryptocurrencies are:

- **Seizure-Proof:** Instead of relying on a bank to hold your assets, you control all of your funds with your own wallet. As such, there's no one to seize your assets, limit withdrawals or tell you where you can and can't spend your money

- **Permission-Less:**   Users don't need permission from a bank to access their funds. Anyone with money and an internet connection can buy any cryptocurrency in markets that are open 24 hours a day, 7 days a week and 365 days a year

- **Private:** Users can choose to (and often do) remain anonymous

_____

_____

- **Borderless:** Cryptocurrencies have no borders. Users can store millions (or more) on a thumbdrive or online wallet (not recommended) and go anywhere they please. They can send money home to relatives without anyone ever knowing

- **Cheap:** Although fees for many cryptocurrencies are high now, they're "fixed" (vs. variable) which makes them ideal for sending larger amounts of cash. In addition, as fees continue to decline, it's likely that transactions will be cheaper than traditional credit cards or wire transfers

- **Transparency:** While many claim cryptocurrencies will be a haven for criminals and tax cheats, they're actually much more transparent than traditional currencies as every transaction is permanently recorded on a blockchain

At this point you may be asking "how the heck do we create money that doesn't need a government or banks?" Great question, let's dive into that now…

_____

Chapter 10: How do Cryptocurrencies Work?

Cryptocurrencies like Bitcoin are created by and operate on a decentralized ledger, which serves as the "bank" of a digital nation.

Using a ledger, a book of financial accounts, to run an economy is not a new idea. Accountants have been keeping logs of economic activity for at least 5,000 years – using clay tablets, paper or computers to record who owns what, what trades were made and who is indebted to whom.

Even today, the vast majority of our money isn't "real", as over 90% only exists online as a record in some bank's computer system.

<u>Blockchains are the Latest Evolution in Accounting</u>

| Clay Tablets | Paper Logbooks | Computers | Decentralized Ledgers |
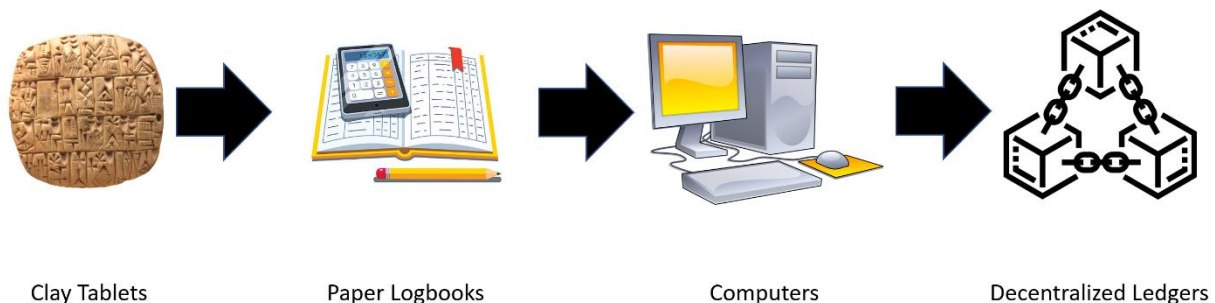
What makes decentralized ledgers so unique is that they are the first iteration of this technology that doesn't require a centralized third-party to oversee transactions and audit the books.

While often colloquially referred to as "blockchains", these structures actually combine three different innovations – blockchains, digital key cryptography and consensus mining – to allow users to create, store and transfer assets without relying on a government or bank.

To understand how this works in practice, imagine that Alice wants to buy a few bananas from Bob's grocery store. She would historically rely on a financial institution to: 1) store her funds in a secure bank account, 2) provide her with a debit card to access these funds and 3) use auditors and accountants to ensure the transaction is legitimate and transfer the funds to Bob's account.

Using decentralized ledger technology, she can perform all of these actions without relying on a bank:

- **Blockchains:** Blockchains serve as the "bank account". They are the distributed, immutable databases that store Alice's assets

- **Digital Key Cryptography:** Digital keys are the "debit cards". They are cryptographic instruments that allow Alice to access her assets and send them to Bob

_____

- **Consensus Mining:** Miners are the "auditors" and "accountants". They are random individuals that are chosen to ensure that the transaction is legitimate and update Alice and Bob's accounts with the new balances

While often described as "trustless", decentralized ledgers don't eliminate the need for trust. Instead, they simply transfer that responsibility from one, "centralized" party to hundreds or thousands of "decentralized" parties. This democratizes power – shifting it from the hands of the few to hands of the many.

<u>An Oversimplified View of a Blockchain Transaction</u>
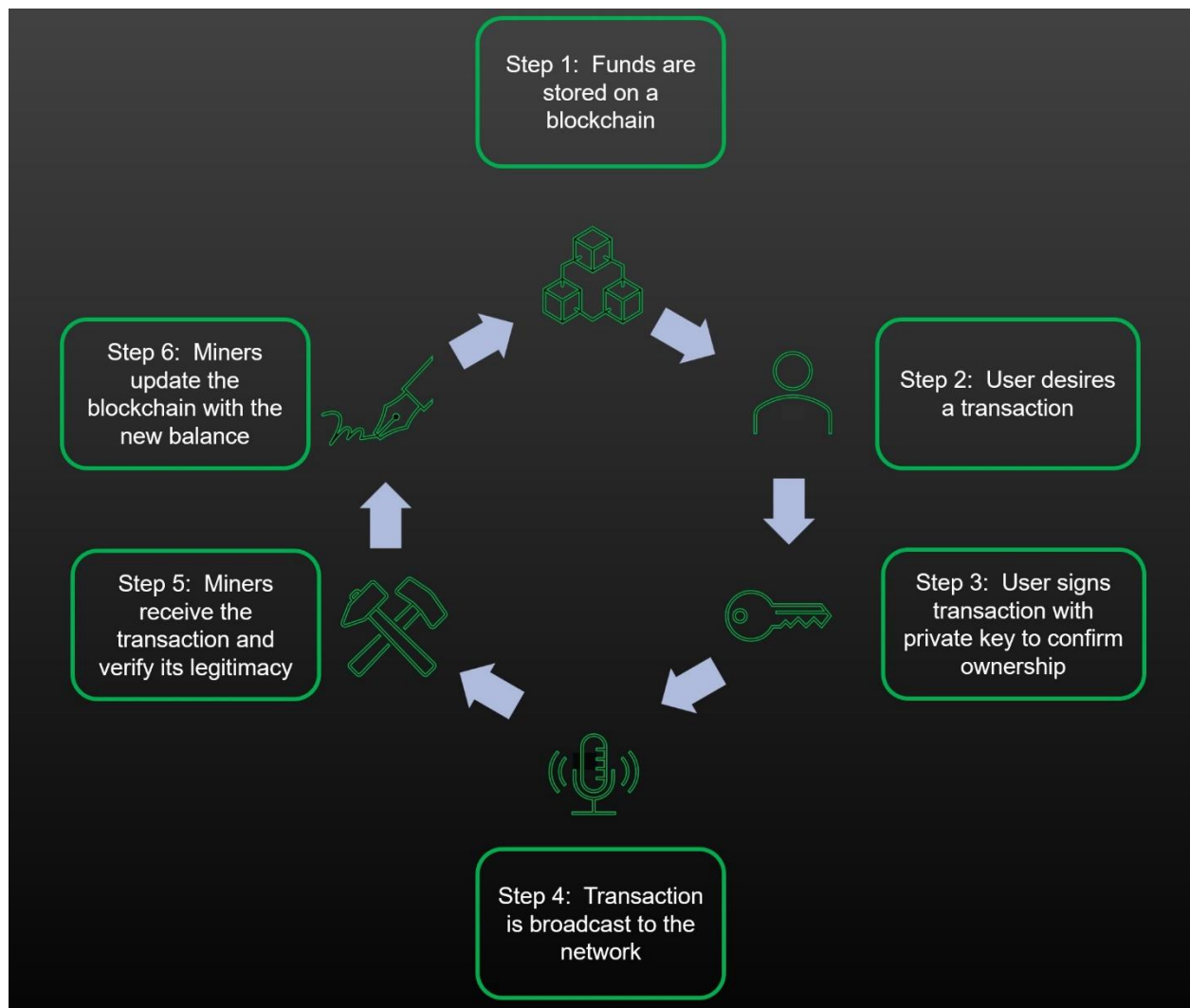
Let's take a deeper look into how blockchains, digital key cryptography and consensus mining work…

_____

What is a Blockchain?

In many ways, a blockchain is similar to an online bank account. It is an electronic database that stores digital assets (such as cryptocurrencies or NFTs) along with a record of who owns them. For example, the Ethereum blockchain may have a record that says that account "0xb794f5ea0ba39494ce839613fffba74279579268" owns 10 Ethereum tokens and one Mutant Ape NFT.

Database of Actual Balances on the Bitcoin Blockchain

Address	Total Transactions	Current Balance (BTC)	Current Balance (USD)
bc1q8q7uce7kqz0jwav2j3axnye7ndsmepe2xgaph8	118	0.0	$0.00
1EPetwSohr5sk4nmyY8gEPSsuPofaSfKF9	105	2.9	$57,166.88
37jAAWEdJ9D9mXybRobcveioxSkt7Lkwog	31,788	13.6	$267,407.87
bc1qmak6ejwefzj28jwej7kru88nzw6czk9geyalwy	67,326	9.7	$191,649.24
bc1qlkdlchlylfdkspvevnlqqlmt4l222hwva2z3n7	2	9,905.9	$195,314,630.30
bc1qnsupj8eqya02nm8v6tmk93zslu2e2z8chlmcej	619,235	379.8	$7,488,516.60
bc1qnhstjh53usshrhmmc295d3jqkz0meg98gvkhe7	1	0.0	$197.17
bc1q32sxnq5hecdurfzgzp5x0zh8du86v9x84wdqdx	13,075	37.8	$746,091.28

Source: Bitcoin Block Explorer. Addresses were selected at random. Data as of 9.7.22.

Unlike a traditional bank account, however, blockchains are distributed and decentralized:

1. **Distributed:** Instead of being hosted in a single location, they are hosted across thousands of individual computers located all over the globe
2. **Decentralized:** Blockchains are not controlled by any one party

Let's take a look at each of these concepts...

How is a Blockchain Distributed?

Unlike traditional databases that live in a geographically centralized "server farms" (such as the ones owned by Amazon or Google), decentralized ledgers are hosted across thousands of individual computers located all over the globe.

_____

_____

These computers are called "nodes", and they each contain an identical copy of the account balances and transaction history of a blockchain's database.

Decentralized Ledgers are Distributed Across Thousands of Individual Computers

Centralized Database   Decentralized Database
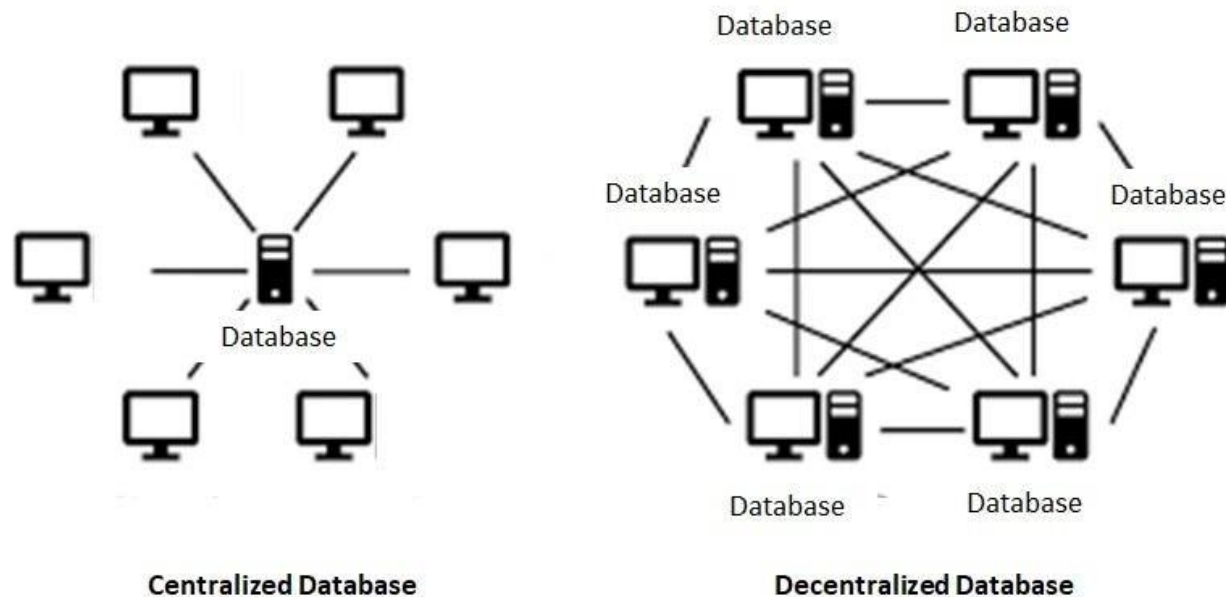
This distribution is very important because it means that: 1) it's almost impossible for a third party to turn them off, 2) they are extremely resilient to hardware failures and 3) practically speaking, a distributed architecture is needed to design a decentralized system.

How is a Blockchain Decentralized?

Traditional banks have always been trusted to protect consumer's assets.

In the old world they did this by storing money in secure vaults and defending it with armed guards. In the information age – where over 92% of money exists only in digital form – they do this with an army of accountants, auditors and cybersecurity experts. These professionals monitor accounts, check for fraud and assure that no one hacks the system and manipulates account balances.

Unlike traditional bank accounts, blockchains can't rely on an in-house staff to safeguard a user's assets and assure that no one tampers with the balances. Instead, they rely on a process known as "hashing" to protect the books.

To initiate the hashing process, blockchains organize all incoming transactions into groups known as "blocks". These blocks have a limited storage capacity, so when they become full, they are locked and linked to the previous block with a "hash". This forms a chain – hence the name, blockchain.

_____

_____

BLOCK 1

Hash: **6U9P2**

Previous hash:

00000

BLOCK 2

Hash: **8Y5C9**

Previous hash:

6U9P2

BLOCK 3

Hash: **9L4Z1**

Previous hash:

8Y5C9
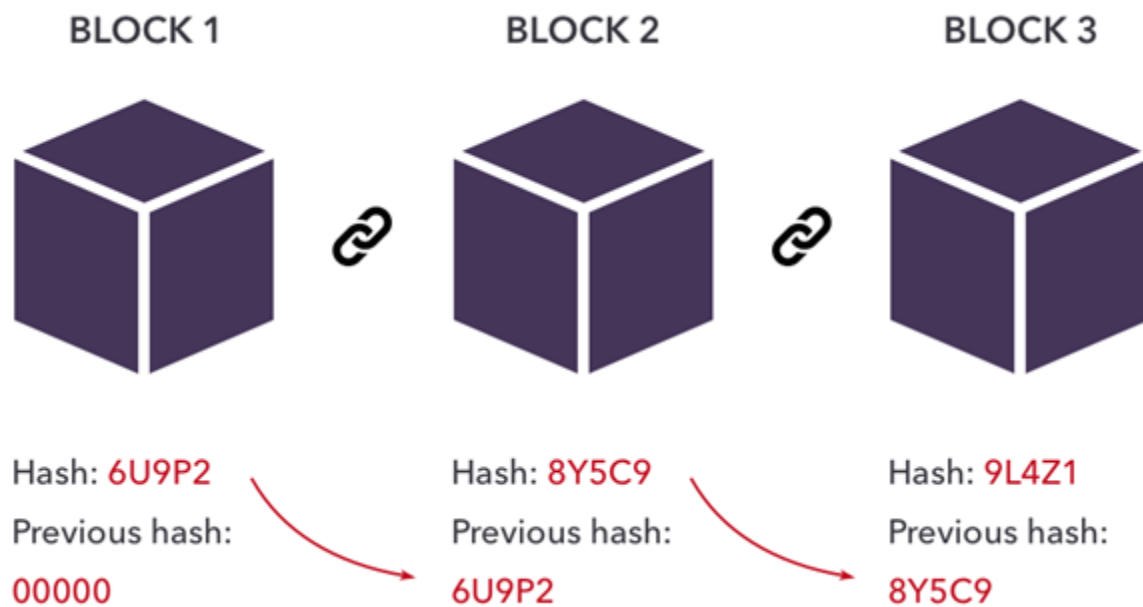
Source: ig.com

These hashes are extremely important because they make blockchains immutable – that is, data (such as your Bitcoin or Ethereum balance) can't be deleted, tampered with or changed once it is locked into the chain.

This is due to the unique properties of hashing, a cryptographic process that takes a given set of information and converts it into a unique code. For example, the word "fox" could be hashed as DFTY786DCFJ894SUSH865AAHJAI978 and the sentence "the quick brown fox jumps over the lazy dog" could be hashed as SOIAUYA7865ASLUAN098A5489USYAN.

There are three important things to note about hashes:

- Virtually anything can be hashed (i.e. you can hash a word, a sentence or the entirety of War and Peace)
- Hashes are always unique (i.e. if you changed a single letter in War and Peace you would get a completely different hash)
- It's impossible to guess the original data from looking at the hash (i.e. you wouldn't know that DFTY786DCFJ894SUSH865AAHJAI9785 was "fox")

Because all new blocks are required to store the hash of the previous block, it's easy to see if the blockchain has been tampered with. If the hash contained in the new block matches the old, you know that the data is secure. If they are different, everyone will know that the block has been manipulated.

What is Digital Key Cryptography?

Digital keys are the "debit cards" of the blockchain ecosystem in that they allow a user to prove ownership, access their account and control their assets.

_____

_____

In reality, digital keys are nothing more than long strings of numbers (256 bits long for Bitcoin) that always come in pairs – a public key and a private key:

- **Public Key**: A public key is similar to a bank account number as it serves as your address on a cryptocurrency network. For example, instead of recording that "Alice owns 2 BTCs", the Bitcoin blockchain would record that "1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2 owns 2 BTCs"

- **Private Key**: A private key is similar to a secret PIN code that allows users to access and control this account

Every public key has only one private key, and – like a key and a lock – they are linked through cryptography. The important thing to note about this link is that it only flows one way. Although one can always access a public key with a private key, it's mathematically impossible to do the reverse.

It's Impossible to Decipher a Private Key from a Public Key

Source: Ledger

This one-way logic forms the basis of cryptocurrency transactions. For example:

- **To Receive Funds**: In order to receive funds, a user would share his public key with the sender, who would deposit the money in that address. Because it's impossible to decrypt a private key from the public key, this is completely safe (and necessary)

- **To Send Funds**: In order to send funds, a user would use her private key to "unlock" her public key on the blockchain to authorize the transfer of the money. Again, because it's mathematically impossible for anyone but the holder of the private key to do this, the blockchain can be sure that this person owns the funds

In practice, users rarely see their keys, as they are often stored inside digital wallets and managed by software (i.e. you just click buttons that say "send" and "sign" on a wallet such as Metamask and the application does the rest for you).

_____

What is Consensus Mining?

Centralized networks, such as banks, have a small army of bookkeepers, accountants and auditors to process transactions.

While decentralized networks can't rely on an in-house staff, they can leverage a distributed group of users known as "miners" for a similar purpose.

Miners are the de facto auditors of decentralized platforms. They are responsible for processing the output of transactions, confirming asset ownership, ensuring there is no fraud and updating the blockchain with the new results. Unlike auditors at a traditional bank, almost anyone can be a miner – there's no hiring process, no location requirements and miners don't even have to disclose their identity (in fact, most miners are completely anonymous).

As such, most decentralized platforms have thousands of miners located all over the world that can validate transactions.

While this seems like an elegant solution to the problem of centralization, it raises a few concerns. In particular: how can we trust the miners? How do we know that they won't abuse their power and send a bunch of money to themselves or their friends?

The answer is surprisingly simple – we use economic incentives to reward good behavior and punish bad behavior.

While there are several incentive schemes, the most popular– used by both Bitcoin and the first iteration of Ethereum – is known as "Proof of Work".

_____

Overview of Proof of Work Mining

Proof of Work

Proof of Work is a consensus algorithm that requires a process called mining
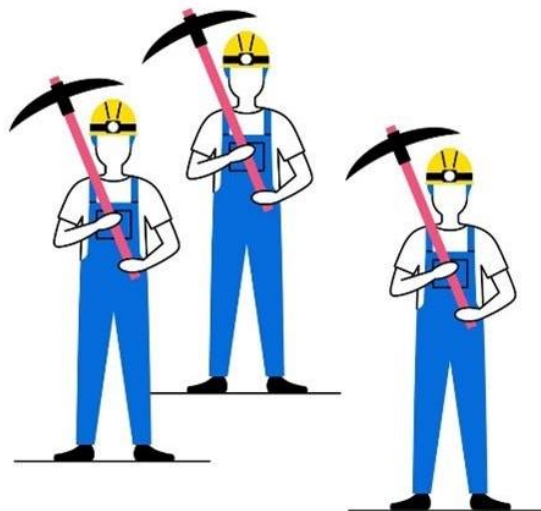
The miners in a network compete to find a solution to a resource-intensive computer calculation

The first miner to find the solution receives a block reward

Source: Bitpanda

_____

_____

Proof of Work requires miners to solve an extremely difficult math problem to earn the right to validate new blocks. This problem is so difficult that it can only be solved by random guessing. As such, miners often employ dozens to hundreds to thousands of computers to make millions of guesses, hoping that one of them gets the correct answer.

This uses a lot of electricity, and therefore effectively costs miners a lot of money to "bid" on the right to validate transactions (it's not uncommon for a miner to spend tens to hundreds of thousands on electricity costs before successfully mining a block).

Once a miner solves the puzzle, she will then update the blockchain with the new transactions and send it to the other miners on the network for approval.

- If she did everything correctly, the network will accept the new block and she will receive a reward (at the time of writing, the current reward for mining a Bitcoin block is ~$120K).

- If, however, she tries to cheat the system, it would be painfully obvious to everyone – the aforementioned hash would be broken and the new block wouldn't connect to the old one. As such, the network will reject the new block, causing the miner to not only lose out on the rewards, but also waste money on electricity costs.

So, at the end of the day, the network is secured by economic incentives and game theory – a miner who acts appropriately could receive hundreds of thousands of dollars in rewards, while one who attempts to cheat the system will almost certainly be left with nothing but a huge electricity bill.

Note: Ethereum switched to a different consensus mechanism – known as Proof-of-Stake – in mid-September 2022. We will cover Proof-of-Stake in more detail in Chapter 18.

How to Read a Decentralized Ledger

As discussed, one of the cool things about decentralized ledgers is that everyone can view every single transaction in real time. For instance, if you go to the Blockchain.com Bitcoin explorer, you will see all of the given transactions at any moment.

_____

Transactions on the Bitcoin Network at 10:58PM on September 7th, 2022

Hash	Time	Amount (BTC)	Amount (USD)
dacaaf1fb52dabb75583e935dc08606401feb1701c4e3c8a4adb4babec812c16	22:58	0.00269283 BTC	$51.80
48d6ca24348d51be067d5185d81074b8446c0463bad0fc92d9ddb8214ba858b6	22:58	4420.13192602 BTC	$85,033,392.96
bb7b2cd71c5e7dd4cc3f67b9606144927bc879e7c2f64d8837bd2caacac77fad	22:58	0.62740712 BTC	$12,069.90
44a32325007eda4e2860fbaacd7549f853f8c4f391e182f89b58ce88cc620eac	22:58	0.00194224 BTC	$37.36
31dc8c4eaf35bbb46a3a0a7e4828fac887946c814928ad875eadf658fe98b0b0	22:58	0.03728612 BTC	$717.30
cfebcda238730ee839a4ff42bf6c8e160872778a36f237e9367fa09b01c49b5f	22:58	0.31294431 BTC	$6,020.34
a4478fdb3db21075ba654c2f3c283b8b207aed36d7b7bd6582f0abe645030c60	22:58	0.00114482 BTC	$22.02
a82a83f769d601485c5857721c67c72adb9fd591b6670c2ac92b1046e7545bb7	22:58	0.70219707 BTC	$13,508.69
b235e2eef159e7edd17fa4feaddec153bcfbf1f0270166e4f6b889694f15ce3b	22:58	0.06602435 BTC	$1,270.16
026cfcace0873d2204b6faea5fccda24dfa25d2182fc052137acc01d5c421a54	22:58	0.82703800 BTC	$15,910.35
990de70473fcf85669ff9d7551f9ec15947904ed46e2e52c3db45175fdf64fa6	22:58	0.04208540 BTC	$809.63
62d76792b5d975d348eae0a495284c610b86c4cab71f910c35ee7d856781da4c	22:58	0.00393706 BTC	$75.74
da464ab19f224123f5073ea91d5bc8cf5039757202507ea67b98161ab8dc81a9	22:58	0.03115040 BTC	$599.26
1eb7c212467cde16aef55c4c39704b5803e20005befc790333131715cf12720a	22:58	0.11181304 BTC	$2,151.03
26176033e4ae41676b295259082180c15a83d0dd086a4e241d9893b585b04e62	22:58	0.00390005 BTC	$75.03
d8d4b23a6203afa15a35d4c8987039ced1d7bfff7dc4aa10b6a8630de028592b	22:58	0.00652940 BTC	$125.61
e973d6eabdcb24a19fdac50692ecf50b20c1872b6ac8bcffecd9eced6297635f	22:58	0.00803791 BTC	$154.63

Source: Bitcoin Explorer as of 9.7.22 10:58PM ET

If you click into any of these transactions, you will see details on who is sending the funds, how much they are sending and who is getting paid. Ledger provides a great graphic and writeup explaining this:

Details of a Specific Bitcoin Transaction

Source: Ledger

_____

_____

Let's dig into each:

1. **Transaction ID:** The "hash" represents the unique ID of each transaction. You can always save this number to look up the specific details later
2. **Sender:** This shows the public address of the person sending the BTC and how much they are sending
3. **Fees:** Shows the fees associated with the transaction
4. **Receipient:** This shows the public address of the person or persons receiving the BTC and how much they are receiving. Note that there is a particular technical quirk of Bitcoin that requires them to send all of your Bitcoin everytime you make a transaction and then send the unused amount back to you. So if Alice had 10 BTC and wanted to send 1 BTC to Bob, she would actually send all 10 BTC out, 1 BTC would go to Bob and the remaining 9 BTC would go back to her.
5. **Transaction Status:** Transactions often take several minutes to clear, so this section will often read "unconfirmed" until the transfer goes through

While all blockchains have slightly different formats, virtually every one has a public "block explorer" where you can view the transaction history (e.g. Ethereum's is at etherscan.io).

Again, the ability for anyone to do this is groundbreaking in that it allows us to create highly transparent organizations that greatly reduce corruption and fraud. Imagine, for instance, if we could see where every dollar our government spent went today!

Even today, authorites are using these public block explorers to track (and often recover) stolen funds from cryptocurrency hacks.

_____

_____

Chapter 11: Overview of Notable Cryptocurrencies

Although there are many different types of cryptocurrencies, the market is dominated by three: Bitcoin, Ether and stablecoins.

Market Share of Major Cryptocurrencies

Other 28%

BTC 39%

Stablecoins 16%

ETH 17%
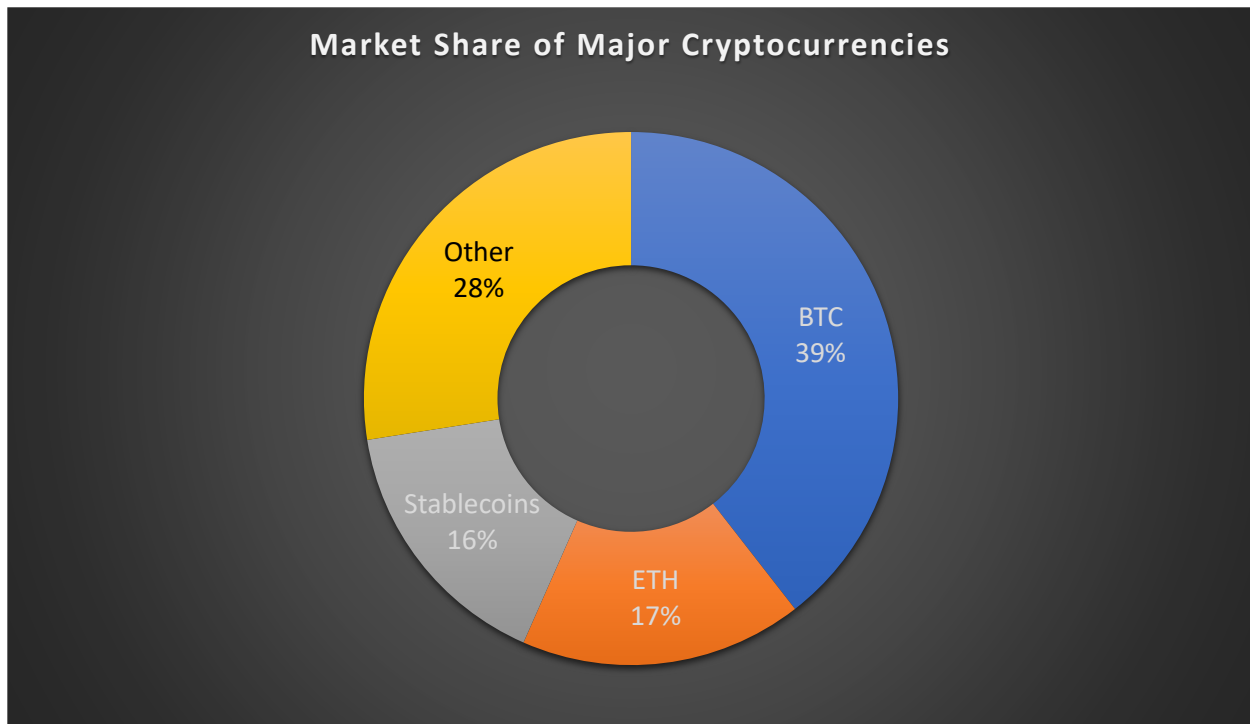
Source: Coinmarketcap as of 10.2.22. Respective market caps divided by total market cap.

- **Bitcoin**: Bitcoin is the world's first and largest pure cryptocurrency
- **Ether**: Ether is the native token of the smart contract platform Ethereum. It can be thought of as a form of "programmable money" (e.g. it can be coded to automatically repay loans, hold funds in escrow, automatically execute contracts, etc…)
- **Stablecoins**: Stablecoins are cryptocurrencies pegged to the value of fiat currencies such as the Dollar, Euro, Renminbi or Yen

We'll dive into each of these a bit more below (and also cover Ether and stablecoins in more detail in later chapters).

Bitcoin

What is Bitcoin?

Bitcoin ("BTC") is the grandfather of all cryptocurrencies. It was created in 2008 by an unknown person or group of people using the alias Satoshi Nakamoto and as of October 2nd, 2022, it has the largest market capitalization of any asset in the space at $369 billion (and it exceeded one trillion in the bull market of 2021).

_____

_____

Bitcoin's Market Cap Exceeded $1 Trillion in 2021
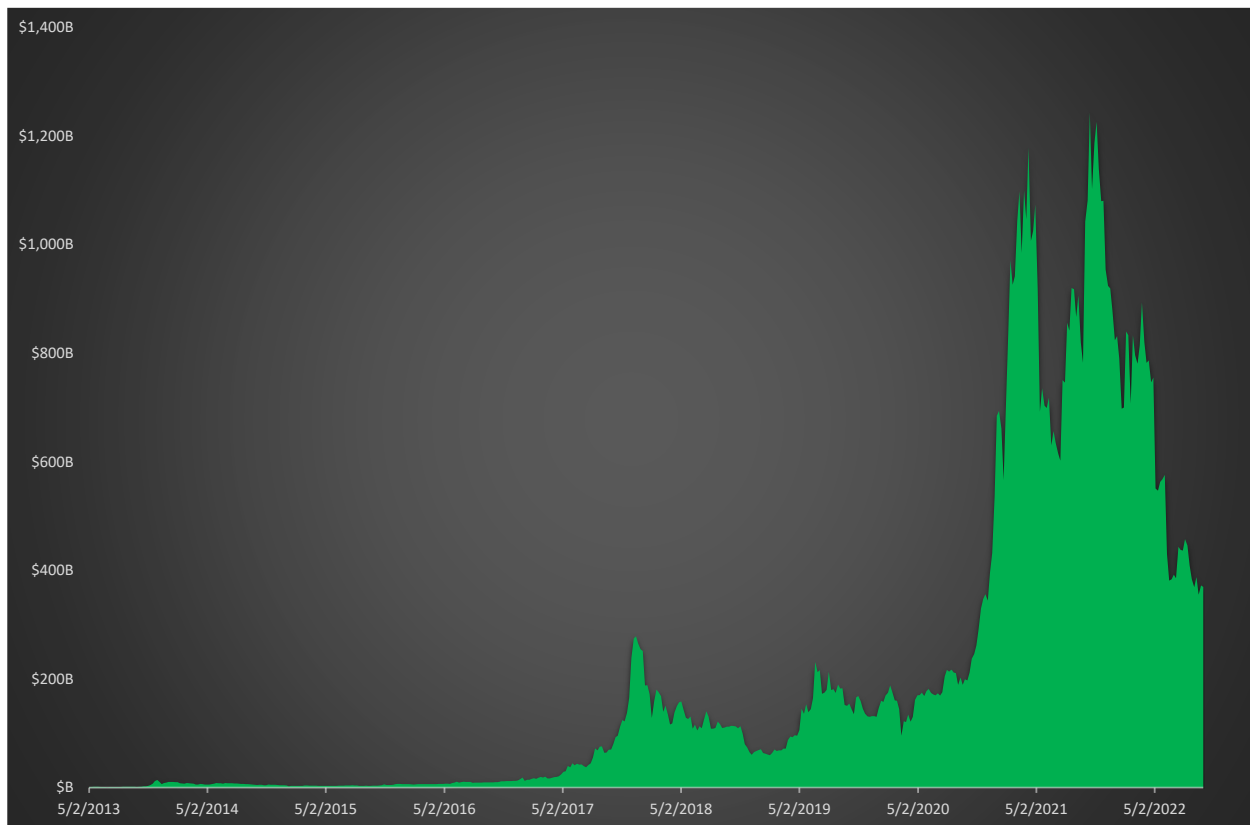
Source: Coinmarketcap as of 10.2.22

Satoshi created the currency to combat what they saw as the perils of unchecked spending by the government. As such, Bitcoin famously limits its supply to 21 million coins, and often earns the moniker "digital gold" as a result.

A few local and national governments are officially using Bitcoin in some capacity, with one country, El Salvador, adopting it as a legal tender.

What are the Benefits of Bitcoin?

Bitcoin proponents believe that the currency is unique among its peers. The most extreme of them, often called "maxis", argue that anything else is a "shitcoin".

While that may be a bit extreme, the currency does have its strong points, including:

1. **Network effect**: Bitcoin is the undisputed market leader with almost 40% share of all cryptocurrencies and almost 90% share of digital currencies. Although this percentage has been steadily declining, it will likely serve as one of the dominant forces in the spaces for years to come.

_____

_____

2. **Decentralization**: While most cryptocurrencies are migrating to a Proof-of-Stake system to lower transaction costs, Bitcoin will continue to use Proof-of-Work. While this means that the currency might be more expensive and less environmentally friendly, proponents argue that it's the most secure and most decentralized method, as it would be extremely difficult for anyone to monopolize the supply of electricity.

3. **Inflation resistance**: Many Bitcoin enthusiasts believe its strongest benefit is lies in inflation resistance. In his book *The Bitcoin Standard*, Saifedean Ammous argues that fiat currencies have been "unsound money" since they went off the gold standard in the 70s. According to Ammous, unsound money leads to recessions and debt, hyper-inflation and even war! By limiting its supply to 21 million BTC, the currency reduces the threat of inflation and therefore (hopefully) mitigates these downsides.

Although Bitcoin is by far the largest digital currency, there are a few other players in the space.

<u>Who are the Other Players in the Space?</u>
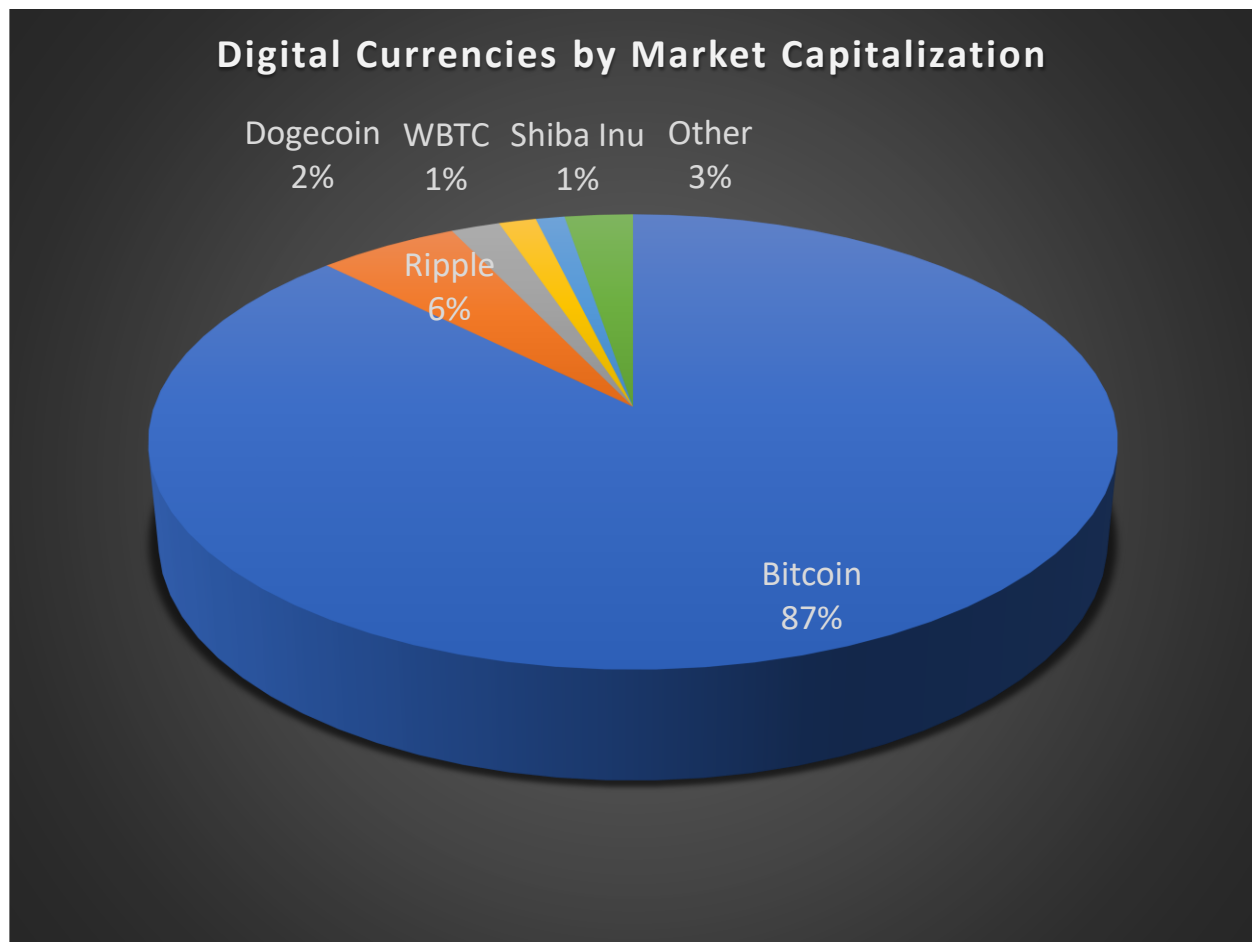
Source: Coinmarketcap as of 10.2.22

Bitcoin dominates the digital currency market holding almost 90% market share. In addition to Bitcoin, other notable projects that can be considered pure "digital currencies" (as opposed to

_____

smart contract platforms, stablecoins or tokens designed to run a specific protocol) are Ripple, Dogecoin, Shiba Inu and Wrapped Bitcoin.

Project	Market Share	Description
	87%	Bitcoin is the world's most popular digital currency.
	5%	Ripple was built to provide an international payments network for banks via XRP, its native cryptocurrency. The project intends to replace legacy systems such as SWIFT with a cheaper and faster method of sending funds. Ripple has fallen out of favor with many in the blockchain community amidst concerns of centralization and ongoing issues with the SEC.
	2%	Dogecoin was originally created as a joke to lampoon cryptocurrencies, but it has grown in popularity. It's similar to Bitcoin in that it uses Proof-of-Work, but proponents argue it's superior because it's faster and cheaper. Unlike Bitcoin, Doge is inflationary, which critics argue is a major issue.
	1%	Shiba Inu is another "meme coin", created on the Ethereum network as a competitor to Dogecoin.
	1%	Wrapped Bitcoin is a "clone" of Bitcoin that operates on the Ethereum network. As such, it has the same value as a Bitcoin but it can be used, traded, borrowed or lent through DeFi applications.

_____

Ether

What is Ether?

Ether is a form of "programmable" money. It was conceived in 2013 by Vitalik Buterin, launched in 2015 and is currently the second largest cryptocurrency with a current market capitalization of $160 Billion (and the project exceeded $500 billion in the bull run of 2021).

Ethereum's Market Cap Exceeded $500 Billion in 2021
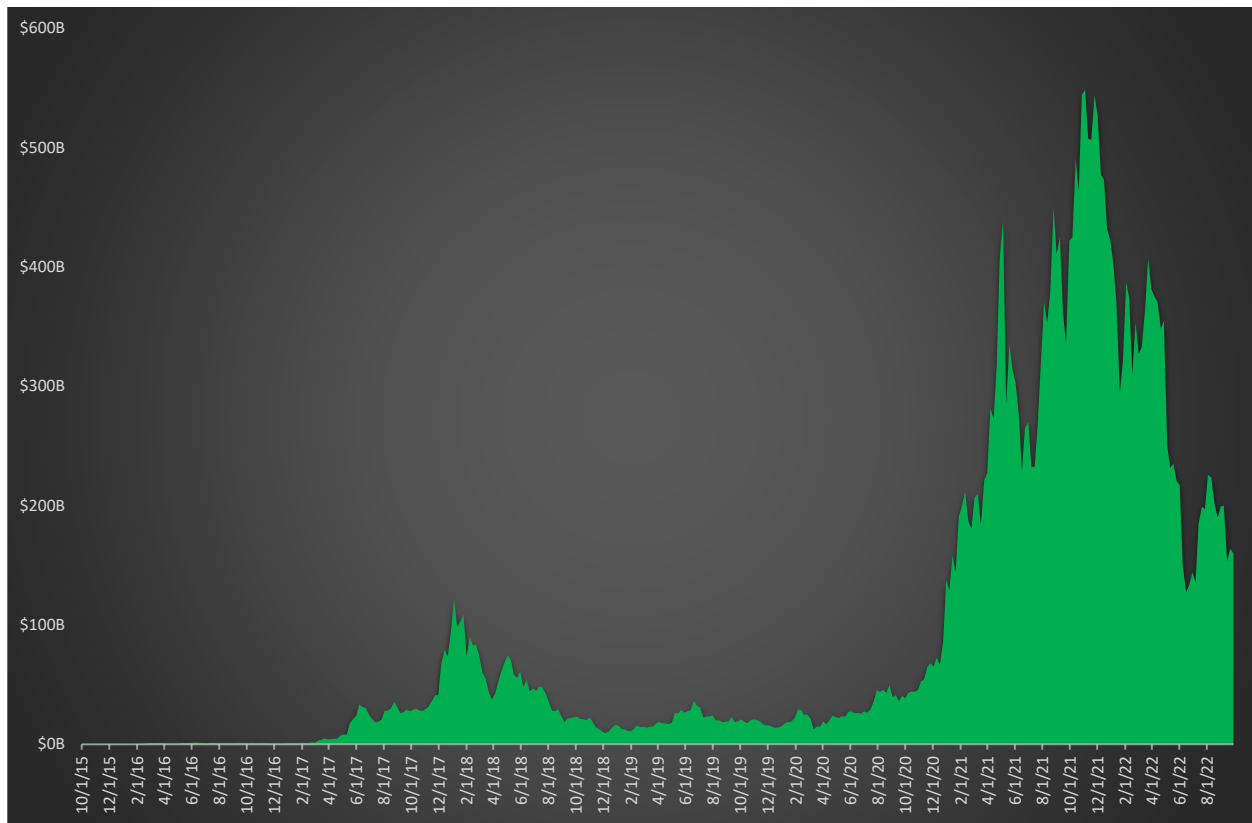
Source: Coinmarketcap as of 10.2.22

Unlike Bitcoin – which functions very similar to traditional forms of money such as the USD or gold – Ether can be programmed to act in a certain way if predetermined criteria are met.

This has several important applications such as:

1. **Recurring Payments**: Ethereum can be programmed to make automatic payments at predetermined times. This has an almost unlimited number of use cases including loan repayments, stock divided payments, automated payroll, etc…

_____

_____

2. **Escrow**: Large transactions often require escrow services to hold funds while a sale takes place. Currencies like Ethereum eliminate the need for this as they can be programmed to automatically release the funds once the deal is consummated.

3. **Contracts**: Ethereum can also be programmed to settle more complex transactions. For instance, one could write an insurance contract that automatically pays policy holders if certain criteria are met (i.e. it could pay drought insurance funds to a farmer if the temperature averages over 90 degrees for any given month)

This functionality is supported by a decentralized "cloud" computer known as the Ethereum Virtual Machine ("EVM"). Like any computer, it can run a variety of programs – not only the ones listed above, but it can also host a variety of decentralized applications such as cryptocurrency exchanges, play-to-earn games, lending and borrowing protocols, music streaming services, etc… (we will discuss these in more detail in Part 3: Smart Contract Platforms).

In addition to serving as a currency to buy goods and services, Ether is also needed to i) pay for the computing power required for transactions on the EVM and ii) serve as the platform's primary consensus mechanism.

This trifecta of uses makes the coin unique among assets.

Benefits of ETH

Perhaps the most interesting take I've heard on the potential of Ether as money comes from David Hoffman of Bankless in his article "Ether: The Triple Point Asset".

Hoffman references an argument by economist Robert Greer that maintains that assets have historically served one of three functions. They are either:

- **Capital Assets:** Capital assets generate cash flows for the owner. Examples include stocks that pay dividends, bonds or rentable real estate

- **Consumable Assets:** Consumable assets generate value when they are used. Oil, coffee and electricity all fall in this category

- **Store-of-Value Assets:** Store of value assets can't be consumed nor do they provide cashflows, but they nonetheless have value. Examples include gold, traditional currencies, real estate, art, or Bitcoins

Although real estate and gold come close, no single asset has satisfied all three functions.

<u>No existing asset simultaneously produces cash flow, stores value and is consumable</u>

_____

_____

[placeholder]	CAPITAL ASSETS "Ongoing source of something of value…valued on the basis of net present value of its expected returns."	CONSUMABLE/ TRANSFORMABLE ASSETS "You can consume it. You can transform it into another asset. It has economic value. But it does not yield an ongoing stream of value."	STORE OF VALUE ASSETS "Cannot be consumed; nor can it generate income. Nevertheless, it has value; it is a store of value asset."
EQUITIES	X		
BONDS	X		
INCOME-PRODUCING REAL ESTATE	X		X
PHYSICAL COMMODITIES (e.g., grains or energy products)		X	
PRECIOUS METALS (e.g., Gold)		X	X
CURRENCY			X
FINE ART			X

Source: PlaceholderVC via Bankless

Ether, however, does. A token on the Ethereum network has what Hoffman calls an "economic trifecta" because it acts as a:

- **Capital Asset:** Ether produces passive income through staking

- **Consumable Assets:** It is needed to pay gas fees on the Ethereum Virtual Machine

- **Store-of-Value Asset:** Ether is the most used form of collateral to be "locked" in DeFi

So in a sense, an Ethereum token is like a dollar bill, blue chip stock and barrel of oil all rolled into one!

_____

_____

Who are the Other Players in the Space?

Smart Contract Platforms by Market Capitalization

Other
18%

Avalanche
4%

Solana
5%

Cardano
6%

Binance Smart Chain
18%

Ethereum
49%
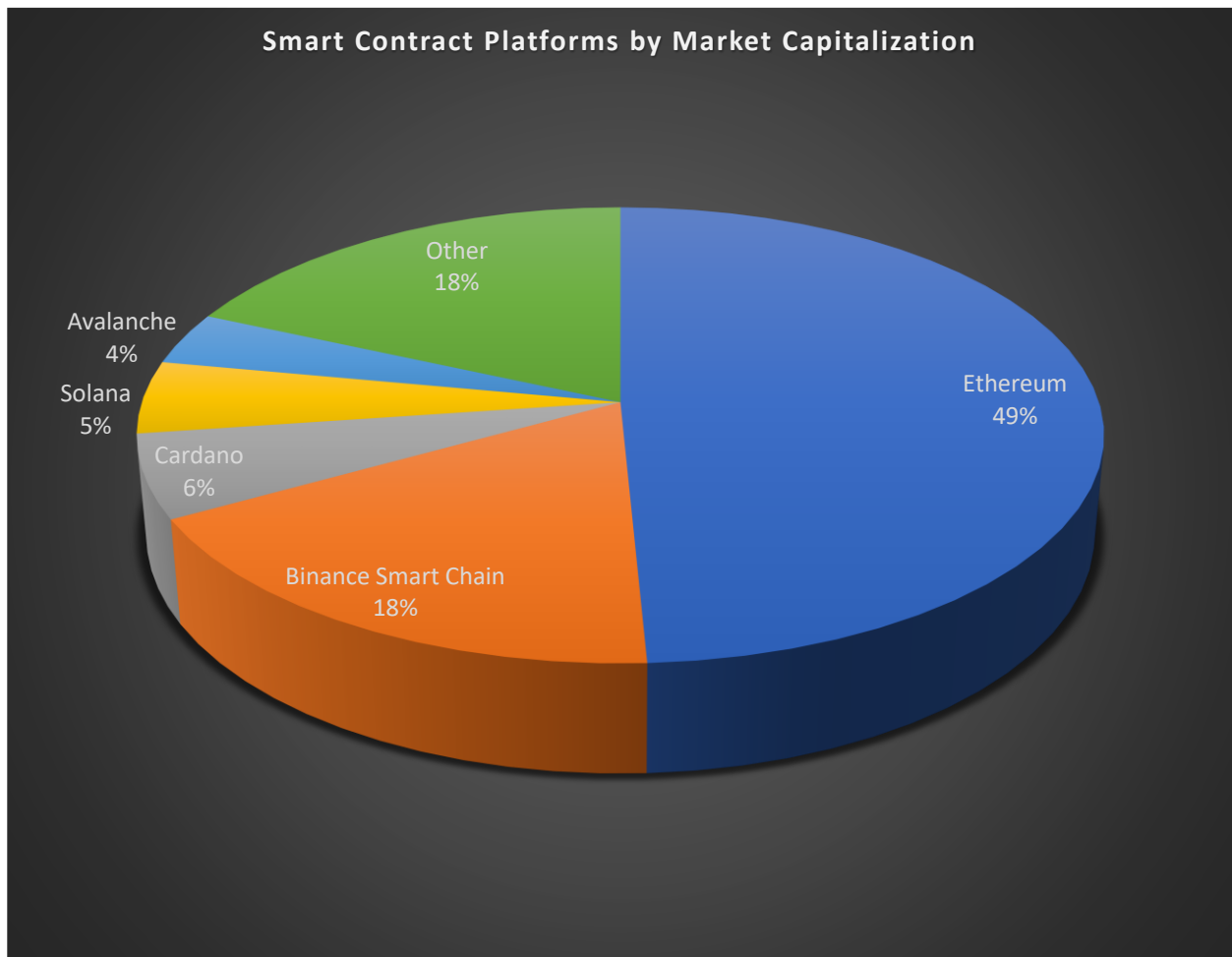
Source: Coinmarketcap as of 10.2.22. Represents fully-diluted market capitalization.

The smart contract market is highly consolidated, with Ether holding nearly 50% market share and the second four players – BNB Chain, Cardano, Solana and Avalanche garnering an additional 32%.

_____

_____

Protocol	Market Share	Description
ethereum	49%	Despite losing a third of its market share in 2021 due to high fees, Ethereum is still the undisputed king of Layer 1s. With the upcoming release of Ethereum 2.0, it will likely continue to be the dominant force in the space
BNB CHAIN	18%	BNB Chain is the native smart contract platform of the crypto currency exchange Binance. Despite capturing a relatively large share, it is criticized for being highly centralized
CARDANO	6%	Often called the first "third-generation" blockchain, Cardano was conceived in 2015 by Ethereum Co-Founder Charles Hoskinson and launched in 2017. After several years of development, smart contracts started to go live in late 2021
SOLANA	5%	Solana is a single-chain protocol that boasts the fastest speeds (>50,000 TPS) and lowest fees (<$0.00025) of any major smart contract platform
AVALANCHE	4%	Avalanche has historically been one of the fasted growing smart contact platforms, increasing TVL by over 60x in 2021 (although skeptics will say that they "bought" growth through aggressive incentive programs)

_____

Stablecoins

What are Stablecoins?

While both Bitcoin and Ethereum have their benefits, one thing limiting their development is price volatility. After all, how can we use cryptocurrencies as a medium of exchange if the value is so unpredictable? What good are double-digit interest rates if the value of the underlying assets can decrease by 50% overnight?

Stablecoins help mitigate this volatility. In a sense, a stablecoin is nothing more than a cryptocurrency pegged to a (relatively) secure asset such as the US Dollar. They can be used to buy things, lend and borrow, collect interest and even hold as a store of value. In effect, anything you can do with cash you can do with a stablecoin.

Total Stablecoin Supply
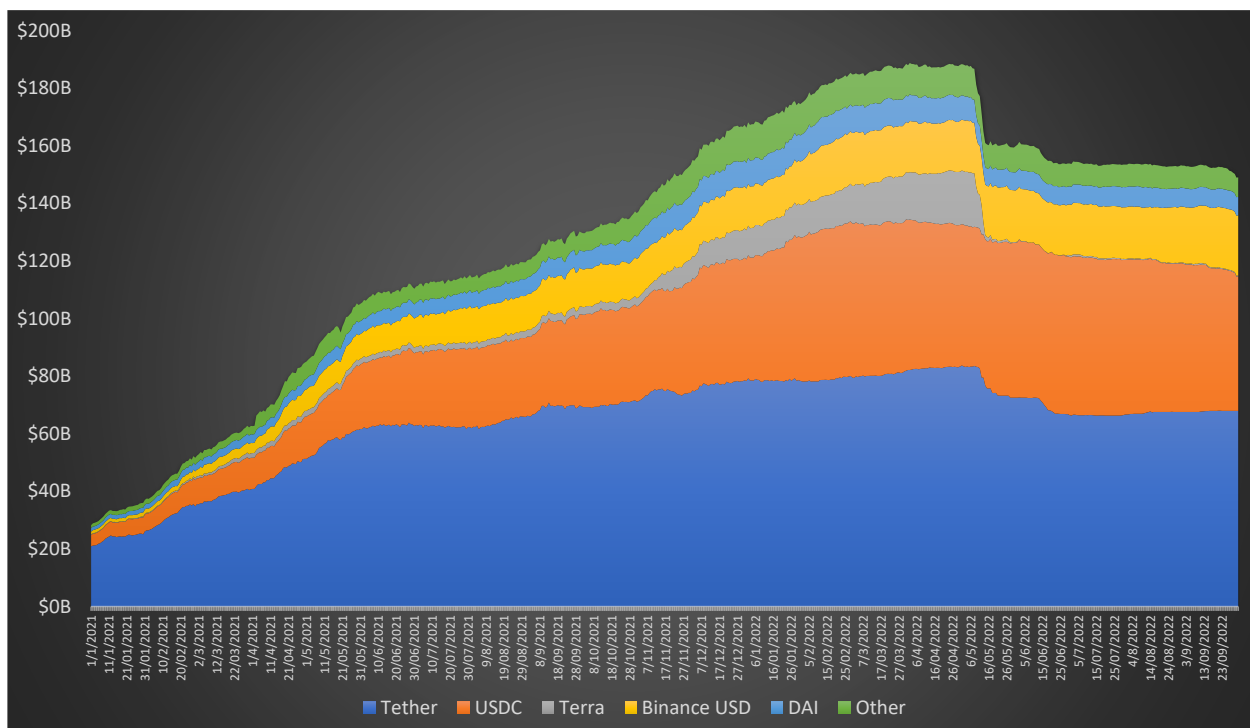
Source: DefiLlama as of 10.2.22

The stablecoin market has grown almost 500% from 2021, and currently stands at $149B.

How do Stablecoins Work?

While on the surface stablecoins might seem very similar to the digital money we use today, under the hood they are very different animals. Perhaps the most glaring distinction is in the ownership and control of the assets. The dollar is owned by the United States government – the Fed sets the rules and controls the supply, commercial banks distribute the funds through fractional reserve banking and depositors receive interest.

_____

Stablecoins on the other hand, are a form of private money. They either are governed by a corporation or a DAO (to keep things simple you can think of this as a collective), users create and distribute the funds by depositing collateral and token owners claim the interest.

Today, there are three main types of stablecoins:

1. **Fiat-Collateralized**: Fiat-collateralized stablecoins such as Tether and USDC are (or at least claim to be) fully backed by cash or similar assets. That is, for each $1 of Tether, there should be $1 sitting in a bank account somewhere.

   The problem with these coins is that, by definition, they are still centralized, relying on banks and other third-parties to keep custody of the collateral. This goes against the decentralized ethos of crypto, as any centralized point in the chain makes the entire system vulnerable and serves as a magnet for regulators.

2. **Crypto-Collateralized**: Crypto-collateralized stablecoins such as Dai are, as the name suggests, backed by a basket of cryptocurrencies and use autonomous protocols to maintain the peg.

   While promising, crypto-collateralized stablecoins are currently very inefficient, requiring huge amounts of overcollateralization. That's why the holy grail of DeFi has long been the creation of an Algorithmic Stablecoin.

3. **Algorithmic**: Algorithmic stablecoins are decentralized and do not require collateral. The peg is maintained through a complicated incentive program. In essence, when the price goes above $1, more coins are issued, diluting the supply and lowering the price. When it goes below $1, coins are bought back to raise the price.

While algorithmic stablecoins are great in theory, they may not be possible in practice. Economists are quick to point out that they violate the "impossible trinity", which states that you can't have a free capital flow, sovereign monetary policy and a fixed exchange rate at the same time.

Indeed, virtually every experiment in this space has failed because incentives stop working if people don't believe there's inherent value in the currency. Once trust is loss, everyone sells, contributing to a "death spiral" that quickly reduces the value of the coin to zero.

The most notable example of this was the collapse of the algorithmic stablecoin Terra, which grew to a 10% share of the market and then abruptly collapsed in May 2022, wiping out tens of billions virtually overnight.

<u>What are the Benefits of Stablecoins?</u>

Whether or not this problem is solved by the current batch of market participants, stablecoins will likely continue to play a major role in the economy as they offer several core benefits:

- **Permissionless**: Anyone can access stablecoins and use them to freely move assets across international borders

_____

_____

- **Cheaper:** Although Ethereum is currently experiencing a significant fee problem, many competing networks offer near-zero fees for using stablecoins (much less than the 2-3% charged by Visa and Mastercard)

- **Faster:** Stablecoin transactions and transfers are near instant and can be performed at any time

- **Programmable:** It's helpful to remember that stablecoins are software and, as such, can be easily programmed into smart contracts, creating a variety of potential use cases

- **Transparent:** Anyone can view the underlying code and all transactions are easily discoverable on blockchain explorers

Who are the Key Players in the Stablecoin Market?

Stablecoins by Market Capitalization

Dai
4%

Other
5%

Binance USD
14%

Tether
46%

USD Coin
31%

Source: Defillama as of 10.2.22

The market for stablecoins is currently dominated by the fiat-collateralized model, with Tether, USDC and BUSD holding a combined 91% market share.

_____

_____

Project	Market Share	Description
tether	46%	Tether is a fiat-collateralized stablecoin that is (or at least claims to be) fully backed by cash or similar instruments. For each $1 of Tether, there should be $1 sitting in a bank account somewhere.
USD Coin	31%	Like Tether, USDC is a fiat-collateralized stablecoin backed by US dollars held in reserve. The token is very popular on Coinbase.
BUSD	14%	BinanceUSD is another fiat-collateralized stablecoin backed by US dollars or treasury bills. It was created as a partnership between Binance and Paxos.
DAI	4%	MakerDAO is a decentralized organization responsible for the creation and management of DAI, a decentralized, crypto-collateralized stablecoin.
Terra	<1%	Terra is an algorithmic stablecoin that once held 10% market share in the stablecoin market. The project rapidly collapsed in May 2022, destroying tens of billions of value.

Other

This report focuses on cryptocurrencies that are primarily used as a form of payment or, in the case of smart contract platforms, to run a payment network.

That said, while virtually all cryptocurrencies can be used as a form of money, many were designed primarily for other means, including tokens that are used to:

- Run DeFi protocols (e.g. Uniswap and Aave)
- Power decentralized oracle networks (e.g. Chainlink)
- Serve as gaming tokens (e.g. Axie Infinity)
- Provide currency for virtual worlds (e.g. Decentraland and Sandboxx)
- Assist with DAO governance (e.g. ApeCoin)
- Enable key web3 infrastructure (e.g. Arweave, Filecoin, Helium, Pocket Network, The Graph)
- Assist with interoperability (e.g. Thorchain)

Since there are tens of thousands of cryptocurrencies, we won't focus on these here, but they will be covered in detail in other reports.

_____

_____

Chapter 12: The Long-Term Potential of Cryptocurrencies

While pundits have long compared the rise of cryptocurrencies to the infamous 'Tulip Bubble' that gripped Amsterdam in the early 1600s, I think we're well beyond that point.

Bitcoin has Lasted Over 4x Longer Than Comparative "Bubbles"
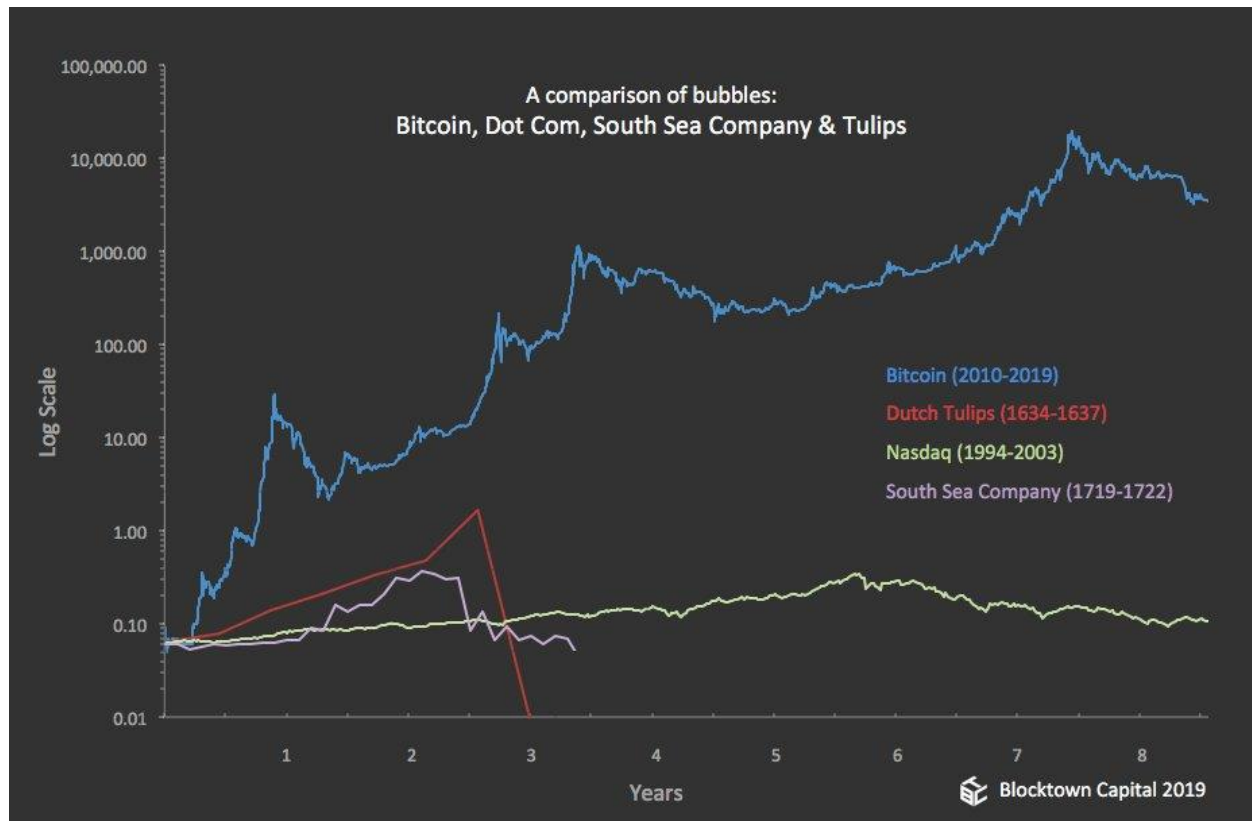
Source: Dan Held via Twitter

Bubbles don't pop and form again, and the Bitcoin "run" has lasted significantly longer than either tulips or the South Sea Company (where Issac Newton famously lost more than $3 million in today's money)

Indeed, cryptocurrencies have survived on merit, and one could argue that they're the best form of money that the world has ever known.

The Best form of Money the World Has Ever Seen

If we were to use the six properties of money discussed earlier to compare cryptocurrencies to the USD and gold, we would see that they are superior in almost all aspects.

_____

_____

Strengths and Weaknesses of Gold vs. USD vs. Bitcoin as a Form of Money

	Gold	USD	Bitcoin	Notes
Durability	◕	◑	●	Because it exists on an immutable blockchain backed up by thousands of computers, cryptocurrencies are extremely durable
Portability	○	◑	●	As electronic money, cryptocurrencies are highly portable. In addition, because there are no restrictions on international transfer, they are more portable than dollar-backed electronic currencies.
Uniformity	◕	●	●	Cryptocurrencies are fungible, meaning that they can always be exchanged for another coin from the same family
Divisibility	◔	◑	●	Every Bitcoin can be divided into 100 million pieces called Satoshis
Limited Supply	◕	○	●	Unlike the USD, Bitcoin cannot be inflated (there will only ever be 21 million)
Acceptability	◔	●	◔	Acceptability is crypto's greatest flaw
Total	◔	◑	◕	Taken as a whole, cryptocurrencies are a superior form of money by almost any definition

The only area where crypto falls short is the fact that it's not widely accepted. But adoption has been steadily increasing now, and we may soon see a "tipping point". According to Zippia:

- Over 15K businesses worldwide accept Bitcoin, including Microsoft, PayPal, Whole Foods, Etsy, Home Depo, AMC Theatres and Starbucks
- 36% of small and midsize businesses in the US accept cryptocurrency
- There are over 35K Bitcoin ATMs in the US

In addition, El Salvador became the first country to accept Bitcoin as legal tender in 2021 and several researchers argue that Panama, Cuba, Ukraine and Paraguay may soon follow suit.

_____

Stoking the Fires of Disruption

In addition to being a better form of money, cryptocurrencies are leading revolutions in several other related spheres including:

1. **Digital Gold**: Gold has long been sought out as both an inflation hedge and seizure-resistant asset. Bitcoin offers all the benefits of gold with two major advantages – it's infinitely divisible and internationally portable. This could benefit numerous parties, including the super-wealthy who want to replace their Swiss bank accounts, those in developing countries who need an inflation hedge but can't access gold and anyone who wants to avoid the cost and restrictive nature of sending money abroad. As such:

   Digital Gold could replace fiat currencies and central banks (e.g the USD, Euro, British Pound, RMB, Yen, the Fed, Bundesbank, Bank of England and IMF)

2. **Decentralized Finance**: Cryptocurrencies, especially stablecoins, are already creating an entirely new financial infrastructure known as decentralized finance ("DeFi"). DeFi offers many of the same features as the traditional financial ecosystem, such as i) lending and borrowing, ii) asset trading, iii) derivatives and iv) insurance without relying on the banks. This eliminates unnecessarily high fees, onerous KYC requirements and the threat of seizure and gives the almost 2 billion unbanked people access to basic financial services.

   Decentralized Finance could replace Wall Street (e.g. Goldman Sachs, Morgan Stanley, Bank of America, Chase, Fidelity, the New York Stock Exchange)

3. **Web3**: Cryptocurrencies such as Ethereum have the potential to form the basis for a new, "internet-first" economy – one owned by its users instead of global mega-corporations. We are already seeing the beginning phases of several new industries enabled by blockchain technology such as NFTs, Play-to-Earn Games, the Metaverse and DAOs. In many of these ecosystems, cryptocurrencies are the dominant form of money. As such:

   Web3 could replace Silicon Valley and Hollywood (e.g. Microsoft, Amazon, Apple, Facebook, Netflix, Spotify, Disney, Activision, Warner Music, Google)

Given the enormous potential of cryptocurrencies, it's not surprising that many analysts believe that the market could still grow by orders of magnitude.

_____

_____

Quantifying the Potential Value of Cryptocurrencies

While it's difficult to put a number on disruption, when we compare cryptocurrencies to the market cap of gold, global equities, global currency, bonds and real estate, we can see that there is still significant room for appreciation.

Cryptocurrencies Represent a Fraction of Global Asset Values
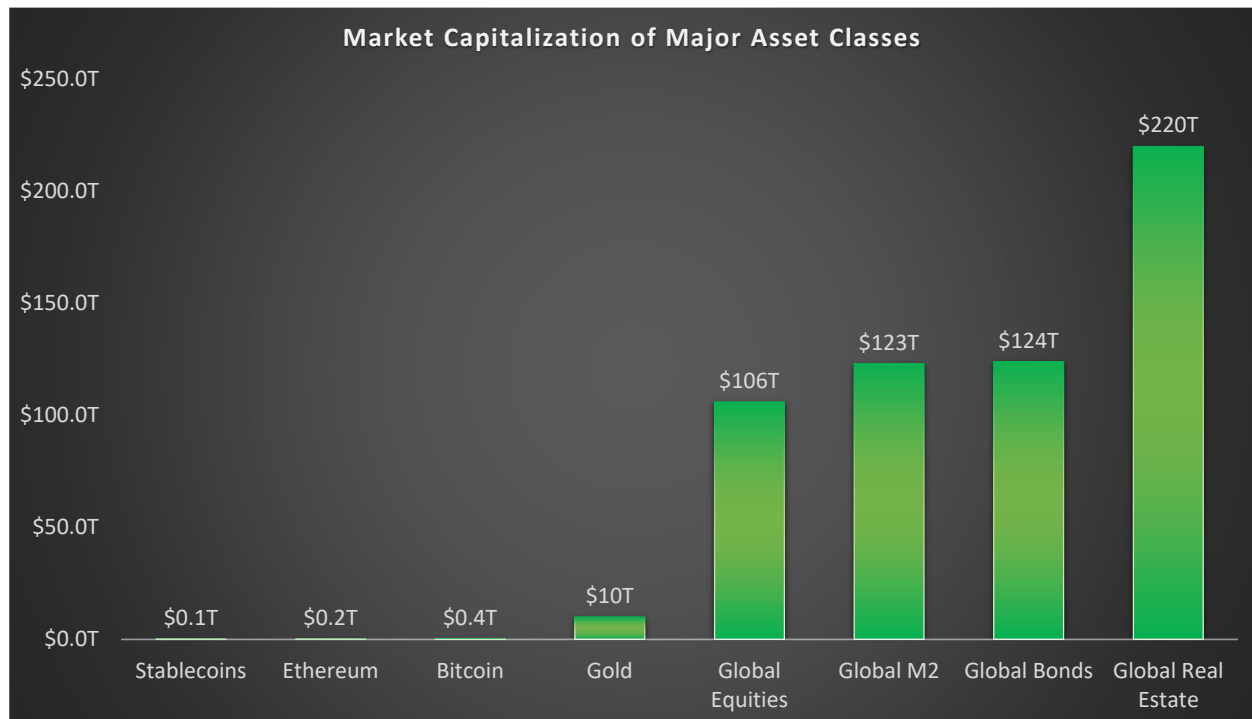
Source: Ark Invest Big Ideas 2022 Report. Gold, equities, M2, bonds and real estate as of November 2021.

Perhaps it's for this reason that we've seen some mind-blowing predictions for the future value of Bitcoin, Ethereum and several stablecoins:

- **The Stablecoin market could grow 1,000x:** While this prediction from Jeremy Allaire, the founder and CEO of Circle (the company behind USDC) is both aggressive and probably a bit biased, there is at least some merit to the logic. Allaire argues that the minimum TAM for stablecoins is $120T (the global value of M2 currency) and that the technology's advantages over conventional money may ultimately grow the market (a la Uber). While achieving 100% market penetration is unlikely, this prediction nonetheless helps make the case that stablecoins likely have a lot of room to grow from their current market cap of $149B.

- **Bitcoin could be worth $1M per BTC:** Ark Invest, the $50B fund founded by Cathie Wood, believes that a single Bitcoin could be worth $1 million by 2030. She reasons that the currency could capture up to 50% of global remittance payments, 10% of M2 in emerging markets, 25% of US bank settlement volumes, 1% of total national reserves, 5% of the

_____

_____

treasuries of S&P 500 companies, 5% of global HNWI wealth, ~3% of the institutional asset base and 50% of gold's total market cap.

- **Ethereum could hit a $20T market cap:** Ethereum has started to see legitimate traction as "money". It's the preferred collateral in DeFi, the unit of account in NFT marketplaces and likely currency of Web3. As such, Ark believes it could capture 15%-20% of the global M2 supply over the next ten years. This would equate to almost $170K per ETH, an >100x increase over the time of writing.

Wherever the future takes us, it's important to watch as it has the potential to be both an existential threat to the existing system and a road to almost unlimited potential for investors.

Part 3: Smart Contract Platforms

_____

Chapter 13: What are Smart Contract Platforms?

Smart contract platforms are the computers that run a digital nation. They are responsible for coordinating all economic activity and enforcing the rules.

From a consumer standpoint, a smart contract platform operates much like your laptop or iPhone – it's a computer that you can use to run programs and access applications. Much like your iPhone can host Airbnb, Uber, Facebook, Tinder and Netflix, these platforms can also host almost any type of digital business.

Unlike traditional computers, however, smart contract platforms are **decentralized and distributed**, meaning that instead of being owned by a company like Apple and hosted on server controlled by Apple, they are hosted on multiple computers located all over the world and aren't controlled by any one entity.

<u>Smart Contract Platforms are Decentralized and Distributed</u>
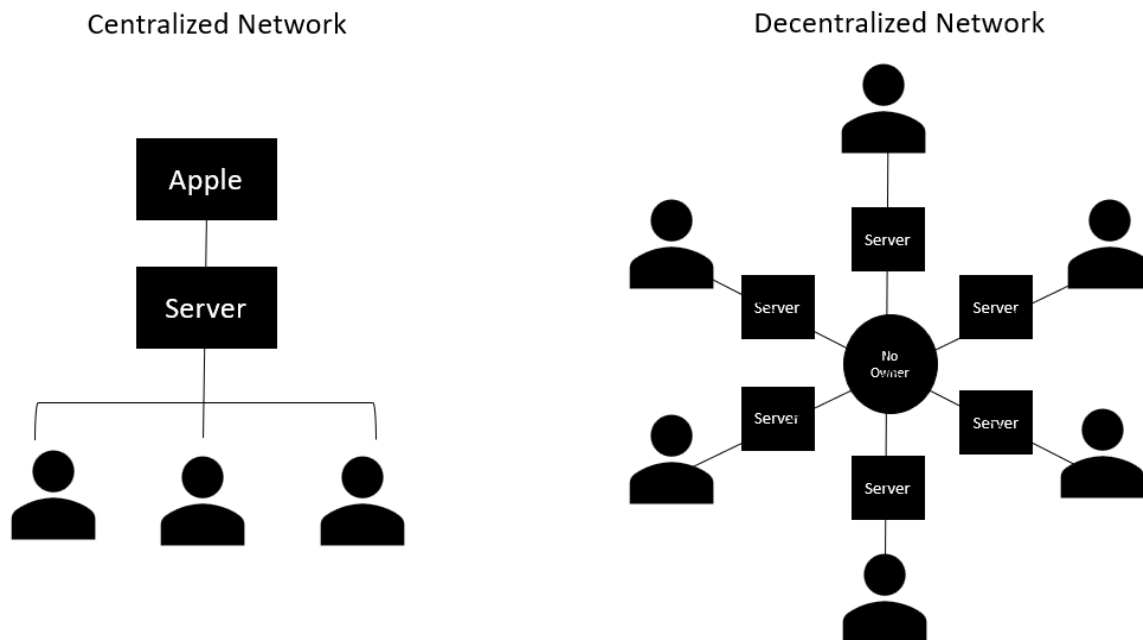
This structure makes smart contract platforms akin to a "shared world computer". Because ownership is shared by multiple parties (i.e. "decentralized"), **no one party can control the network** and tell users what they can and can't do. Because they are hosted over multiple locations (i.e. "distributed"), **no one can ever turn them off or shut them down**.

_____

_____

In addition, smart contract platforms are:

- **Open to Everyone**: You don't need permission to use smart contracts and you can't be blocked – anyone can use them at any time and from any location
- **Permanent**: They can't be changed or manipulated
- **Transparent**: Unlike most corporations today, which choose what users can and cannot see, everyone can see every transaction on a smart contract platform and easily audit things when necessary

As potential world computers, smart contract platforms have the potential to become the fundamental infrastructure layer of a decentralized economy. As such, <u>they are also known as "Layer 1" platforms</u>.

_____

Chapter 14: The History of Smart Contract Platforms

Bitcoin was the predecessor to smart contract platforms, as it introduced the world to the concept of "decentralization" by creating a currency that didn't need the banking system to function.

Although this revolutionized the concept of money, **Bitcoin has limited use outside of its core role as a peer-to-peer payment network**.

Not only is its functionality restricted to the simple transfer of currency, but it also requires users to manually perform all transactions. For instance, if Alice makes a loan to Bob in Bitcoin, Bob will still have to manually access his wallet each month to send Alice the interest payments.

Vitalik Buterin would build upon this foundation with the launch of Ethereum in 2015. Ethereum retained many of the benefits of Bitcoin, such as decentralization, but added the ability to run software programs, making it the first true smart contract platform.

Developers quickly realized the potential of this "world computer", and began to build decentralized applications, known as dapps, on Ethereum. 2017 and 2018, in particular, witnessed an explosion in development with the ecosystem growing almost 10-fold during that period (from 247 dapps in January of 2017 to 2,235 dapps in January of 2019).
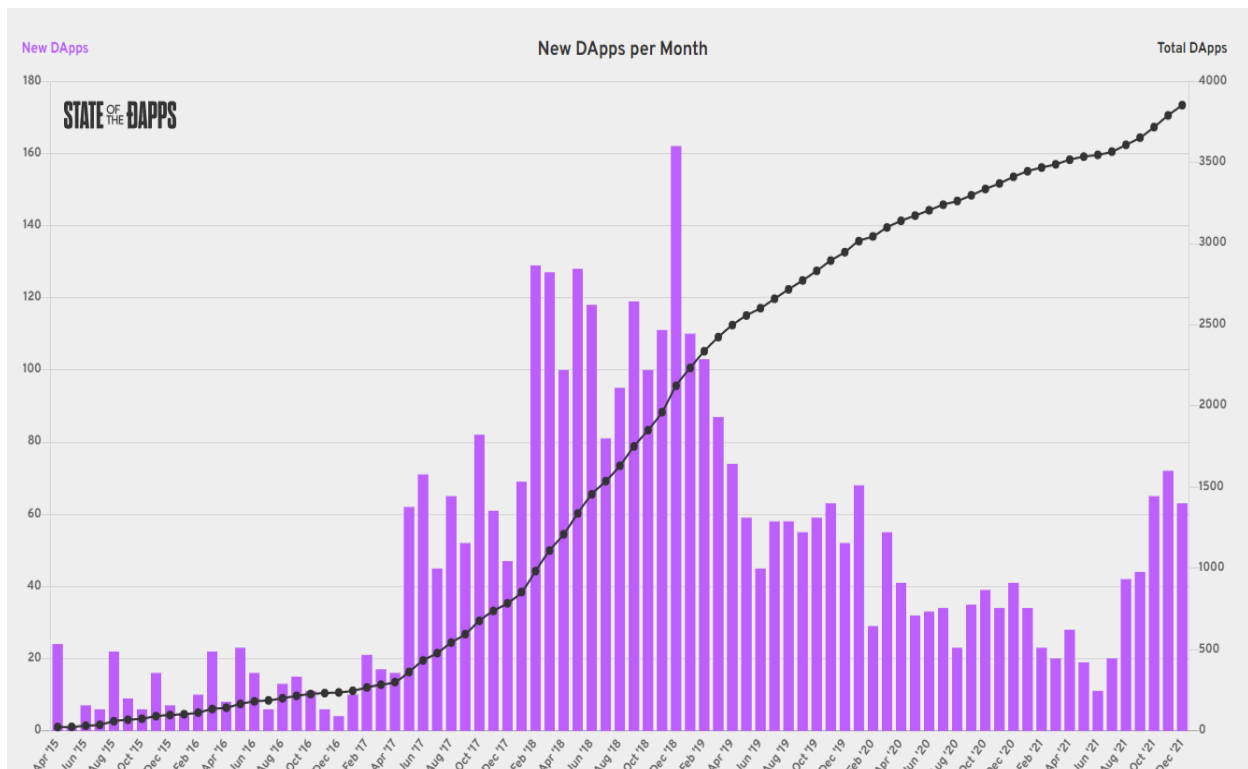
Source: State of the Dapps

_____

Notable dapps launched in 2017-2018 include:

- Uniswap, a cryptocurrency exchange
- Aave, a lending and borrowing protocol
- Nexus Mutual, a decentralized insurance broker
- Cryptokitties and Cryptopunks, early NFTs
- Axie Infinity, a blockchain-based game

As demand for these dapps grew, we began to see an explosion in new smart contract platforms. 2021, in particular, was a year of robust development as projects such as Binance Smart Chain, Solana, Terra and Avalanche began to gain traction, reducing Ethereum's market share from over 95% to almost 60%.

_____

Chapter 15: Why are Smart Contract Platforms Important?

On their own, smart contract platforms are actually terrible computer networks. They are very slow, require more resources than centralized systems and don't have customer support.

But they do one thing well that no other network in existence can do – smart contract platforms can operate without being controlled by a centralized third-party, and this is *extremely* important.

The Problems with Centralized Economies

Our economy is currently dominated by centralized institutions:

- Central banks, such as the The Federal Reserve have sole control over the money supply
- Banks, brokers and exchanges regulate the financial system and control the flow of capital
- National and local governments are the only entities with the power to create and enforce laws
- Companies such as Apple, Amazon, AT&T, Comcast, Disney, Electronic Arts, Facebook, Google, Netflix, Spotify and Sony dominate entertainment, with over 60% market share in a variety of verticals such as publishing, music, gaming and video
- Amazon, Microsoft, Google and Alibaba rule the internet and control over 67% of cloud infrastructure

MARKET SHARE OF CLOUD INFRASTRUCTURE

Amazon 32%
Microsoft 20%
Google 9%
Alibaba 6%
Other 33%

_____
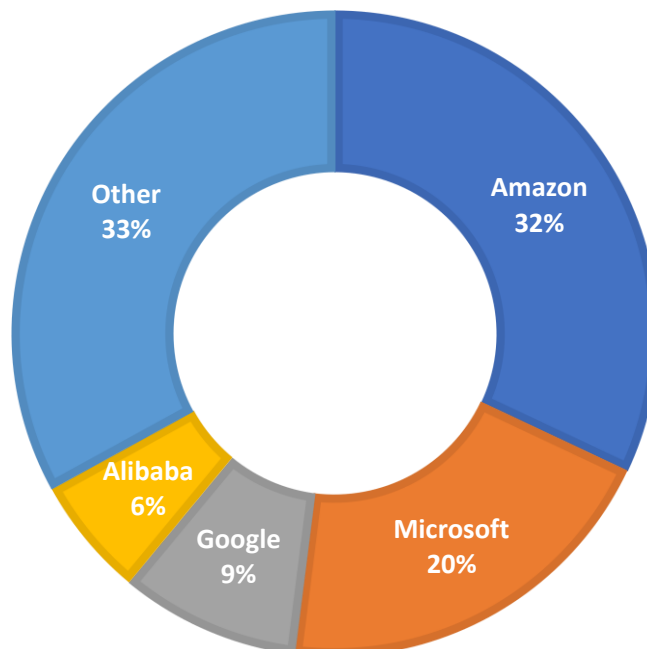
While these institutions have historically benefited us in several ways, they also cause several problems including:

- **Third-Party Ownership of Assets**: In our current financial system, you don't really hold your funds – the banks do. This means that they can freeze and even seize your assets at will (while this may seem far-fetched, consider that in 2013, the Government of Cyprus seized 47.5% of all bank accounts over €100,000 to bail-out its failing banking system)

- **Censorship**: Our economy is ripe with censorship. Social media platforms such as Facebook and Twitter can deny you access and / or censor your content and ISPs can choose to remove websites that they disagree with. In one of the worst examples of a centralized entity abusing its power, Instagram co-opted a woman's "metaverse" username for themselves (Instagram's parent company, Facebook, had recently changed its name to Meta), and only returned it after the press got involved

- **No Privacy**: Banks must collect detailed personal information to adhere to KYC, AML and CFT regulations and require credit scores for borrowing. The internet giants constantly collect data on our income, behavior, interests, location and online activities. To make matters worse, this data is often sold to third parties

- **Expensive and Inefficient:**   Companies such as Netflix and Spotify take the majority of profits from artists. For example, at the turn of the century, a musician could expect to earn over $1.20 for each CD she sold (and that is with the 47% cut taken by her label). But entrance of digital distributors such as Spotify has now plunged this share to between $0.006 and $0.0084 per stream

- **Central Point of Failure:** Centralized services are vulnerable to hacks and denial or service attacks, and also vulnerable to government intervention, regulation or outright banning. This could prove to be a major risk for the "gig economy" as an interruption in service could cost millions of lost wages and a government ban could eliminate millions of jobs

The Benefits of Decentralized Economies

Smart contract platforms such as Ethereum offer the promise of a decentralized economy – one where users can deal directly with one another without needing middlemen.

This can yield a host of benefits, including:

- **User Ownership of Assets**: In a decentralized economy, users control their assets. As such, there's no one to seize their funds, limit withdrawls or tell them where they can and can't spend their money. This is a very important development and forms the basis of DeFi, which we will cover in Part 5.

_____

- **Censorship-Resistant:** Blockchains are permissionless, which means that anyone with an internet connection can use them. You can't be denied based access based on income, geography, gender, etc… You also can't be censored – since there is no central authority that controls blockchains, you can post anything you want at any time you want

- **Privacy:** In the decentralized economy, users can remain completely anonymous. No personal data is required to make payments, receive money or access any website or service

- **Cheap and Efficient:** Innovations such as NFTs will allow artists to deal directly with their consumers, cutting out middlemen like Netflix and Spotify and greatly increasing profits. For example, an artist could create an NFT of a song, sell that to fans and write a contract that distributes the profits from song streaming directly to the owners of the NFT

- **No Central Point of Failure:** Because blockchains are hosted across multiple computers around the world, service disruptions are very unlikely and important data is backed up multiple times.   In addition, because there is no central authority or access point, governments will not be able to shut down sites

The above benefits aren't just theoretical, as we have already seen them play out in several industries. As of October 2022, there's nearly $60 billion flowing through the DeFi space (with a peak of almost $200 billion in 2021), NFT sales are approaching $40 billion, and there has been a flight of talent from Silicon Valley to Web 3 companies.

_____

Chapter 16: How do Smart Contract Platforms Work?

Smart contract platforms are **computer networks that can store information**.

While this may not sound impressive at first glance, it's important to note that **today's Internet cannot store information** – it can only transfer it. In computer science parlance, it is known as a "stateless" protocol.

This greatly limits the inherent functionality of the web. For instance, if a system can't store information, it has no way to conduct economic transactions such as sending and receiving money. After all, imagine having an online bank account that forgets your balance everyday!

To get around this problem, companies need to store data outside of the internet in centralized computers known as "servers".   Each time you need to access information – such as accessing your online bank account – your computer sends a request to one of these servers.

Data is Currently Stored Outside of the Internet on Servers
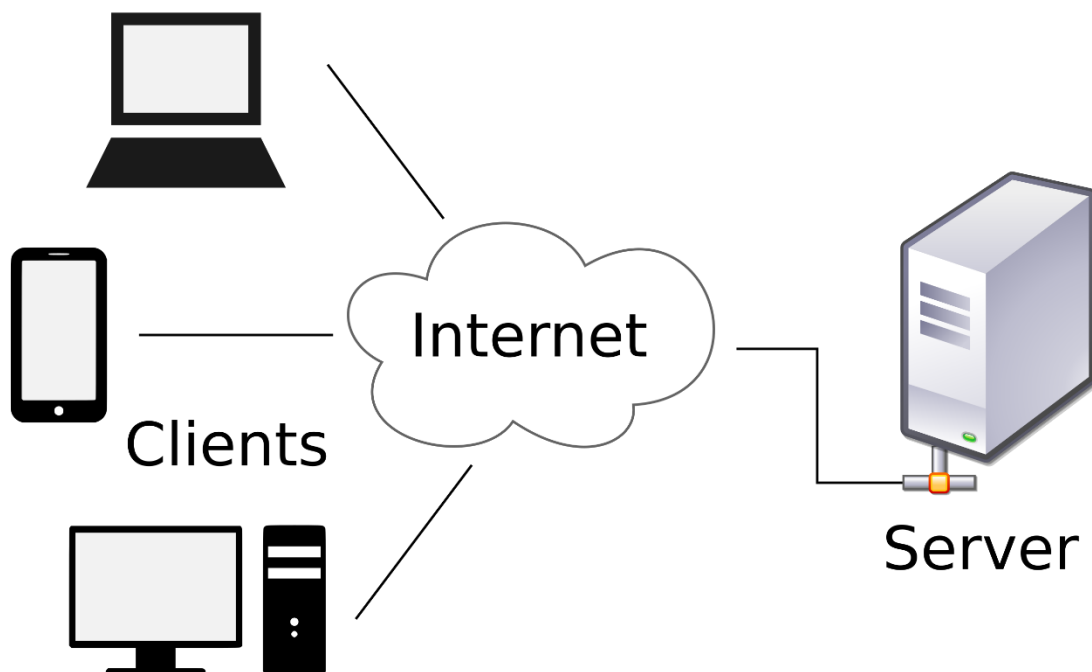
This is part of what is known as the client-server-database architecture which, as the name suggests, has three components:

- **Clients**: Your personal PC or laptop is known as a "client". When you want to visit a website it makes a request to a server to get the relevant information

_____

- **Servers**: Servers are responsible for routing your request to the correct database and then sending the information from the database back to you

- **Databases**: Almost all of the information that you find on the internet is stored somewhere in a database

While this architecture solves the problem of data storage, it unfortunately also requires the oversight of centralized parties such as large technology companies or banks. As stated earlier, companies such as Amazon, Microsoft, Google and Alibaba already control over 67% of cloud infrastructure.

Smart contract platforms are disruptive because they can **store information online without relying on centralized third parties**. This is groundbreaking, as it gives us the ability to create online financial systems that don't need banks, social networks that aren't controlled by Big Tech, entertainment studios that aren't controlled by Hollywood and even entire digital nations that can function without a traditional government.

Let's dive a bit deeper into how this works …

What is "State"?

Smart contract platforms are "transaction-based state machines". I know that's a mouthful, so let's describe what that means.

The concept of "state" refers the ability of a computer network to remember previous information. A system can either be "stateless" or "stateful":

- **Stateless**: Stateless systems **do not** remember previous information.   Most early communications systems, such as radio, telephone, television or the internet are innately stateless. For example, before the introduction of the VCR, there was no way to save what you watched on TV

- **Stateful**: Stateful systems **do** retain and save previous information. Most physical systems, such as a bank vault, are inherently stateful – if you have $100 in a bank vault and add $50, you now have $150

At any given time, the current status of information in a stateful protocol is known as the system's "state". In the prior example, the state of the bank vault is $150 after your deposit.

As discussed, the Internet was originally designed as a "stateless" protocol that could only transfer information and not save it. Before the introduction of third-party data storage services you couldn't shop online, upload photos to a social media service, play games or have an online bank account. In fact, all you could really do was read webpages.

Smart contract platforms, by contrast, are inherently "stateful".

This means that they store important information – such as your bank account balance or the number of points you've earned in an online game – and update this data after each transaction you

_____

perform. So if you transfer $10 to a friend, the next update in a smart contract platform will decrease your balance by $10 and increase theirs by $10.

Smart Contract Platforms Are Transaction-Based State Machines
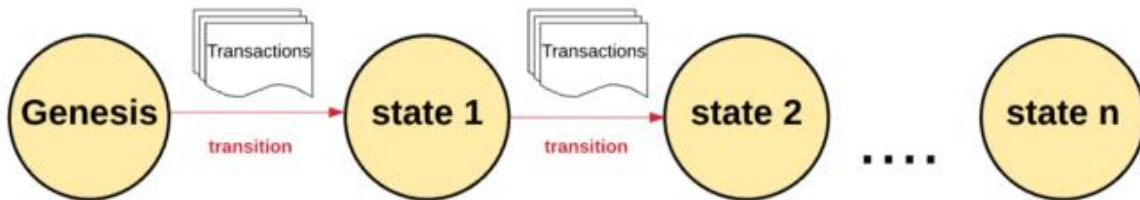
Source: Preethi Kasireddy

This means that we can use smart contract platforms to do all the fun things on the internet – go shopping, watch videos, peruse social media, play games, check our bank account balance, etc… – without having to rely on banks or companies such as Facebook, Apple, Amazon and Google.

How is State Updated?

Smart contract platforms begin with a blank slate known as a "genesis state". Each time a transaction occurs, all balances are updated and a new state is created. As long as the network keeps running, this process will continue indefinitely. At any given point in time, the current state represents the official state of the smart contract platform.

Like cryptocurrencies, smart contract platforms use a combination of three elements – blockchains, smart contracts and consensus mining – to update state without relying on centralized third parties.

_____
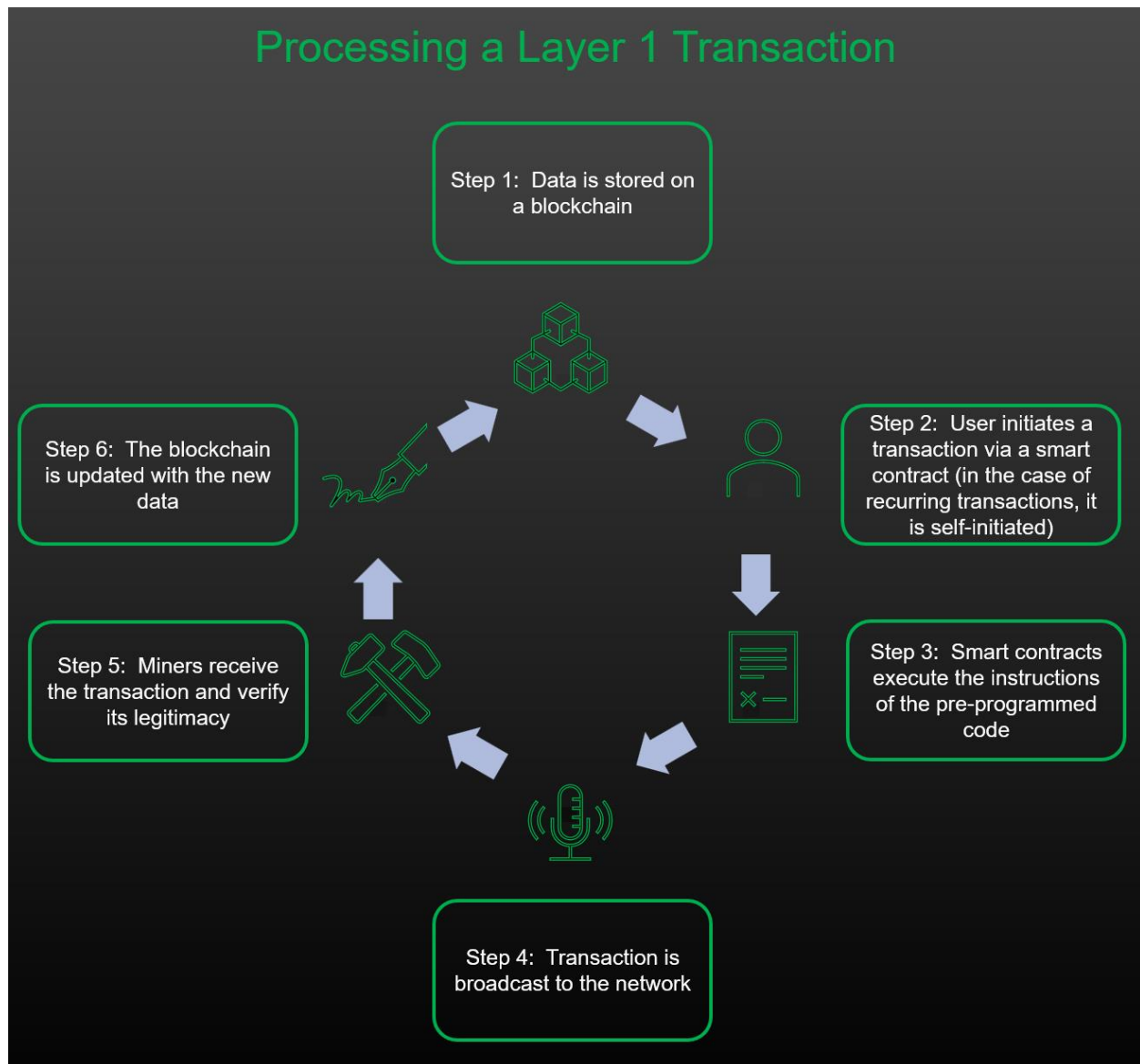
To understand how this works in practice, let's imagine that Bob borrows $100 from Alice and promises to repay $10 each week. He would historically: 1) deposit the $100 in a secure bank account, 2) manually initiate a transaction to send Alice $10 each week and 3) rely on the bank to ensure the funds are transferred to Alice's account.

Using a smart contract platform, Alice and Bob can perform all of these actions automatically and without relying on a bank:

- **Blockchains**: Blockchains **store the current state of the system**. In this case, the original (genesis) state would show that Bob had $100 in his account and Alice had $0

- **Smart contracts**: Smart contracts **change the state of the system**. In this case, the smart contract would be programmed to automatically transfer $10 from Bob's to Alice's account each week

- **Consensus Mining**: Consensus mining **finalizes the new state**. Like with cryptocurrencies, miners serve as the "auditors" of a smart contract platform, ensuring the transaction was performed correctly and updating the blockchain to show that Bob now has $90 in his account and Alice has $10

Let's dig more into each of these technologies below…

What are Blockchains?

Smart contract platforms store their data on a blockchain.

As discussed in Chapter 10, a blockchain is little more than an electronic database – i.e. a collection of information – that is shared across many different computers.

They are an ideal venue to store data as they are:

- **Immutable:** Data can't be hacked or manipulated
- **Distributed:** Blockchains are hosted on thousands of computers located all over the globe and therefore almost impossible to shut down
- **Decentralized:** They aren't controlled by any one party
- **Secure:** Because identical copies of a blockchain are stored across thousands of computers, there is little risk of information loss
- **Transparent**: All transactions and account balances are publicly available for anyone to see

Blockchains can store virtually any type of data including a user's cryptocurrency balances, virtual assets and even point totals for online games.

What are Smart Contracts?

Smart contracts are **digital agreements that execute automatically when pre-determined conditions are met.** They are responsible for changing the state of a Layer 1 platform.

Unlike traditional contracts, smart contracts don't rely on corporations, banks, lawyers, courts or local laws to guarantee their enforcement. Instead, users **trust the technology** and its pre-programmed code to automatically execute when they've upheld their end of the deal.

_____

Smart Contracts Don't Need Lawyers, Brokers, Banks, Courts or Governments
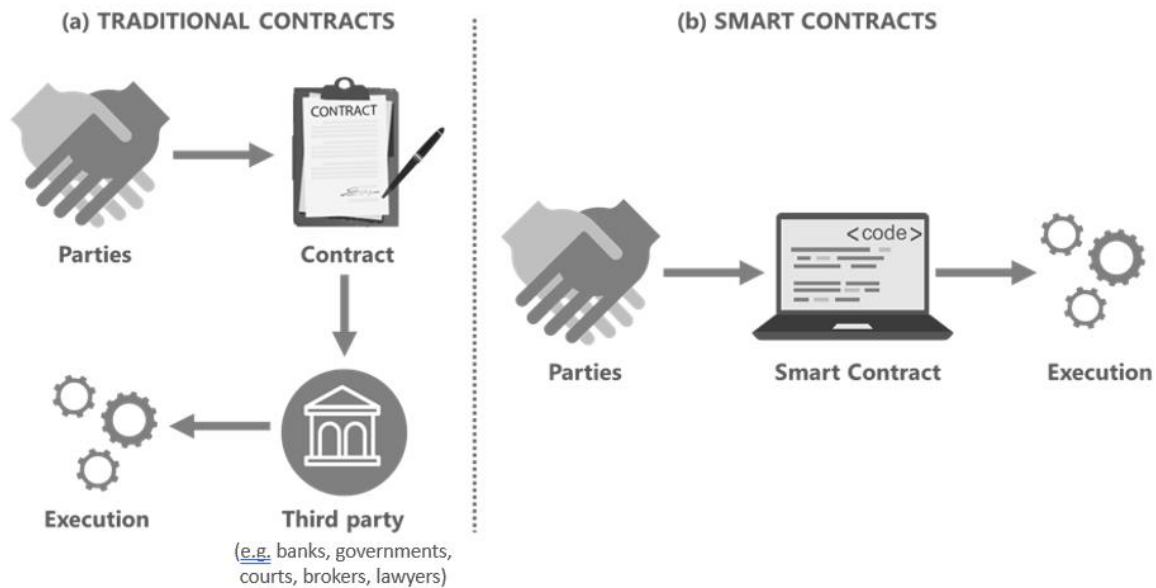
Source: Techskill Brew via Medium

One could program a smart contract to make recurring interest payments on outstanding debt, pay an employee each time she launched a new product or even create a complex insurance instrument. For example, let's say that Farmer John wants to use a smart contract to insure his crops against a drought:

1. Farmer John and Block Insurance (a fictitious entity) agree that if the temperature is above 90 degrees for 5 days in a row, his crops will die
2. Farmer John sends Block Insurance 1 Ethereum (ETH) token to insure his crops
3. The 1 ETH is deposited into a smart contract
4. Block Insurance would deposit 10 ETH into the smart contract as collateral in case of a drought
5. The smart contract monitors the temperature
6. If the temperature remains under 90 degrees, nothing happens and Block Insurance keeps Farmer John's 1 ETH
7. If the temperature goes over 90 degrees for 5 days in a row, the smart contract pays Farmer John 10 ETH
8. Farmer John can offset his crop loss with the profits from 10 ETH

Despite the fancy name, smart contracts are just software programs – snippets of code that execute a series of programmed instructions. As such, they aren't limited to financial transactions

_____

or even "contracts" in the traditional sense and can be used to create art, play games, watch videos, stream music, host documents, store healthcare data, etc…

Basically, any program that can be run on a traditional computer can be run with a smart contract.

What is Consensus Mining?

Consensus mining finalizes the next state of a smart contract platform. Like with cryptocurrencies, miners serve as the "auditors" of a network, ensuring that transactions are legitimate and updating the balances.

While the first smart contract platforms, including Ethereum, used the Proof-of-Work mining system discussed in Chapter 10, newer iterations have transitioned to a consensus mechanism known as Proof-of-Stake ("PoS").

Most Smart Contract Platforms Use a Proof-of-Stake Consensus Mechanism

Proof-of-Work Consensus	Proof-of-Stake Consensus
Bitcoin	Ethereum (after September 2022)
Ethereum (prior to September 2022)	Binance Smart Chain
	Cardano
	Solana
	Polkadot
	Polygon
	Tron
	Avalanche
	Cosmos
	NEAR Protocol

Proof-of-Stake is similar to Proof-of-Work in many ways in that validators (PoS's version of miners) are still required to authenticate and secure the network, and they still receive rewards for doing so. Instead of spending electricity though, validators put up large amounts of the native cryptocurrency as collateral. If they are found to be negligent (or worse, malicious) they run the risk of losing some or all of this deposit.

The main benefit to using Proof-of-Stake is that it's generally orders of magnitude faster and cheaper. This is why nearly all newer blockchains are built using Proof-of-Stake and why Ethereum transitioned to this mechanism in September 2022.

Proof-of-Stake is discussed in more detail in Chapter 18.

How are Stateless Systems Used in Digital Nations?

As decentralized computers, smart contract platforms coordinate all economic activity in a digital

_____

nation. They set the rules for the ecosystem and allow users to create, store and trade cryptocurrencies and digital assets such as NFTs.

Much like a traditional computer can host apps such as Airbnb, Uber, Facebook, Tinder and Netflix, smart contract platforms such as Ethereum can host a variety of decentralized applications such as Uniswap (cryptocurrency trading), Aave (lending), LooksRare (NFT creation and trading), Axie Infinity (a blockchain-based game) and can even be used to run entire decentralized businesses known as DAOs.

<u>Smart Contract Platforms are Computers That Can Run a Variety of Decentralized Applications</u>
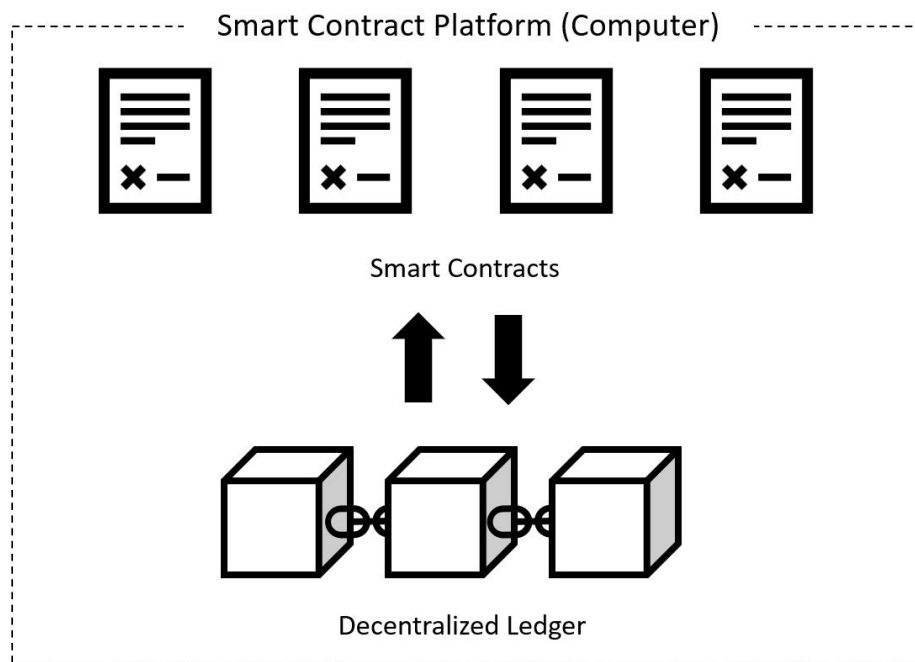
Decentralized Applications

_____

_____

Unlike conventional computer networks – which are run by centralized third parties such as Facebook, Microsoft or Google – these platforms retain the same benefits of Bitcoin in that they are 1) distributed (i.e. simultaneously hosted by thousands of different computers all over the world) and 2) decentralized (i.e. not controlled by a single entity).

This gives smart contract platforms several unique benefits, including the fact that they are:

- **Democratic:** No single party can control the network and tell users what they can and cannot do

- **Open to Everyone:** You don't need permission to use smart contracts and you can't be blocked – anyone with an internet connection can access them at any time and from any location

- **Permanent**: Because they are hosted on thousands of nodes scattered across the globe, no one can ever turn them off or shut them down

- **Immutable:** Data recorded on a smart contract platform is permanent, and can never be changed or manipulated

- **Transparent:** Everyone can see every transaction on a smart contract platform and easily audit things when necessary

- **Secure:** Information is stored on a decentralized and distributed blockchain, meaning that no one can manipulate the data and there is no risk of information loss

Perhaps most importantly, smart contract platforms are *autonomous*.

Because they use decentralized ledger technology to store their own funds and smart contracts to enforce their own laws, smart contract platforms don't need to rely on traditional intermediaries such as banks or courts. As such, they can largely **operate outside of the purview of the existing financial and legal ecosystem**, allowing them to eliminate many of the costs, restrictions and regulations imposed on conventional networks.

Indeed, as they like to say in cryptoland – "code is law".

_____

Chapter 17: What are the Problems with Smart Contract Platforms?

Although Ethereum represents a substantial innovation, it is not without its faults. In particular, the protocol is plagued by high gas fees.

"Gas" refers to the fee required to execute a transaction on the Ethereum network. Whether you want to transfer a token, loan your assets on Ethereum or mint an NFT, you must pay gas to incentive the miners to approve your transaction and include it on the blockchain.

Because space on the Ethereum network is limited – it can only execute around 25 transactions per second – priority is determined by an auction process. This means that gas can get very expensive when the network is busy.

Unfortunately, lately the Ethereum network is always busy, so average gas fees have ballooned across the board. During the height of the bull market, the average fee for a transaction exceeded $30. While we are in a bit of a lull at the time of writing, the 200-Day Moving Average transaction fee still remains close to $10.00, a substantial increase from the $0.18 recorded three years prior.

This makes transactions impractical for the average user.

The Average Transaction Fee on Ethereum is Nearly $10
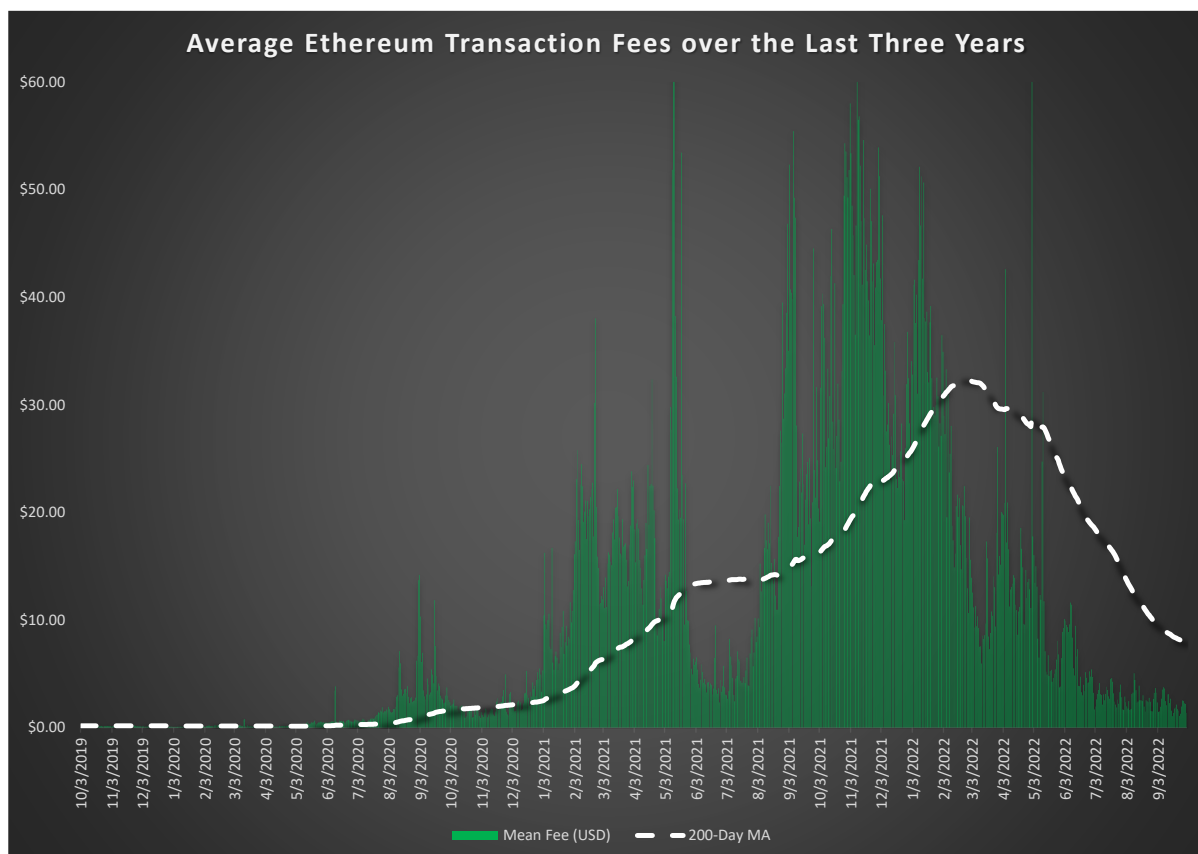
Source: Coinmetrics as of 10.2.22

_____

Keep in mind these are average fees for *all* transactions, including simple ones like a token ETH transfer. As some transactions – such as minting an NFT or borrowing / lending ETH – are generally much more complex, it is not uncommon to see fees of several hundred dollars.

In fact, in times of extreme congestion, commonly known as "gas wars", fees can be in the thousands. The most notable example of this occurred during the Bored Ape Yacht Club's April 30th launch of Otherside, where users had to pay a minimum of $6K in fees to purchase land!

The reason Ethereum is so slow is due to a phenomenon known as the scalability trilemma.

To understand the trilemma, it's important to note that an ideal blockchain would possess three key features:

- Scalability: The ideal blockchain is very fast, can handle a high throughput and is cheap to use
- Security: It would be highly secure and resistant to external attacks
- Decentralization: Perhaps the core tenet of the crypto movement, the ideal blockchain would allow anyone to join and not be controlled by any central authority

Unfortunately, the prevalent theory in the development community states that you cannot have all of these at once and that:

- You can develop a secure and decentralized blockchain, but it will be slow
- You can develop a fast and decentralized blockchain, but it will not be secure
- You can develop a fast and secure blockchain, but it will be centralized

Source: Messari

_____
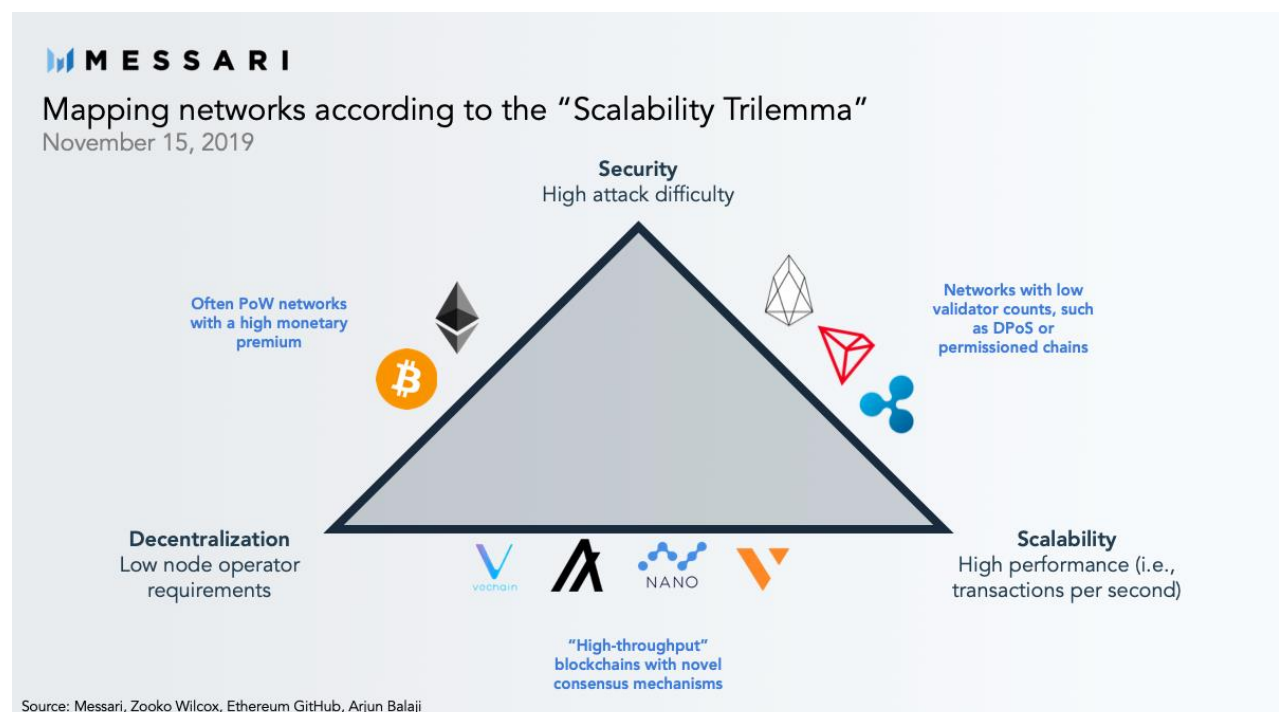
While there's some debate over whether the trilemma is a hard law (which we will get into later), to date we have generally seen these tradeoffs play out, with existing first and second generation blockchains making compromises. For example, networks such as Bitcoin and Ethereum have chosen to focus on decentralization and security over scalability, while others such as BNB Chain and Solana are fast, cheap and secure, but at the cost of being highly centralized.

So how can we mitigate the trilemma and achieve security, scalability and decentralization simultaneously?

Chapter 18: How do we Solve these Problems?

Rest assured that the Ethereum foundation is working hard to find solutions. As Vitalik said:
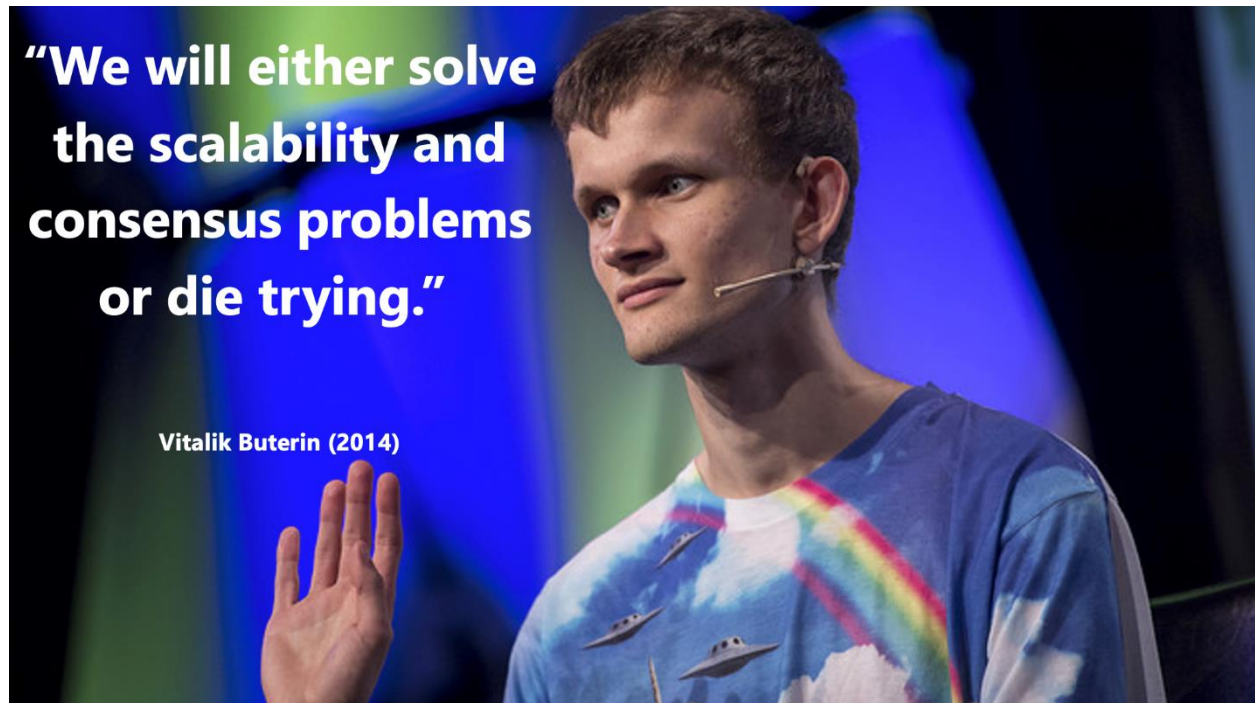
Source: [Messari](#)

Currently, there are several proposed strategies to solve Ethereum's Scalability problem, and they can be broken into two categories:

- **On-Chain Solutions:** On-Chain solutions focus on improving the native blockchain itself. The most popular flavors are i) Consensus Protocol Improvements and ii) Multi-Chain Architectures

- **Off-Chain Solutions:** Off-Chain solutions move transactions, data and or / security off of the native blockchain to increase efficiency. Popular off-chain solutions include Rollups, Side Chains, Plasma and Validium

On-Chain Solutions

Many of the newer blockchains such as Solana, Binance, Cardano, Avalanche, Polkadot and Terra – also known as the "Ethereum Killers" are primarily focused on solving the scalability problem by making improvements directly to their native chain. In particular, all of these projects rely on consensus protocol improvements and several leverage multi-chain architectures.

We will cover these two concepts below as well as examine their potential flaws.

_____

<u>What are Consensus Protocol Improvements?</u>

Consensus protocols are one of the most important elements of a smart contract platform as they provide a specific method to verify transactions, review data and confirm what needs to be added to the ledger. When people say blockchains are "trustless", they are referring to the benefit of these protocols, as they allow a distributed group of strangers to work together to agree on a network's current state.

As discussed earlier, many first and second generation blockchains, such as Bitcoin and Ethereum, used Proof-of-Work (PoW) as their consensus protocol. While Proof-of-Work is proven and very secure, it's also extremely slow (performing fewer than 25 transactions per second) and requires a lot of energy (at the time of writing, Bitcoin alone consumes about as much power as Finland, a nation with over 5 million inhabitants).

That is why virtually all newer blockchains are built on a much more efficient mechanism known as Proof-of-Stake (and why Ethereum migrated to it in September 2022).

Proof-of-Stake is similar to Proof-of-Work in that a distributed group of miners is still required to secure the network. These miners – properly called "validators" in PoS systems – are selected at random and receive an economic benefit for their work in the form of transaction fees.

Unlike Proof-of-Work, which use electricity costs to discourage bad actors, Proof-of-Stake systems require validators to put up large amounts of a smart contract platform's native cryptocurrency as collateral. If they are found to be negligent (or worse, malicious) they run the risk of losing some or all of this deposit.

_____
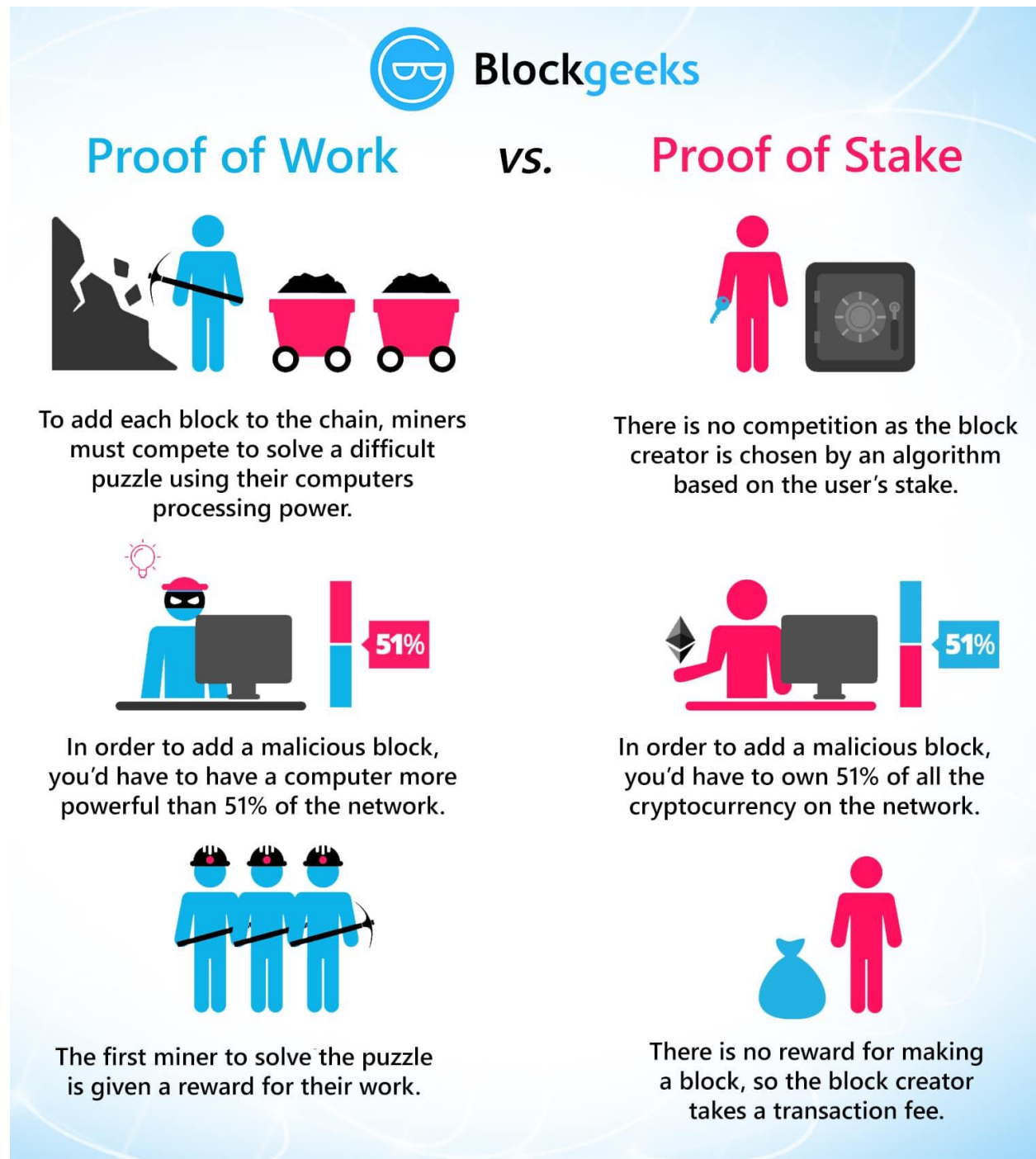
Source: Blockgeeks

The main benefit to using Proof-of-Stake is that it's generally orders of magnitude faster and cheaper. For instance, a protocol known as Solana is combining the mechanism with a concept known as Proof-of-History to achieve a theoretical TPS of 65,000 to 710,000 and fees under $0.00019 (vs. 25 TPS for Ethereum 1.0 and fees of $10).

Solana is discussed in more detail in Chapter 19.

_____

<u>What is a Multi-Chain Architecture?</u>

Single or "monochain" blockchains such as the original version of Ethereum can only process a limited amount of traffic and can quickly become congested.

One simple solution to this is to split blockchains up into many different smaller chains, allowing the network to process transactions in parallel.

Like a freeway adding more lanes, this greatly increases the efficiency of the native blockchain and creates potentially infinite speed (i.e. adding four subchains would theoretically result in a 400% improvement in performance, ten a 1,000% increase, 100 a 10,000% increase, etc…).

Three notable projects using multiple blockchains are Cosmos, Polkadot, Avalanche and the expected upgrade to Ethereum, commonly referred to as "Ethereum 2.0".

<p align="center"><u>Potential Drawbacks to On-Chain Solutions</u></p>
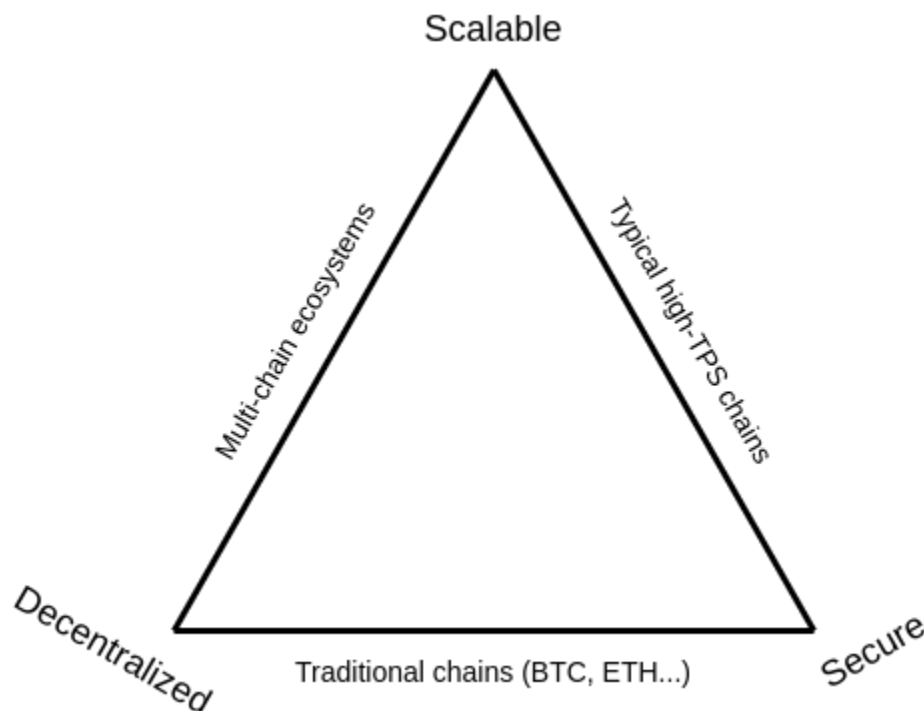
<p align="center">Source: Vitalik.ca</p>

Critics argue that smart contract platforms that rely solely on on-chain solutions will not be sufficient and will be forced to continue to make trade-offs along the trilemma. In particular, they argue that among the current batch of "Ethereum Killers":

- High-TPS chains such as Solana rely on a small number of validators and therefore sacrifice decentralization
- Multi-chain ecosystems aren't as secure because an attacker could gain majority in only one of the chains and break the entire network

_____

They believe that a third piece of the puzzle is required, and that's the implementation of off-chain solutions.

Off-Chain Solutions

<u>What are off-chain solutions?</u>

Off-chain solutions – also known as Layer 2 solutions because they are built 'on top' of a Layer 1 blockchain such as Ethereum – aim to increase scalability while retaining the security and decentralization of the underlying blockchain.

For the purposes of this article, I will highlight four main types of Layer 2 solution:

- State Channels
- Custodial Sidechains
- Non-Custodial Sidechains
- Rollups

<u>Landscape of Layer 2 Solutions</u>
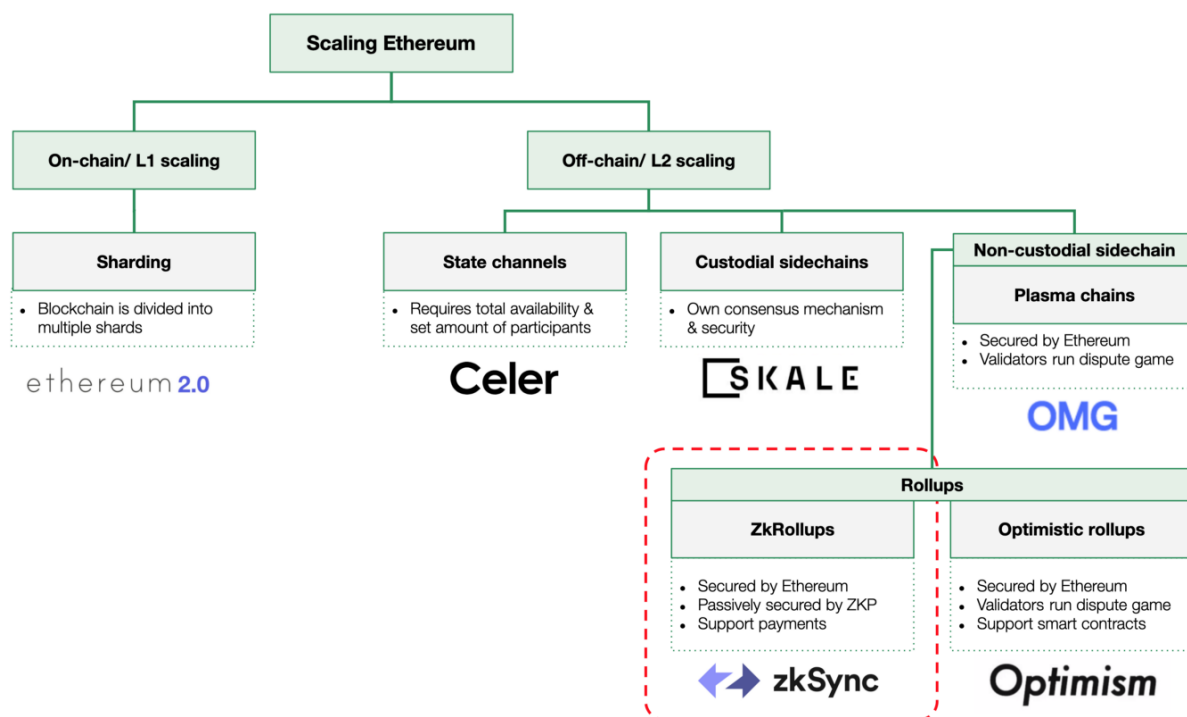
Source: Token Terminal via Medium

Before diving in, however, it's important to remember the three basic functions of a smart contract platform:

- **Execution**: Run programs via smart contracts

_____

- **Data**: Store important data such as account balances
- **Security**: Provide consensus protocols to secure the network

Several of these Layer 2 solutions increase efficiency by **taking responsibility of at least one of these functions off of the main chain**. For example:

- Custodial sidechains remove *all responsibility* from the main chain by maintaining their own security, storing their own data and performing their own execution. For this reason, many people argue that they are not really "Layer 2" solutions at all, but are simply separate blockchains

- Non-Custodial sidechains utilize the security of the Layer 1, but lessen the load by keeping their own data and doing their own execution

- Rollups utilize the security **and** data of the Layer 1, but do their own execution

To summarize:

	Security	Data	Execution
Custodial Sidechains	Layer 2	Layer 2	Layer 2
Non-Custodial Sidechains	Layer 1	Layer 2	Layer 2
Rollups	Layer 1	Layer 1	Layer 2

While most Layer 2 solutions increase speed, many still suffer from similar tradeoffs in functionality, security and decentralization. More detail on this is below:

State Channels

State channels are a very basic scaling solution where two or more users take their transactions "off-chain" and then submit the final results back to the chain. For example, if Alice and Bob frequently transact with one another, they may elect to break off into a state channel for most of their transactions to increase speed and save on fees.

While state channels can be very fast and cheap, they suffer from three main flaws:

- Participants must already know and trust each other
- Users must lock up a large sum of capital
- State channels can't execute smart contracts

While easy to implement, these flaws make state channels unappealing and it is expected that they will continue to lose relevance.

Popular state channels include Bitcoin's Lightning Network and Ethereum's Raiden Network.

Custodial Sidechains

_____

_____

Custodial Sidechains are Ethereum-compatible, **independent** blockchains that maintain their own security. These chains connect to the Ethereum network through a bridge, and users can transfer their tokens to them and process transactions in parallel.

Like the multi-chain solutions described above, adding additional blockchains is a very effective method of reducing congestion on the network, and therefore reducing fees. In addition, because they are completely separate blockchains, sidechains can choose to run protocols – such as Proof-of-Stake – that allow them to operate much faster.

The fact that they are separate blockchains are also their greatest flaw. Users are effectively trusting an entirely different entity with their assets, so if the sidechain breaks (or worse, its creators are malicious) users could lose everything they transferred to that chain.

Given that they are entirely separate blockchains, many would argue that sidechains are not true Layer 2 solutions at all.

Major sidechain projects include Polygon's Matic Network and Skale.

<u>Non-Custodial Sidechains</u>

The security flaws of custodial sidechains led to the development of "non-custodial" sidechains. These solutions are also separate blockchains, but they rely on the security of the main chain.

They do this by 1) removing data from the main chain, 2) performing the necessary calculations and 3) returning the results to the main chain in regular intervals.

Unfortunately, anytime data is taken off-chain, we have to assume that there is a chance that it has been manipulated. As such, non-custodial sidechains have mechanisms designed to prove that the data hasn't been tampered with.

There are two types of non-custodial sidechains:

- **Validium**: When returning data to the main chain, Validium sidechains submit a cryptographically secure "validity proof" to the network, showing that all calculations are valid. The mechanics of this proof are out of the scope of this article, but for reference it is called a "zero-knowledge proof" because it can be used to prove something is true without relaying any additional data.

- **Plasma**: Plasma takes the opposite approach. Instead of submitting a proof, it is assumed that the data is correct BUT users can easily check this through a "fraud proof", which means that there is a 7-14 day waiting period that allows validators to review and reverse the transaction if they suspect fraud.

At first glance, non-custodial sidechains seem like ideal L2 solution as they retain the important benefits of custodial sidechains (i.e. speed) while also retaining the security of the main chain. Unfortunately, they suffer from a few drawbacks:

- Both Plasma and Validium have limited functionality when it comes to smart contract execution

_____

_____

- • Plasma can take weeks to complete a withdrawal
- • Validium is faster than Plasma (10 – 30 min), but can be expensive due to the computational requirements of zero-knowledge proofs

Major plasma projects include Polygon's Plasma Chain and OMG and major Validium projects include Starkware and Loopring.

Rollups

While non-custodial sidechains move both data and computation to a separate blockchain, rollups only move computation off chain. That way, users know that important data, such as their account balance, is secured on ETH.

ZK and Optimistic Rollups Execute Transactions Off-Chain
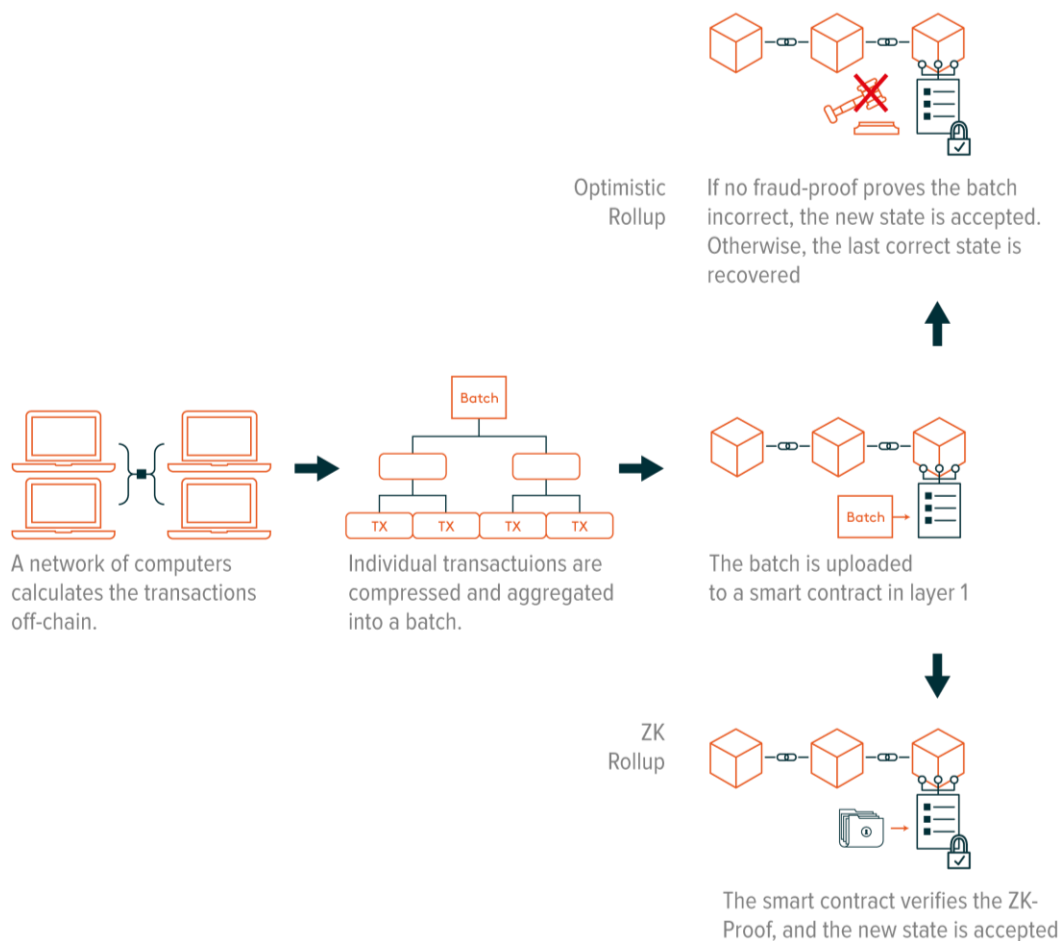
Source: GlobalXETFs

Because rollups execute off-chain, they still need a way to prove to the main network that they're not being malicious. In these types of proof, we find the two different flavors of rollups:

_____

_____

- **zk rollups**: Like Validium, zk rollups use zero-knowledge proofs (that's where they get the name) to show that all calculations are valid.

- **Optimistic rollups**:   Optimistic rollups use "fraud proofs" in a manner similar to Plasma – they institute a waiting period that allows validators to challenge transactions they believe might be fraudulent. This is an important role for validators, who risk having their collateral slashed if they fail to catch a dishonest submission.

In general, zK rollups are faster but offer less functionality, while optimistic rollups have more functionality but are also slower due to the potential of fraud challenges.

As zK rollups mature and more functionality is added, many expect for them to become the dominant L2 solution for ETH.

In fact, Vitalik wrote: "In general, my own view is that in the short term, optimistic rollups are likely to win out for general-purpose EVM computation and ZK rollups are likely to win out for simple payments, exchange and other application-specific use cases, but in the medium to long term ZK rollups will win out in all use cases as ZK-SNARK technology improves."

Major optimistic rollup solutions include Optimism and Arbitrum and major zK- rollup projects include ZKSync, Loopring and Starkware.

_____

Chapter 19: What are the Key Smart Contract Platforms?

Below we dive deeper into some of the top smart contract platforms.   The top 10 participants in the space by fully-diluted market cap are Ethereum, BNB Chain, Solana, Avalanche, Polygon, Polkadot, Tron, Cosmos and NEAR.
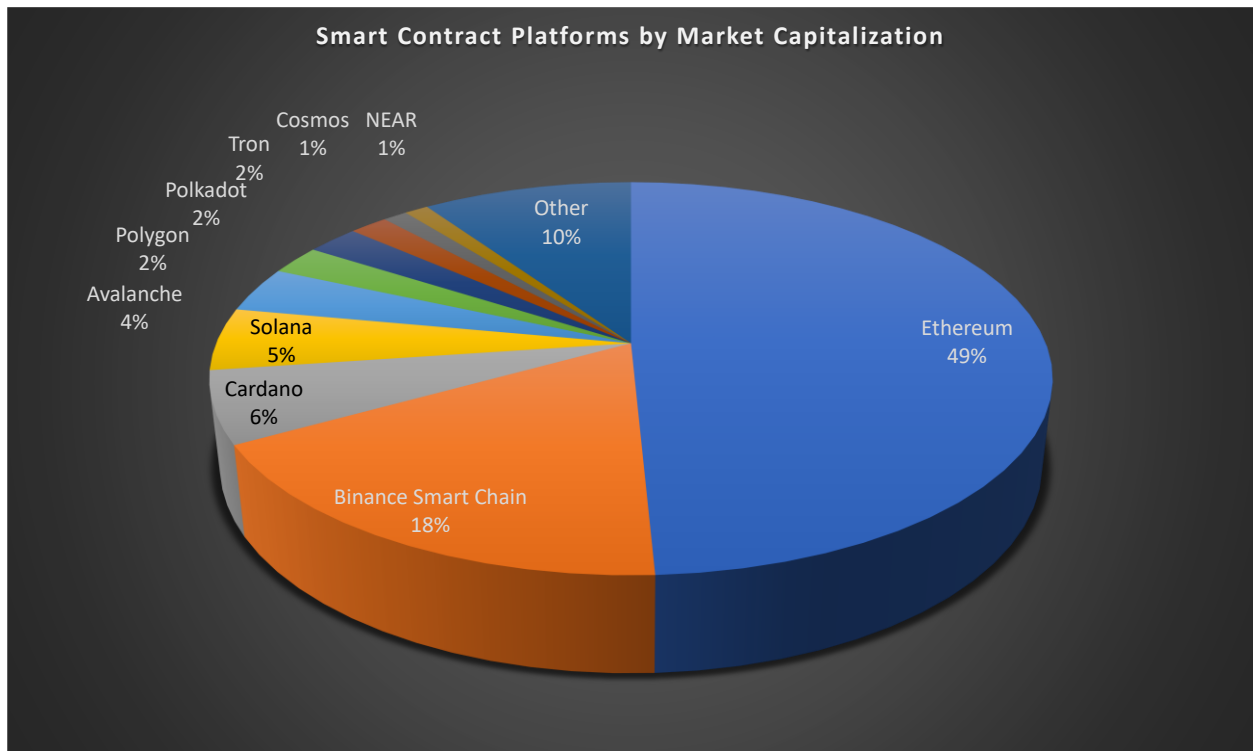
Source: Coinmarketcap as of 10.2.22. Ranked by Fully-Diluted Market Capitalization.

Let's dive deeper into each of these protocols below…

Ethereum

#1 in Fully-Diluted Market Capitalization (as of 10.2.22)

The most notable "Ethereum Killer" might be Ethereum itself.

The protocol has been working on its ETH 2.0 upgrade for some time now, and although the final version may not be released for years, Vitalik hopes that the eventual launch will solve the scalability trilemma once and for all.

(It's worth noting that one of the most critical updates on the path to Ethereum 2.0 – known as "The Merge" – was completed on September 15th, 2022. Buterin estimates that this brings the protocol to the halfway point on its roadmap, representing 55% completion.)

The team at Bankless provides a great overview of Ethereum 2.0 in its article Ultra Scalable Ethereum, but I'll attempt to summarize below.

As discussed above, smart contract platforms perform three basic functions:

1. Execution: Run programs via smart contracts
2. Data: Store important data such as account balances
3. Security: Provide consensus protocols secure the network

Ethereum currently has a "monolithic" architecture, meaning that a single chain must perform all of these functions. As one can imagine, this can be unwieldy and slow.

Ethereum 2.0, on the other hand, aims to transition to a "modular" structure to divide the execution of these functions into three separate parts – the Beacon Chain, Shards and Rollups.

_____
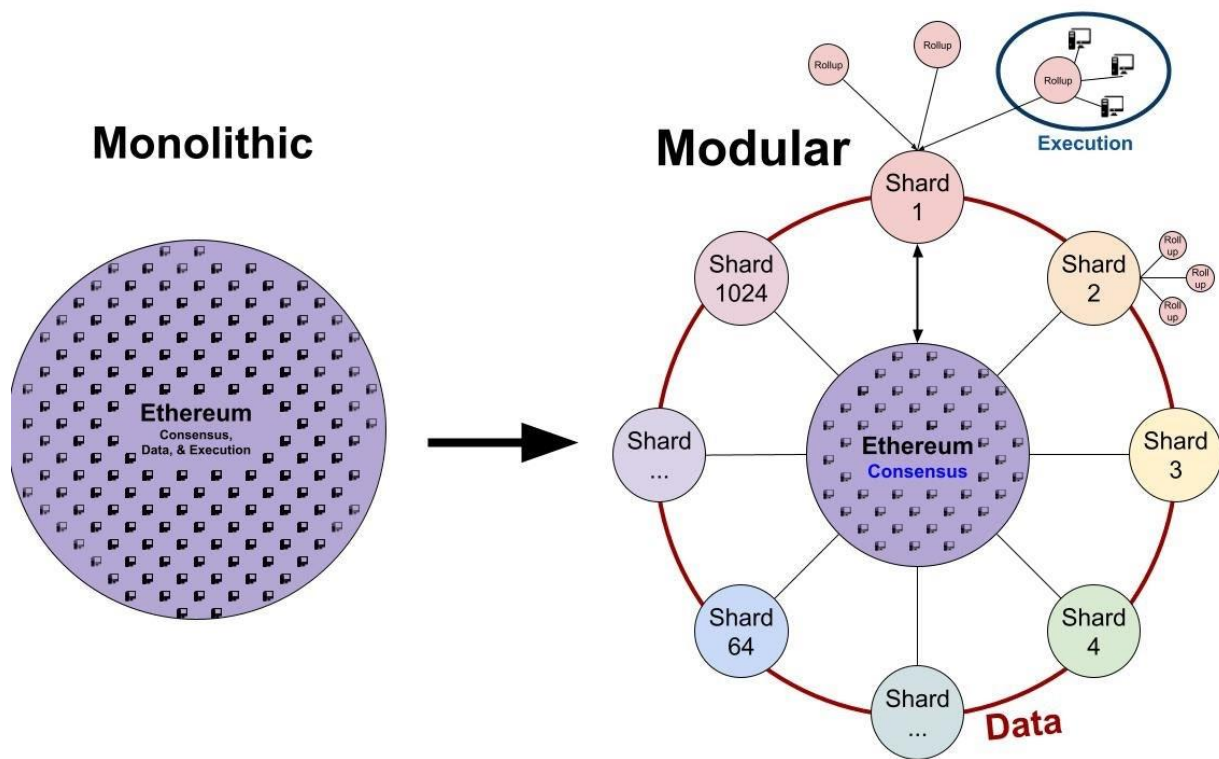
Source: Bankless

Rollups (Execution Layer)

Execution on ETH 2.0 will be handled by rollups – tools that move transactions off-chain, perform the necessary computations, and then plug the results back into the chain.

The most promising candidates for rollups are the two solutions we discussed above:

- Optimistic rollups
- Zero knowledge (zk) rollups

The Ethereum community is extremely bullish on rollups, and many believe that they will increase transaction speeds by up to 100x.

Shards (Data Layer)

Instead of living solely on the Ethereum Mainnet, ETH 2.0 plans to split its existing data layer into 64 smaller blockchains known as shards. This will make the entire network more efficient as:

- Each validator only has to store one shard of the network instead of the whole blockchain
- Shards can be processed in parallel

To combat the security risks faced by other multi-chain systems, ETH 2.0 plans to use random sampling to select validators.

Beacon Chain (Security Layer)

_____

_____

All shards will connect directly to the "Beacon Chain" – a Proof-of-Stake "master chain" that will maintain security and facilitate communication between the shards.

Unlike the Ethereum Mainnet of today, the Beacon Chain is only used for consensus and can't handle account data or execute smart contracts.

Potential Problems with ETH 2.0

While proponents believe that ETH 2.0 can achieve speeds in excess of 100K TPS without sacrificing decentralization or security, it's important to remember that the project is far from complete and, at this point, largely unproven.

Some of the biggest questions at this time are:

- Will it be composable? One benefit to Ethereum's current monochain structure is that it's "composable". In other words, it's very easy for dapps living on the same chain to communicate and "stack" together to create new products. For example, you could use an exchange dapp, lending dapp and insurance dapp all in the same transaction. As Ethereum moves to a modular model, critics worry that some or all of this composability will be lost.

- Will it be secure? Vitalik himself points out the multi-chain architectures may be less secure as it's easier for an attacker to expose a weak link. While Ethereum 2.0 hopes that its random validator selection process will avoid this, it's still unproven.

- Will it actually be faster? While Ethereum 2.0 will almost certainly be faster than its predecessor, it's not clear how much faster, as the dynamics of interchain communication are largely untested. Furthermore, the long wait times of proposed rollup solutions such as optimistic rollups may present a problem.

Should ETH 2.0 be successful, it would only deepen the moat of the smart contract platform that powers most (if not all) of crypto's "blue chip" dApps. Indeed, Ethereum ecosystem today accounts for over 60% of the total value locked in DeFi, over 75% of NFT sales and includes such notable projects as:

_____

The Ethereum dApp Ecosystem

Source: Coin98 Analytics

Indeed, despite losing some market share, **Ethereum is still the dominant smart contract platform**. It commands the largest position in DeFi and NFTs, the largest social communities, the most brand awareness, has the best security score, is the most decentralized and – perhaps ironically – is one of the most undervalued on a fully-diluted market cap to TVL ratio.

Should the migration to ETH 2.0 go as planned, it will almost certainly help solidify this position for years to come.

BNB Chain

#2 in Fully-Diluted Market Capitalization (as of 10.2.22)

BNB Chain ("BNB") is a standalone blockchain that was launched by Binance – the world's largest cryptocurrency exchange – in late 2020 to provide smart contract capability that was not available on the original system. It was originally named Binance Smart Chain.

The project leverages a monochain model that combines Delegated Proof-of-Stake with Proof-of-Authority to achieve consensus, achieving excepted speeds of up to 250 TPS with 3 second block times. BNB Chain uses the existing BNB token and is EVM-Compatible.

There are over 1,000 dApps in the BNB ecosystem including:

BNB Chain Ecosystem Overview

Source: Coin98 Analytics

BNB Chain has its share of supporters and detractors. Some of the more common praises and criticisms are listed below:

_____

Praise	Criticism
• **Binance-Backing:** As the largest exchange in the world, Binance has instant credibility. Furthermore, BNB Chain runs on the existing BNB token, making it very easy for users to onboard. • **Ecosystem:** The project has over 1,000 dApps and has consistently been the second or third largest player in both DeFi and the NFT market. • **Compatibility:** BSC is EVM-compatible and supports pegged tokens from several other chains.	• **Centralization:** BSC only has 21 validators and a Nakamoto Coefficient of 7. To make matters worse, critics argue that these validators are likely tied to Binance and therefore more likely to collude. • **Performance:** While an estimated maximum TPS of 250 and average fees of $0.24 are a significant improvement over Ethereum, they pale in comparison to newer third-generation blockchains.

Although BNB Chain spent most of the year as the undisputed #2 project to Ethereum, it has been steadily losing share to competitors and has recently fallen behind Tron in TVL. Perhaps even more worrisome, some critics argue that its centralization effectively disqualifies it from being classified as a true smart contract platform. Again, decentralization is the only attribute that makes blockchains disruptive, so a centralized chain is little more than an extremely inefficient copy of Visa.

_____

_____

Cardano

#3 in Fully-Diluted Market Capitalization (as of 10.2.22)

_____

Often called the first "third-generation" blockchain, Cardano was conceived in 2015 by Ethereum Co-Founder Charles Hoskinson and launched in 2017. After several years of development, smart contracts started to go live in late 2021.

Cardano achieves scalability through two main methods:

- Its "Ouroborous" Proof-of-Stake algorithm, which uses the random sampling of validators for consensus
- A two-layer approach, which splits the blockchain into a settlement layer that holds data and a computation layer that supports contract execution

Notable dApps in the Cardano ecosystem include:

Cardano Ecosystem Overview

Source: Coin98 Analytics

_____

_____

Although Cardano officially launched smart contracts in September of 2021, the project now [claims](#) to host over 200 dapps.

The protocol has its share of supporters and detractors. Some of the more common praises and criticisms are listed below:

Praise	Criticism
• **Founding Team**: The project was co-founded by Charles Hoskinson, one of the co-founders of Ethereum • **Academic Focus**: The Cardano team is heavily academic, relying on peer-reviewed research to build their product • **Developer Interest**: According to the Outlier Ventures Developer Report, Cardano consistently leads the pack in developer interest and activity	• **Slow Execution**: Cardano has been performing peer-reviewed research for almost six years now and it only recently released its first smart contracts. • **Poor Traction**: Cardano holds only 0.14% market share in DeFi and has no tangible presence in the NFT space • **Relatively Weak Performance**: While Cardano's technology may have been cutting edge when it was envisioned, its 250 TPS and $0.18 average transaction fee pale in comparison to some of the newer third-generation blockchains

While Cardano is very popular among developers (no doubt due to its academic focus), the lack of commercial traction is concerning. Silicon Valley is rife with stories of a superior technologies losing because they waited too long to go to market, and it's starting to seem like this could be the case for Cardano as well.

_____

Solana

#4 in Fully-Diluted Market Capitalization (as of 10.2.22)

Founded by former Qualcomm, Intel, and Dropbox engineers in late-2017, Solana is a single-chain, delegated-Proof-of-Stake protocol whose focus is on delivering scalability without sacrificing decentralization or security.

Core to Solana's scaling solution is a decentralized clock that uses a process known as Proof-of-History (PoH). Although this is vastly oversimplifying the concept, the thinking behind PoH goes like this:

> The concept of time is extremely important for computer networks, as it is necessary to track the passage of time accurately to put transactions in the correct order. For instance, if Alice, Bob and Charlie are all making transactions with one another, we need to know the order in which they occurred to route the funds correctly and ensure that Bob didn't send all his Ethereum to Alice and then try to send it again to Charlie.

> Centralized networks resolve this issue by maintaining a central clock and timestamping all transactions. Unfortunately, decentralized systems cannot rely on a centralized clock, and because we can't trust the actors, it's surprisingly difficult to agree on time (after all, Bob could create fake timestamps if he wanted to trick the network).

> Many argue that the most important benefit of traditional consensus mechanisms such as Proof-of-Work is that they act as a de facto "clock" for decentralized systems, relying on validators to arrange transactions in the correct order. Unfortunately, this wastes a lot of time, as validators and miners need to chat back and forth until they agree on the order of transactions.

> Solana's Proof-of-History function steals a page from the centralized playbook by allowing each validator to maintain their own clock and timestamp their transactions. To prevent the problems discussed above, the accuracy of this clock is verified through a cryptographic proof.

_____

This saves validators from wasting time on ordering transactions – they can simply check the timestamp, organize them and go.

This innovation allows Solana to be unbelievably fast and cheap, boasting a theoretical TPS of 65,000 to 710,000 and fees under $0.00019 without resorting to sharding.

Notable dApps in the Solana ecosystem include:

Solana Ecosystem Overview

Source: @solanians_ via Twitter

While growth and market share has recently declined, the project showed incredible transaction in 2021, growing from 70 to over 500 dapps and generating almost $12B in TVL. In addition, the

_____

market cap of NFTs sold on Solana's platforms was nearly $1 billion, and the project partnered with high profile personalities such as Michael Jordan and Snoop Dogg.

Like most smart contract platforms, Solana has its share of supporters and detractors. Some of the more common praises and criticisms are listed below:

Praise	Criticism
• **Unbelievably Fast and Cheap**: Solana is currently the fastest blockchain by almost an order of magnitude, possessing a stated TPS of 65,000 (with a theoretical limit of 710,000), sub one-second block times and an average fee of $0.00019 • **Robust Ecosystem**: Solana was one of the fastest growing projects of 2021. Although growth has slowed, it's still the undisputed #2 in the NFT market and generally ranks within the top 5 in DeFi • **Strong Team, Backers and Community**: The core technical team comes from Qualcomm, they're backed by A16Z and Polychain and they have over 150,000 community members on Reddit growing at 12% a month • **Developer Activity**: Solana ranks 2nd in terms of developer activity with over 2,500 developer actions a month	• **Monolithic Architecture** : Many - including the team at Bankless - argue that monochains such as Solana are inherently flawed and will always have to sacrifice decentralization for speed. Digging deeper, the evidence for this isn't concrete, but it's still likely a criticism that will plague the project for years to come (although as I note below, it's not clear whether this is a feature of a bug). • **Centralization:** Although Solana's Nakamoto Coefficient is relatively strong, it has the highest % of initial insider ownership of any major chain • **Security**: DeFi Safety ranks Solana as the worst chain in terms of security, and the network has experienced several major outages and its Wormhole bridge was hacked for $325 million

Solana is unique among the "Ethereum Killers" in that it has chosen to eschew sharding and retain its single-chain structure. While critics argue that so-called monochains are inferior and risk becoming irrelevant, **this might ultimately prove to be Solana's biggest long-term competitive advantage**. As discussed above, monochains allow for very efficient communication between dapps and may be able to support products and uses cases -- such as flash loans – that wouldn't be possible in a modular architecture.

_____

Avalanche

#5 in Fully-Diluted Market Capitalization (as of 10.2.22)

_____

Avalanche (AVAX) is a smart contract platform focused on transaction speed, low costs, and composability. It was launched in 2020 by Emin Gün Sirer, a computer science professor at Cornell University.

The protocol claims two unique innovations:

1. A novel consensus mechanism that purports to have the "best of both worlds", combining the speed and finality of Classical Consensus with the security and decentralization of Nakamoto Consensus.
2. Like ETH 2.0, it uses a modular – three blockchain architecture – that allows each chain to specialize in a task.

_____
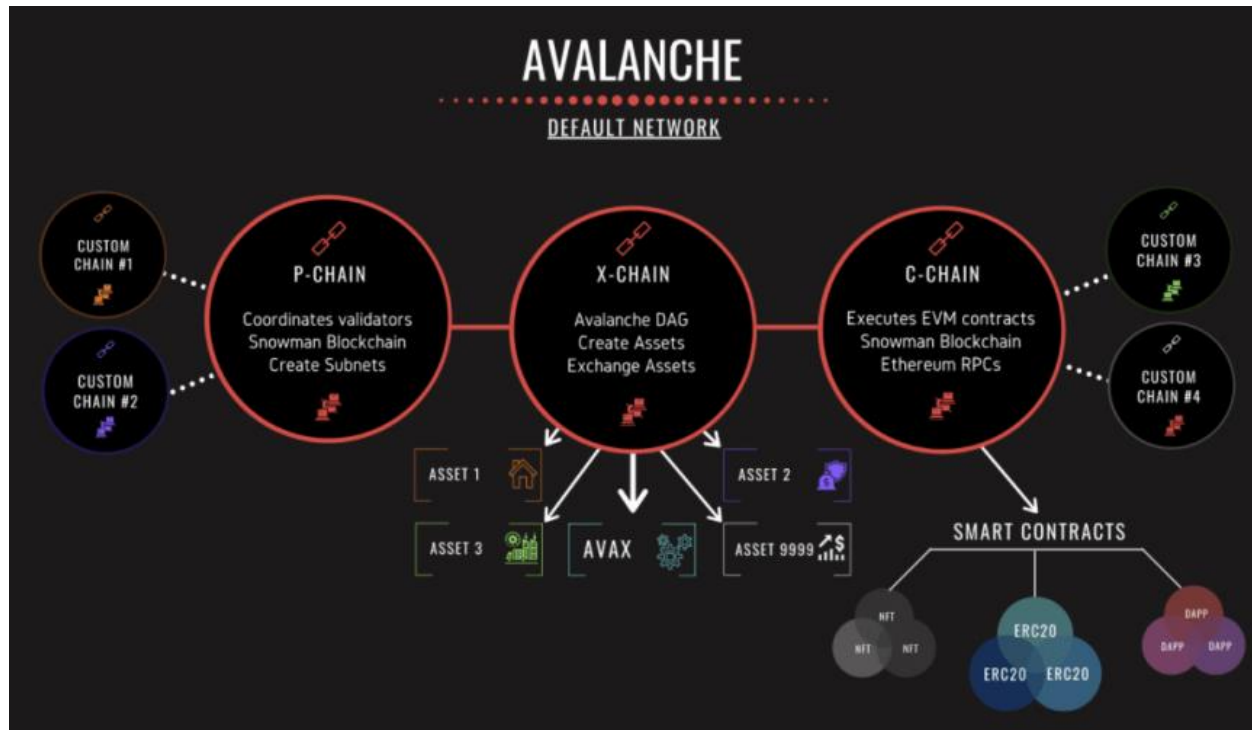
Source: NewsBTC

While Avalanche is fast (up to 4,500 TPS per chain and theoretically infinite with the addition of more subnets) and relatively cheap ($0.01 per transaction), its core focus has always been on "finality", which is the time it takes to finalize a transaction. The project claims it will be able to complete transactions in <1 second, making it much quicker than Bitcoin (60 minutes), Ethereum (6 minutes) and even rival Solana.

Notable dApps in the Avalanche ecosystem include:

_____

Avalanche Ecosystem Overview
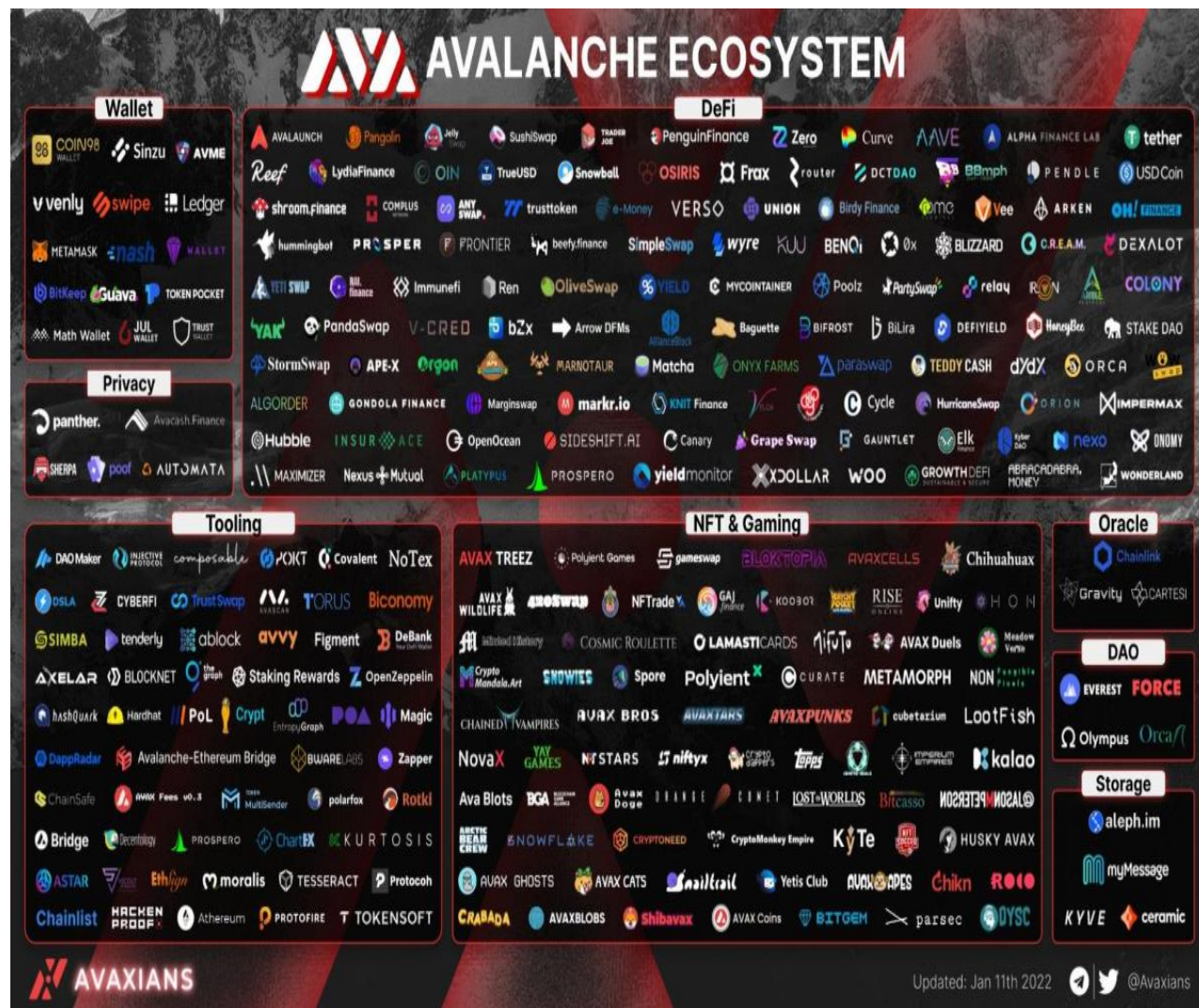
Source: Coin98 Analytics

What truly sets Avalanche apart, however, is its focus on DeFi and historical recent growth in that sphere. Although growth has declined, the protocol increased its TVL from $191 million at the start of Q32021 to $11 billion by the end of the year. That's over 50x growth in six months!

Avalanche is also highly compatible with Ethereum, making it relatively easy for developers to move their apps between the two chains.

Some of the more common praises and criticisms of Avalanche are listed below:

_____

Praise	Criticism
• **Great Architecture**: Avalanche's unique design gives it great performance - it's one of the fastest chains when measured by finality, it boasts a respectable TPS of 4,500, its fees are much lower than ETH and many believe it's one of the more secure chains • **Impressive Adoption**: Although growth has recently slowed, Avalanche was one of the fastest growing chains of 2022 and it still maintains a 3% share of the DeFi market. It's also interoperable - meaning existing Ethereum DAPPs can easily be ported over and used - and this bodes well for future adoption • **Strong Team and Backing**: Avalanche's founder, Emin Gün Sirer has a strong academic background in distributed systems research and the project is backed by Three Arrows, Dragonfly Capital, A16Z and Polychain	• **"The Worst of Both Worlds"**: Some critics argue that while the technology seems robust on the surface, that it's actually just making the same tradeoffs as any other Layer 1. In particular, some worry that it's not composable, that the security on the subnets is suboptimal and that's it's making the same centralization tradeoffs. One potential "canary in the coalmine" is that fact that AVAX fees spiked to $10 for a short time in November 2021 due to network congestion - replicating many of the same concerns it was intended to solve • **Poor UX**: While the three-chain system may be great for performance, some users claim that it makes the system extremely difficult to use as they constantly have to make transfers between the chains • **Is interoperability a Feature or a Bug?** The fact that Avax is interoperable - meaning existing Ethereum DAPPs can easily be ported over and used - has been a key driven of its unparalleled growth. But could this work in reverse? If developers tire of the network, can't they switch back to the EVM just as quickly?

At first blush, Avalanche seems like a strong project – solid performance, extreme growth and a loyal community. That said, I'm having trouble identifying the "moat" – I get that it's clearly a sustaining innovation (i.e. potentially a better version of ETH) but I can't see what's disruptive about it (i.e. what ETH 2.0 can't replicate).

Furthermore, given that Avalanche gave out over $180 million in developer incentives in the second half of 2021, it's difficult to tell how much of their growth is organic and how much is "bought-and-paid-for" (always a risk because developers tend to leave when the money dries up).

Polygon

#6 in Fully-Diluted Market Capitalization (as of 10.2.22)
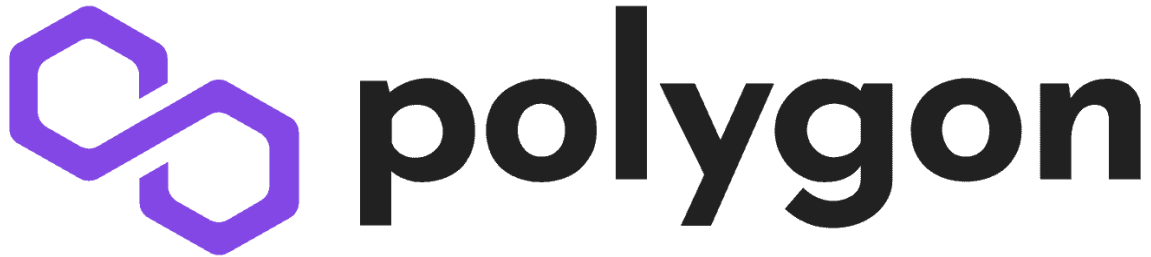
Polygon was founded by Sandeep Nailwal and Anurag Arjun in October 2017. The project's original name was Matic, and it initially provided two Layer 2 scaling solutions to Ethereum – its PoS custodial chain and Plasma chain.

Since launch, however, Polygon has significantly expanded its vision, and now hopes to be Ethereum's "internet of blockchains", allowing developers to build their own sidechains, rollups and plasma chains and connect them to the Ethereum blockchain. As such, it is currently building:

- A "library" of Layer-2 solutions such as standalone sidechains, plasma chains, zk-rollups and optimistic rollups that projects can use to scale
- A software development kit to help developers create their own chains
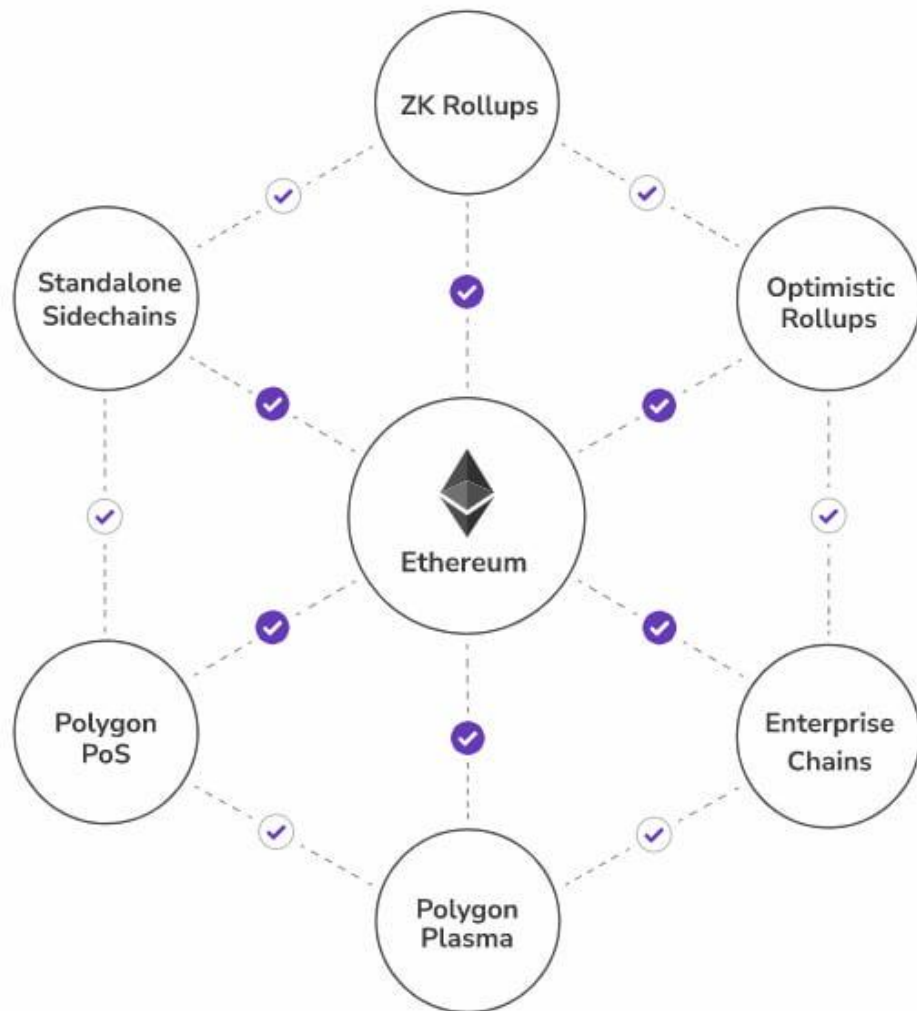
Source: Komodoplatform.com

To further their mission, Polygon has made a host of acquisitions in 2021 including zK-rollup providers Miden, Hermez and Mir.

Notable dApps in the Polygon ecosystem include:

Polygon Ecosystem Overview
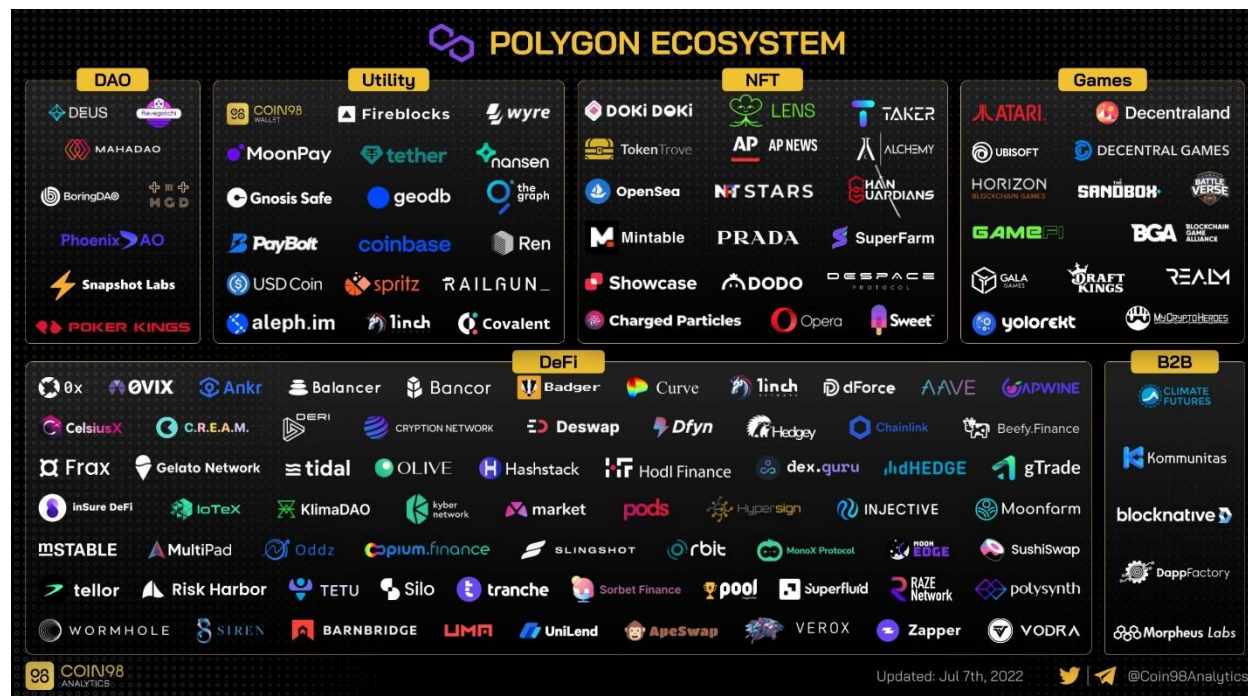
Source: Coin98Analytics

Polygon has achieved significant traction in the last year. According to Coindesk, it hosted almost 3,000 dapps at the end of 2021 – a 100x increase from the prior year – and 62% of these were deployed exclusively on the network. It also executes nearly ~3x as many transactions as Ethereum (although at significantly less revenue per transaction).

Some of the more common praises and criticisms of the Polygon network are listed below:

Praise	Criticism
• **L2 Focus**: Polygon's focus on becoming a "Swiss Army Knife" of L2 solutions may be very valuable as the Ethereum continues to struggle with scalability • **Solid Technicals**: With an estimated maximum TPS of 7,200, an average block time of 2 seconds and fees less than a fraction of a cent, Polygon is a solid technical platform • **Pure Growth**: Polygon was one of the fastest growing projects of 2021 and unlike competitors Avalanche and Solana, it did not rely as heavily on incentive programs (suggesting that much of its growth is due to true demand)	• **No Breakthrough:** Despite growing substantially in 2021, Polygon has yet to truly break through, and is still relatively "middle of the pack" in both the DeFi and NFT markets • **Security:** Polygon scores quite low on DeFi Safety's Chain Score, mostly due to a significant outage that shut down the network for 8 hours in March of 2022

As it becomes clear that L2 solutions will play a significant role in improving the scalability of smart contract platforms, Polygon is well positioned to be a market leader. Furthermore, the project has demonstrated "hustle", in both its successful courting of developers and aggressive acquisition schedule.

Critics would argue that one of the biggest concerns around the future of the project has to do with the utility of its token. As we will see below, many rollups (such as Arbitrum and Optimism) function perfectly fine without one, so that begs the question – as Polygon becomes a network of Layer 2s, is its token really necessary?

Polkadot

#7 in Fully-Diluted Market Capitalization (as of 10.2.22)

Polkadot was created by Ethereum co-founder Gavin Wood in 2016. The project is unique in that it is taking a different approach than many of its competitors – instead of primarily focusing on speed like many of the other "Ethereum Killers", the project is betting on interoperability.

One of the key problems with the crypto landscape today is that smart contract platforms generally have little to no ability to communicate with one another. Polkadot's goal is to connect all of them, creating an "internet of interoperable blockchains."

To do this, it utilizes a "hub and spoke" structure, where different Layer 1 blockchains (called "parachains") can share data via Polkadot's central chain, known as the "Relay Chain".

_____
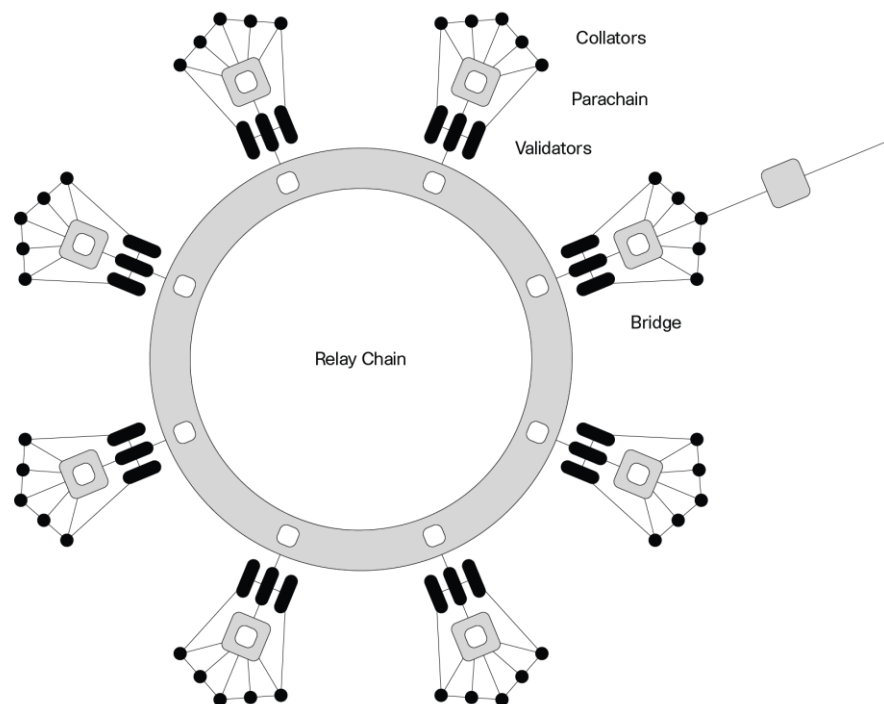
As you've probably noticed, this structure is similar in many ways to Ethereum 2.0's beacon chain and shard architecture. The key difference is that while all chains in Ethereum 2.0 are subchains of Ethereum, Polkadot's parachains are all independent Layer 1s. In Polkadot's ideal world, this could even mean that Ethereum, Cardano, Avalanche, Solana, BSC, etc… all connect to and communicate through the DOT network. For this reason, the project often calls itself a "Layer 0" protocol.

Notable dApps in the Polkadot Ecosystem include:

<u>Polkdadot Ecosystem Overview</u>

_____
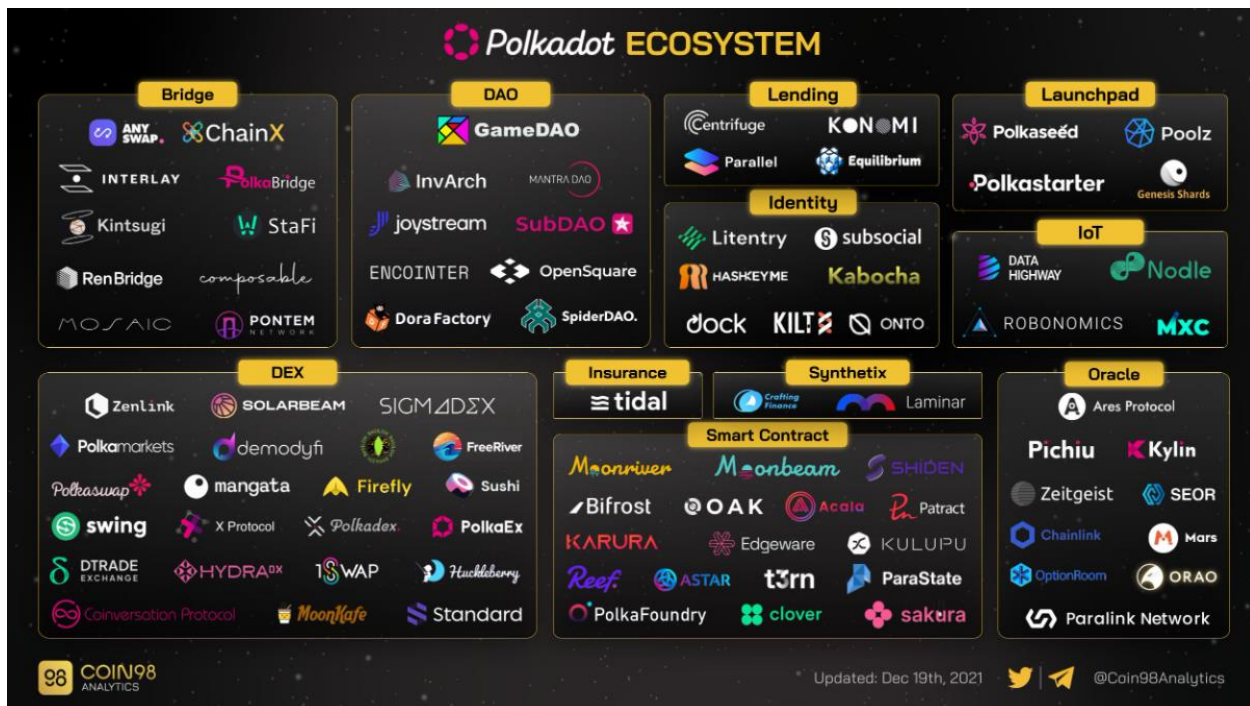
Source: Coin98 Analytics

Like Cardano, Polkadot got off to a slow start, preferring to focus on internal research and development before launching.   That said, the project went live in December, and it is already showing 150 dapps on its website.

Polkadot has its share of critics and fans. Some of the more common praises and criticisms of the protocol are listed below:

Praise	Criticism
• **Respectable Performance**: Polkadot's Relay Chain supports up to 3,000 TPS, and the addition of parachains could boost the system to 100,000 TPS • **"Layer 0" Approach**: Instead of competing directly with the likes of Ethereum, Cardano, Avalanche, etc… Polkadot has tried to carve a niche out by serving as an interoperability solution • **Strong Founder**: Polkadot's founder, Gavin Wood, was one of the co-creators of Ethereum and one of the authors of its Solidarity programming language	• **Slow Executions**: Despite being launched in 2016, Polkadot is only recently went live, with the first of its parachain auctions starting in December • **Poor Traction**: Polkadot's market share in DeFi is less than 1% • **What's the Differentiator?** Polkadot's parachain structure is very similar to ETH 2.0 shards, and given that many projects are already bridging to ETH, one could wonder what value DOT is really adding

It's not clear to me that Polkadot is vastly superior or differentiated to ETH 2.0, and without any real traction, it's tough to make a solid argument otherwise.

_____

Tron

#8 in Fully-Diluted Market Capitalization (as of 10.2.22)

_____

Tron was founded in 2017 by billionaire Justin Sun, a controversial figure in the crypto space that nevertheless has a penchant for marketing and a history of entrepreneurship (he previously founded Peiwo, a live chat app in China with over 10 million registered users and was one of the early representatives of Ripple in China).

The blockchain uses a modified form of the Proof-of-Stake consensus mechanism (PoS) known as Delegated Proof-of-Stake (DPoS). Unlike traditional PoS systems, which randomly select a new set of validators for each and every block, members of DPoS-based systems vote to elect a limited number of "representatives" (called delegates) that are responsible for validating all blocks over a given time period.

In Tron's case, the network elects 27 "super representatives" to serve for a period of six hours (after which voting begins anew).

Proponents of DPoS networks such as Tron argue that limiting the number of validators make the chains more efficient, faster and cheaper. There appears to be some merit to this claim as Tron is theoretically able to achieve a TPS of up to 2,000 and fees that range from zero to a fraction of a cent.

Notable dApps in the Tron ecosystem include:

_____

Tron Ecosystem Overview
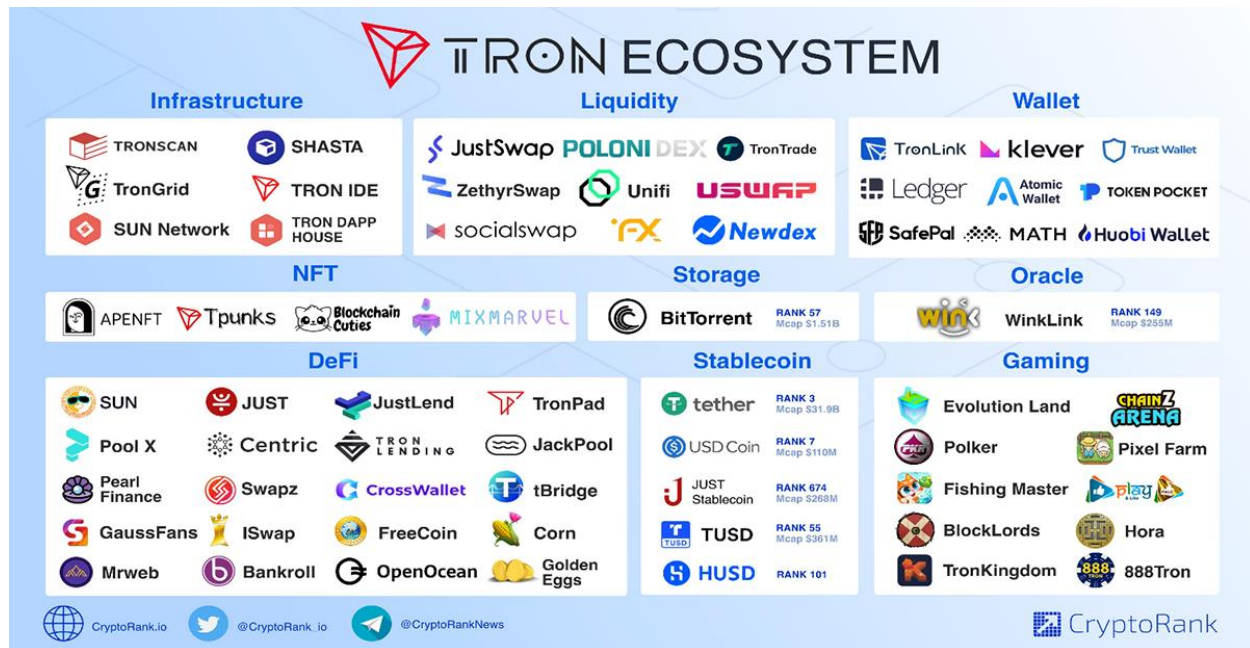
Source: CryptoRank

While the project is often heavily criticized, it has demonstrated remarkable staying power. As one of the oldest smart contract platforms, Tron maintains a loyal cadre of fans and has recently elevated to the number two position in DeFi, increasing its market share in TVL from 3% in February to almost 10% today.

Some of the more common praises and criticisms of Tron are listed below:

Praise	Criticism
• **Strong Adoption**: Tron has been around a very long time and, despite having numerous critics and detractors, it just doesn't seem to go away (as evidenced by the fact that it recently gained the #2 spot in DeFi). • **Loyal Fan Base:** Tron has built a substantial community of 125K Reddit subscribers and 1.4M Twitter followers, and its fans seem to really love the project • **Near Zero Fees:** Tron has extremely low fees, which often range between zero and fractions of a cent • **High Usage:** Tron ranks #2 in daily transaction volume with an average of 5.3K • **Good Valuation:** Although critics would offer that the metric has numerous flaws, Tron currently boasts the lowest Market Cap to TVL ratio	• **Controversial Founder**:: Sun has a colorful history – although he has received multiple accolades, he is considered brash and outspoken and is constantly in the news. Some of his most recent headlines include paying almost $5 million for a lunch with Warren Buffett, becoming a diplomat to Grenada and being forced to apologize to the Chinese government for "vulgar hype and marketing behavior" • **"Scammy":** Many find Tron's aggressive marketing style off-putting and claim the project is "overhyped" • **Centralized**: Tron has a relatively low Nakamoto Coefficient and many argue that delegated proof of stake systems are inherently centralized

Tron is a very peculiar project. A lot of people in the crypto space *really* hate the protocol, claiming that both the software and the white paper were plagiarized and that the project is essentially vaporware.

Much of this may be related to Sun himself, who is a very polarizing figure with an aggressive marketing style and a personality that some find off-putting (e.g. many poke fun at the fact that his Twitter handle is now "H.E. Justin Sun" – for "His Excellency" – given his position as an Ambassador to Grenada).

That said, he's also a notoriously entrepreneurial individual, is rumored to have an unbelievable work ethic and his marketing style has undoubtedly brought a lot of publicity to Tron.

Whatever one's thoughts are on Sun, however, it is undeniable that the project has achieved significant traction across a variety of metrics – it is one of the cheapest chains, ranks #3 in achieved TPS, ranks #2 in the number of daily average transactions and, perhaps most importantly, is now the second largest player in DeFi with nearly 10% market share.

Cosmos

#9 in Fully-Diluted Market Capitalization (as of 10.2.22)

Cosmos was conceived in 2014 and launched in 2019 by founders Jae Kwon and Ethan Buchman.

Like Polkadot, the project is aspiring to be a "Layer 0" protocol that can connect multiple, independent smart contract platforms. In fact, while some call Polkadot the "blockchain of blockchains", Cosmos is often referred to as an "Internet of blockchains".

From a technical level, both projects use a "hub and spoke" model that connects several Layer 1 smart contract platforms (spokes) to a central chain (hub) that is responsible for security and validation.

_____

Cosmos Uses a "Hub and Spoke" Model to Connect Multiple Blockchains
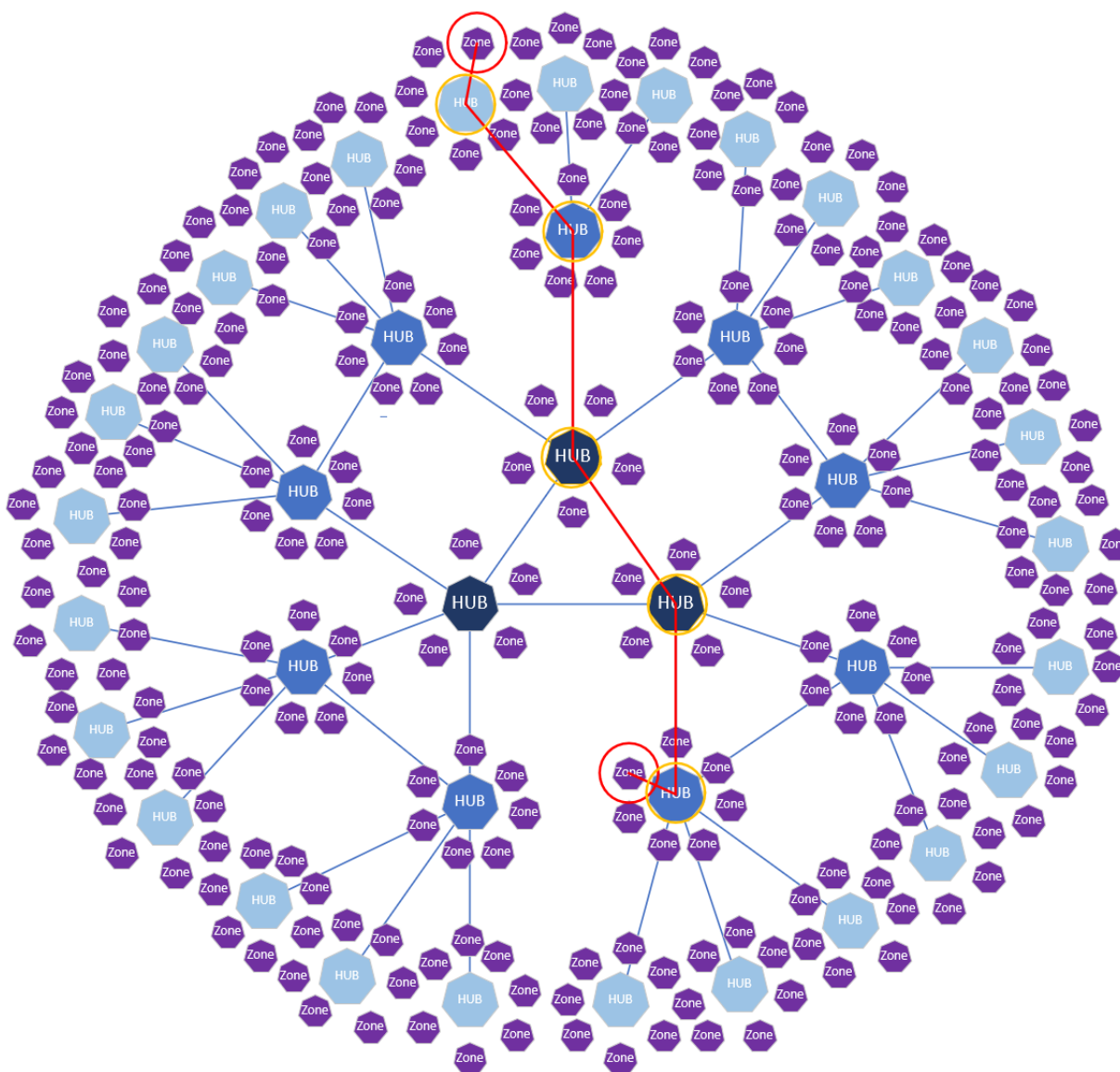
Source: Seq via Medium

That said, there are a few key differences between Cosmos and Polkadot:

1. **Faster Finality:** Cosmos created its own spin on Proof-of-Stake validation through its Tendermint BFT (Byzantine Fault Tolerance) mechanism. This innovation allows the protocol to reach consensus – and therefore execute transactions – faster. Tendermint is also used by several other Layer 1 blockchains including BNB Chain.

2. **Multiple Hubs:** As discussed, both Polkadot and Cosmos employ a "hub and spoke" model. The key difference between the two, however, is that Polkadot only has one hub, while

_____

Cosmos will have multiple hubs that can all communicate with each other through a protocol known as the Inter-Blockchain Communication Protocol (IBC).

3. **Strong Developer Tools**: Cosmos has created a proprietary software development kit (SDK) that allows developers to create highly customizable blockchains. One of the most attractive features of the SDK is that it can translate several popular programming languages, such as Java and C++, into a format that is readable by the Cosmos network.

These three innovations combine to give Cosmos a high TPS (it is estimated to approach 10,000 transactions per second), fast time to finality, low fees and – most importantly – high interoperability.

Notable dApps in the Cosmos ecosystem include:

<u>Cosmos Ecosystem Overview</u>
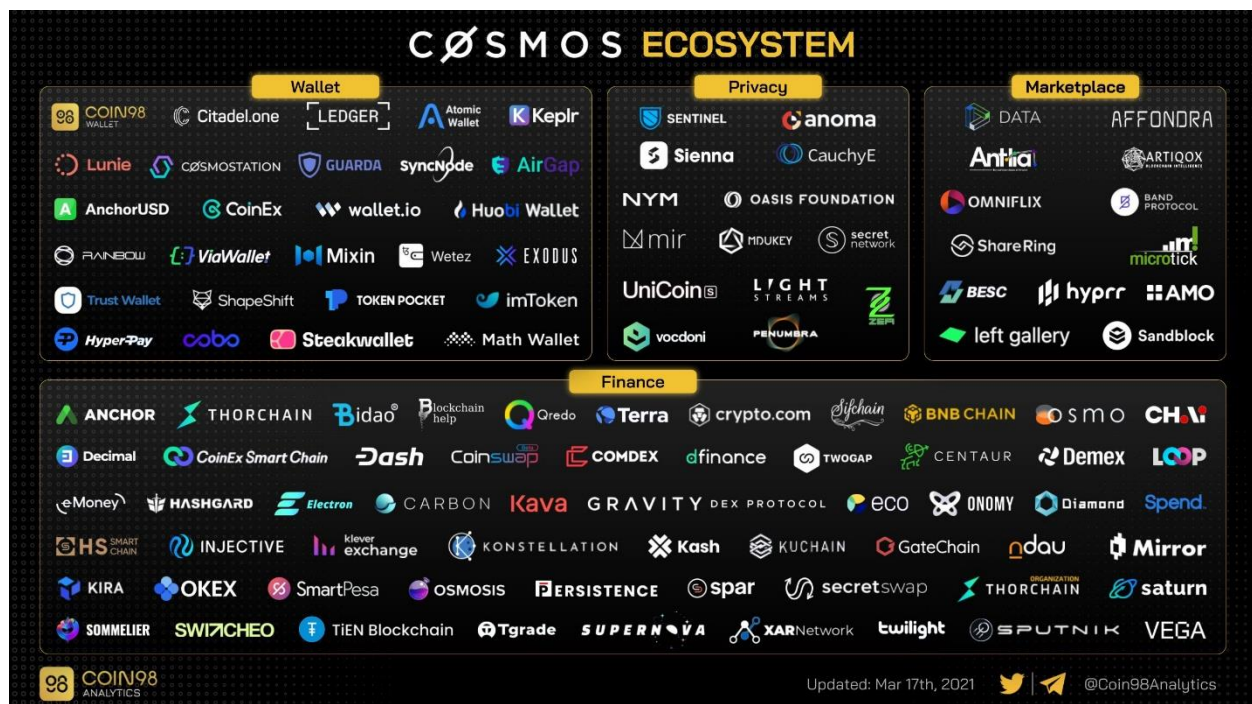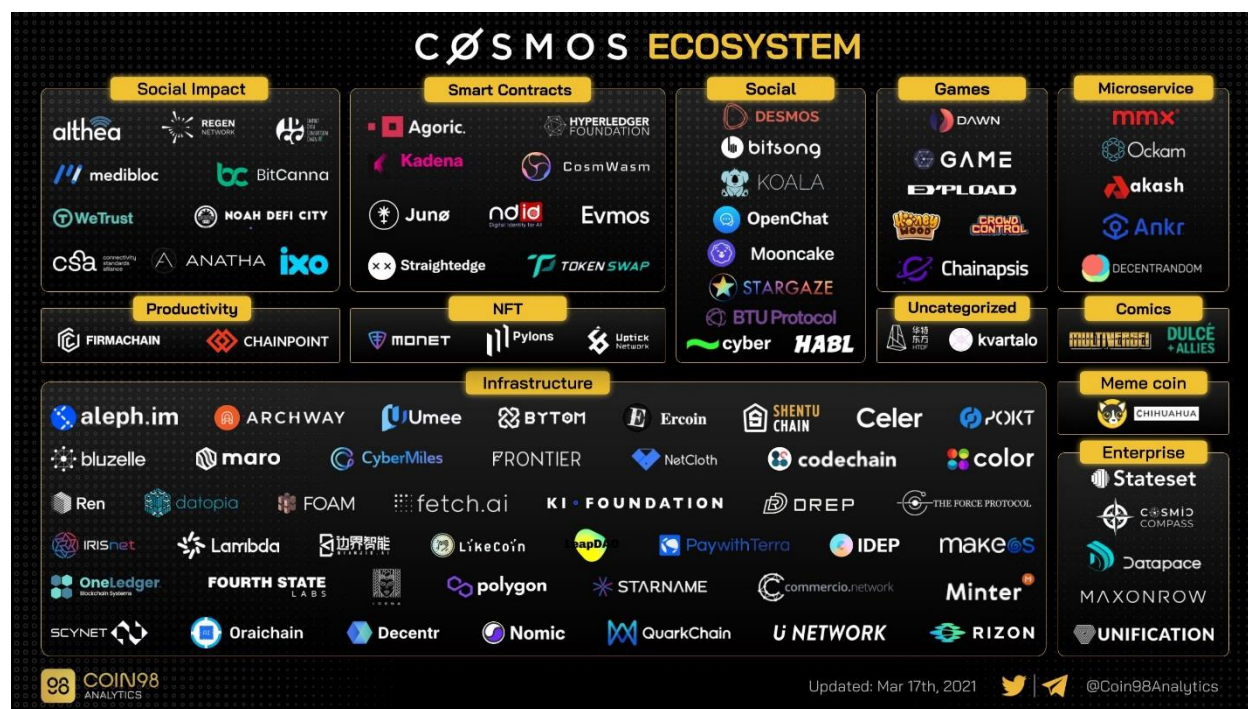
Source: Coin98 Analytics

Although the total TVL of chains connected to Cosmos is relatively small today (~1% of the total market), earlier this year it commanded over 15% market share, as Cosmos was the "Layer 0" base chain for Terra (an algorithmic stablecoin that infamously imploded in May, destroying over $40 billion).

Given that the protocol functions as a technology layer for *independent* blockchains, Cosmos obviously can't be blamed for this collapse, and if anything, the fact that Terra used it to become the #2 chain speaks highly to the technology.

Like most protocols, Cosmos has its share of fans and detractors. Some of their most common arguments are below:

Praise	Criticism
• **Interoperability**: Cosmos's strongest attribute is undoubtedly its interoperable nature – if the "internet of blockchains" thesis takes off, it could represent a paradigm shift in the space • **Strong Ecosystem**: While its share has recently fallen, at one point projects running on Cosmos commanded a substantial share of the DeFi market (most notably Terra and Thorchain) • **Respectable Performance**: The platform has solid technicals, with an estimated 10,000 TPS and average fees of $0.01	• **Centralization**: Critics argue that the use of Tendermint, which can only function with a smaller number of nodes, makes Cosmos inherently more centralized. • **Declining Market Share**: With the loss of Terra and the decline of Thorchain, Cosmos's share of the DeFi market has dropped to 1%

Cosmos is a project to keep an eye on. As we potentially move to a multichain world, interoperability remains one of the greatest unsolved problems.

Unfortunately, the most popular solution today — cross-chain bridges – have proven troublesome. Today's bridges are relatively easy to hack (over $2B has been stolen in 2022 alone) and some question whether a secure bridge is even possible from a technical perspective.

Cosmos's IBC represents a novel way to solve this problem, eliminating many of the problems with traditional bridges. Should the protocol achieve success as the preferred interoperability solution, its potential is nearly limitless.

_____

NEAR Protocol

#10 in Fully-Diluted Market Capitalization (as of 10.2.22)

_____

NEAR Protocol was founded in 2018 by Alexander Skidanov and Illia Polosukhin. It is backed by Notation Capital, Coinbase Ventures, Multicoin Capital, Pantera, A16z and was a participant in Y-Combinator's accelerator.

The project incorporates a number of features to enhance scalability, boost speed and reduce costs, including:

1. **DPoS**: NEAR uses a delegated Proof-of-Stake consensus model to reduce the time to validate a block
2. **Immediate Consensus Mechanism**: Unlike most smart contract platforms, which require multiple confirmations to reach consensus, NEAR has pioneered a novel system called DoomSlug which allows the system to finalize a block after one round of communication
3. **Sharding**: NEAR was one of the early pioneers of sharding with its Nightshade protocol

These innovations allow the protocol to theoretically process over 100,000 transactions per second with near instant finality (and fees that are a fraction of a cent).

Notable dApps in the NEAR ecosystem include:

_____

NEAR Ecosystem Overview

Source: Coin98 Analytics

While still relatively small, the project has been growing steadily since launch, increasing its share of TVL from 0.07% in February 2022 to 0.5% in October.

Some of the more common praises and criticisms of NEAR are listed below:

Praise	Criticism
• **Amazing Tech**: From a purely technical perspective, NEAR seems to be head and shoulders above the pack. The team claims that it can achieve 100,000 transactions per second, near instant finality and transaction fees that are effectively zero • **Strong Team and Backers**: NEAR has a strong team and is backed by a slate of very prominent investors • **Growth**: Although it's off a relatively small base, NEAR has been the fastest growing Layer 1 in terms of monthly address growth and community growth and has seen the third largest increase in share in the DeFi space	• **No Critical Mass**: NEAR's market share in DeFi is still relatively small at under 1% • **Unproven Technology**: While NEAR makes some bold claims, the protocol's highest recorded TPS to date is only 23 (although this is almost certainly because it hasn't had the real-world demand to sufficiently test)

While NEAR has a strong team, very interesting technology and good traction to date, it has yet to achieve critical mass as its TVL market share remains below 1%. As I'm a firm believer that the market is the ultimate judge of a project's usefulness, I'd be hesitant to be too bullish until it starts to cross a tipping point.

Chapter 20: What's Next? The Multi-Chain World

Many argue that a "multi-chain" world is all but inevitable at this point. Due to its high gas fees, Ethereum's market share has steadily decreased since 2020.

Ethereum's Market Share Has Declined From > 95% to ~ 60% over the Last Two Years
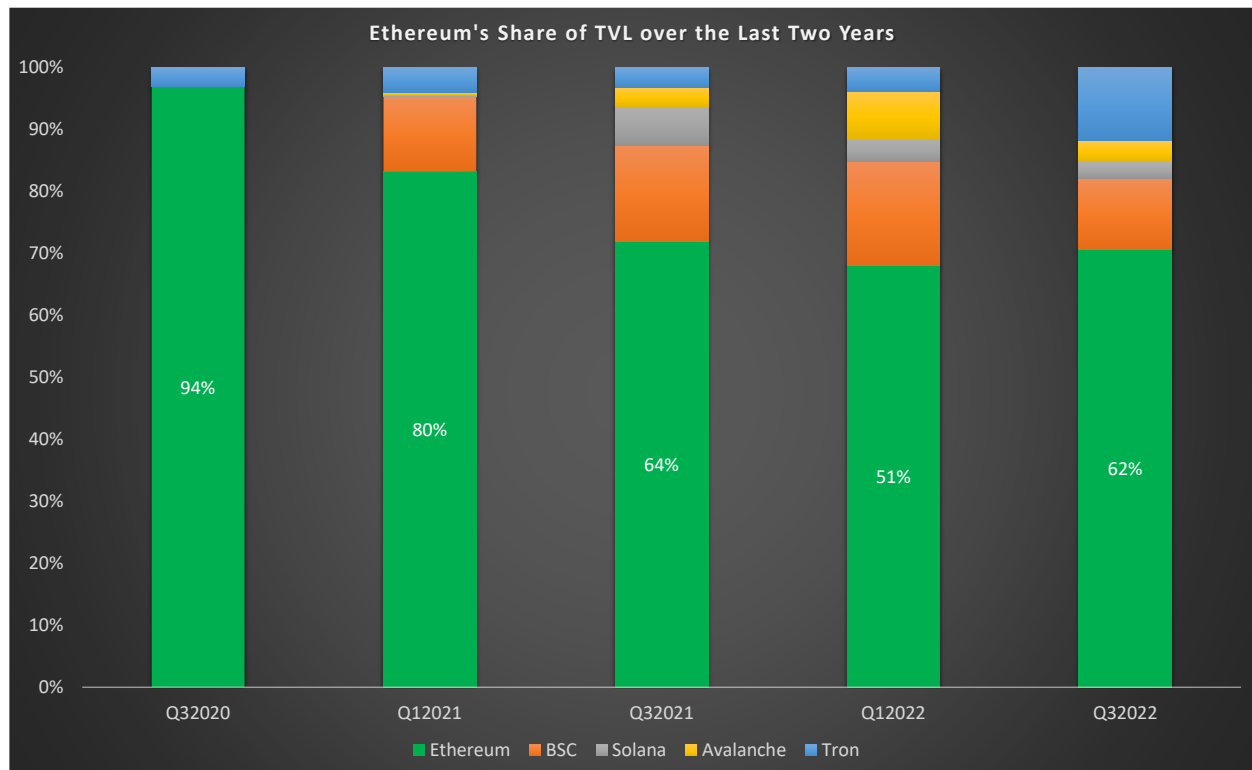
Source: DeFi Llama as of 10.2.22

While "maxis" will claim that this is temporary – that ETH 2.0 is the panacea that will bring everyone back and return the project to 90%+ market share – there are three reasons to be skeptical of this scenario:

1. Platform economies trend towards multiple players
2. Ever increasing demand will drive a constant stream of new entrants
3. The need for specialization will carve out an opportunity for niche players

Platform Economies Trend Towards Multiple Players

The "winner-take-all" phenomenon is one of tech's greatest myths. It's a forgivable mistake – after all, if you define Google and Facebook's markets as search and social media, then they are definitely monopolies. But once you realize those are simply distribution channels, and that their *real* market is digital ad spend, it's clear that's not the case.

There are No True Monopolies in Tech

% OF TOTAL DIGITAL AD SPEND
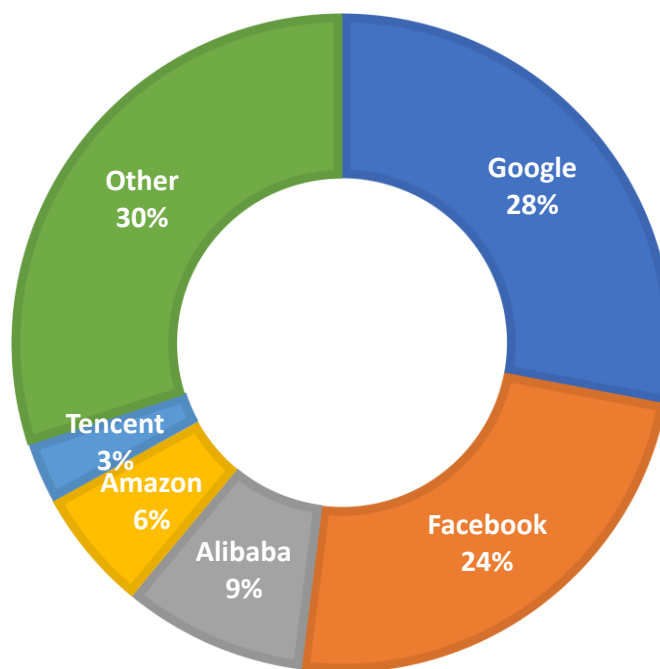
Source: eMarketer.com

Indeed, virtually every platform economy has been dominated by two or more incumbents.

Some technology markets, such as PC and mobile operating systems, browsers, PC chipsets and graphics cards, evolved into duopolies.

MESSARI
Technology platforms trend towards duopolies

Domain	Before	After
PC operating Systems	Windows, Mac, OS2, BeOS..	Windows	Mac
Mobile operating systems	Symbian, Blackberry, Android, iOS, Palm OS, Tizen..	Android	iOS
Browsers	Netscape Navigator, Internet Explorer, Chrome, Firefox, Opera...	Chrome	Firefox
PC Chipsets	Intel, AMD, Quallcom, TI, Broadcom	Intel	AMD
Graphics Cards	Nvidia, AMD, Asus, Intel	Nvidia	AMD

Data as of: September 27th, 2021
Source: Messari

Source: Messari

Other markets saw the emergence of three or four dominant players. For example, the cloud computing network is dominated by Amazon AWS, Microsoft Azure and Google, and the credit card processing landscape is dominated by Visa, Mastercard, American Express and Discover.

SHARE OF CREDIT CARD MARKET

Source: Wallethub

_____
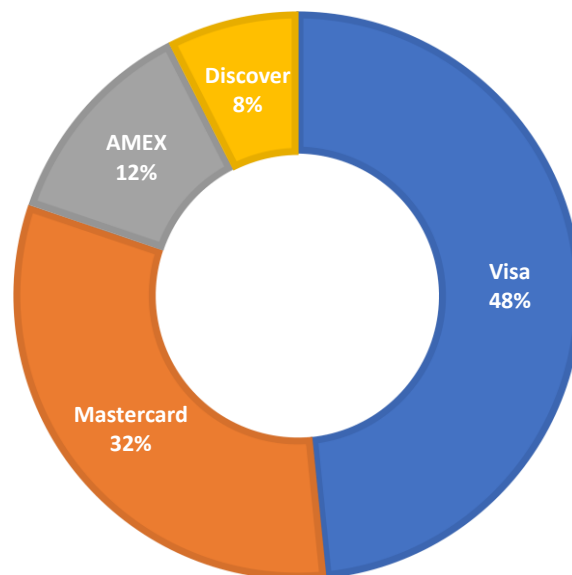
While we can debate whether there will be two, four or ten major players in the smart contract market, one thing is all but certain – platform economies have historically not been "winner take all".

Ever increasing demand will drive a constant stream of new entrants
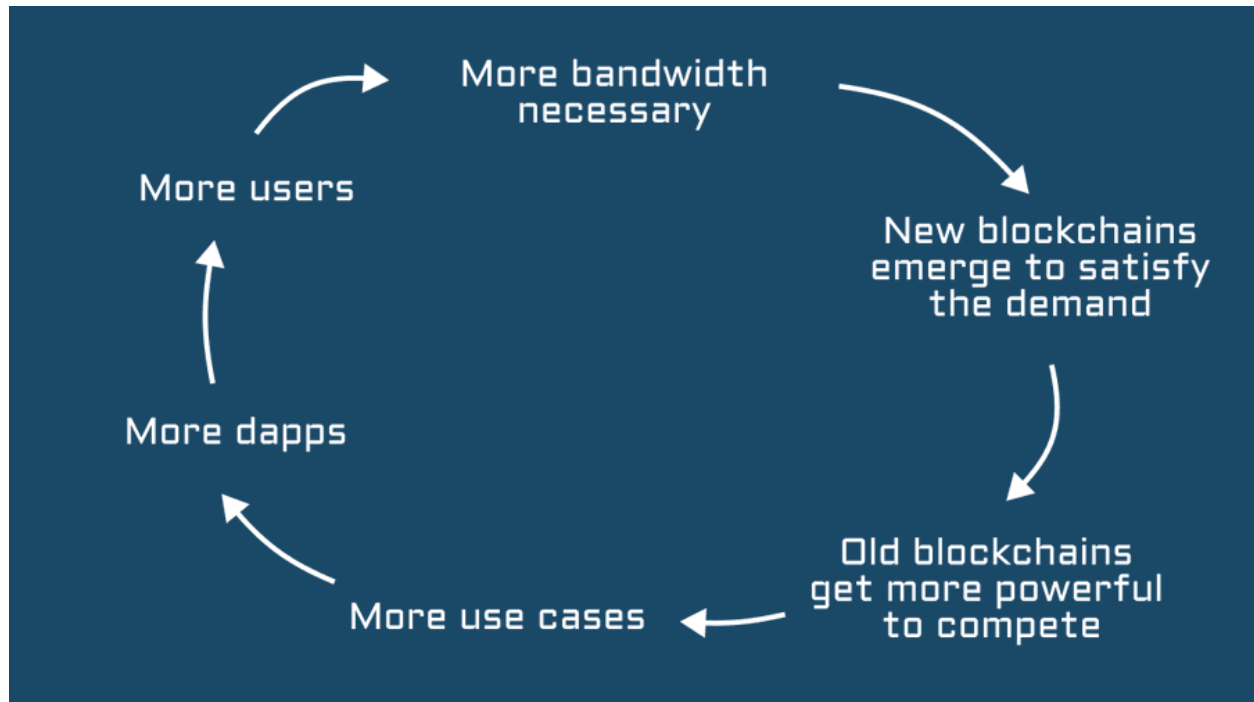
Source: Twitter

Chris Dixon of A16Z argues that the demand for every important computing resource has always outpaced its supply and that this generates a mutually reinforcing feedback loop.

In essence, as demand increases:

1. New blockchains emerge to satisfy the demand
2. Old blockchains are forced to upgrade to compete
3. This generates more functionality and uses cases
4. Which in turn generate more applications
5. Generating more users
6. Who generate even more demand
7. …and start the loop again

We've seen this dynamic play out across multiple industries including CPUs, GPUs, memory, storage, mobile, gaming, etc… and it will likely play out in the crypto space as well, with a constant introduction of new technologies and blockchains.

_____

_____

The need for specialization will carve out an opportunity for niche players

We've discussed the scalability trilemma previously, and to the extent that that isn't fully resolved, it's easy to imagine consumers making tradeoffs between decentralization, security and speed. For instance, it's plausible to imagine a world where financial transactions happen on blockchains that prioritize decentralization and security, while gaming transactions occur on chains that value speed.

Furthermore, even when it comes to performance, there are nuances. In particular, there are two measures of "speed" and efficiency:

- Transactions per second (TPS) refers to the volume of transactions that the network can process and it is strongly correlated with fees
- Finality refers to the time it takes to actually finish a transaction

For some use cases, high TPS and low fees might be ideal, while others might prefer faster finality times.

Finally, as discussed above, different structures (e.g. monochain vs. multichain vs. modular) may have different consequences and tradeoffs themselves. So even if ETH 2.0 eventually offers the best performance, its modular structure may have some composability drawbacks, leaving monochains such as Solana the ideal choice for those that want to maximize interoperability and utilize features such as flash loans.

_____

Part 4: Non-Fungible Tokens

_____
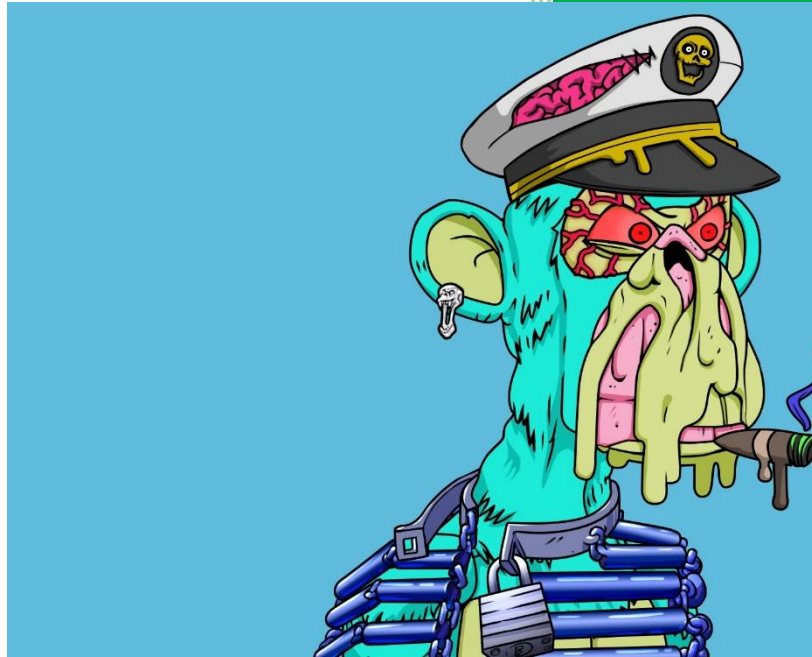
Chapter 21: What are NFTs?

An NFT – or "non-fungible token"– is a certificate of ownership for a digital or physical good that is recorded onto a blockchain.

Almost any asset can be represented by an NFT: a piece of art, a photograph, a song, a concert ticket, a passport or the deed to your house.
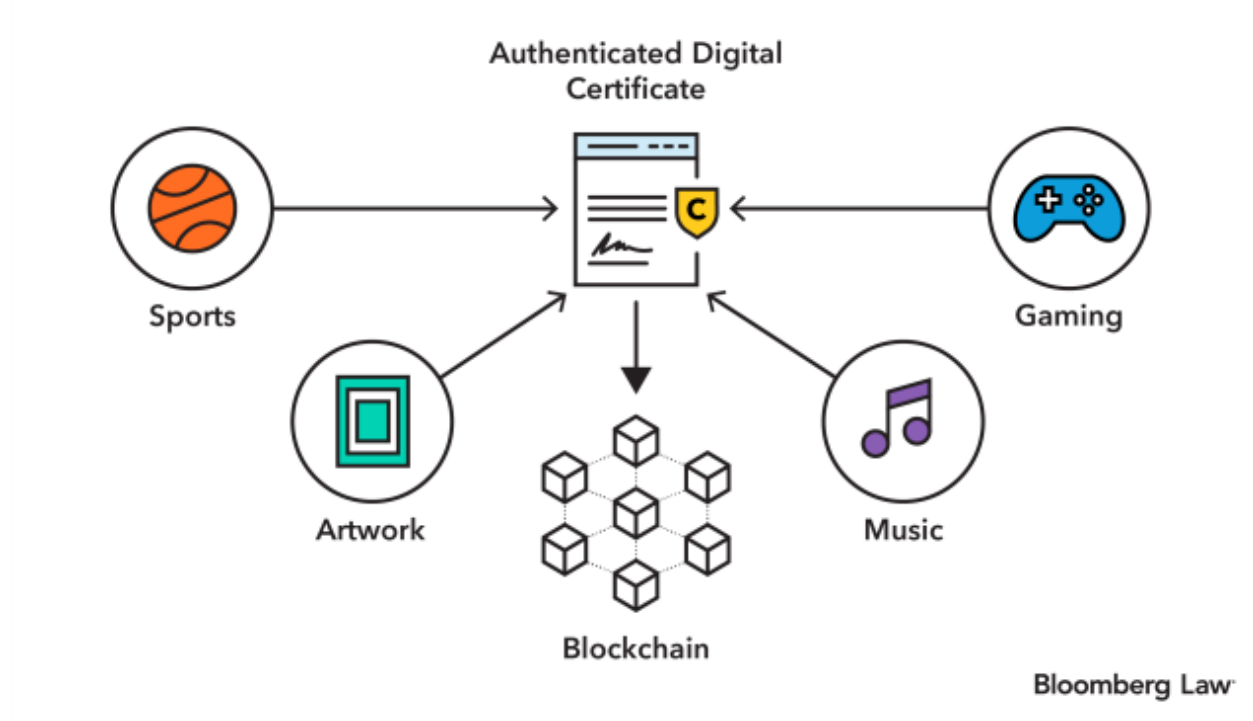
Source: Bloomberg Law

Each and every NFT is unique – in fact, the term "non-fungible" is just a fancy way of saying "unique" – and has three important properties:

- **Proof of Authenticity:** NFTs use cryptography to prove their authenticity. As such, they cannot be counterfeited and it is relatively simple to spot a fake NFT

- **Record of Ownership**: They maintain a record of ownership on a blockchain, which cannot be altered, destroyed, removed or confiscated

_____

- **Inalienable Rights:** Owners can often do anything they want with their NFT – they can sell it, rent it, license it and / or create derivatives works

The market for NFTs exploded in 2021, growing from $64.5 million on January 1st, 2021 to a $38.6 billion peak in January 2022 (nearly 600x growth) and registering multiple eight-figure sales.

Even today, during what many are calling a bear market, the space boasts a total market capitalization of $21.6 billion (almost 400x growth from 2021).

The NFT Market has grown nearly 400x since 2021
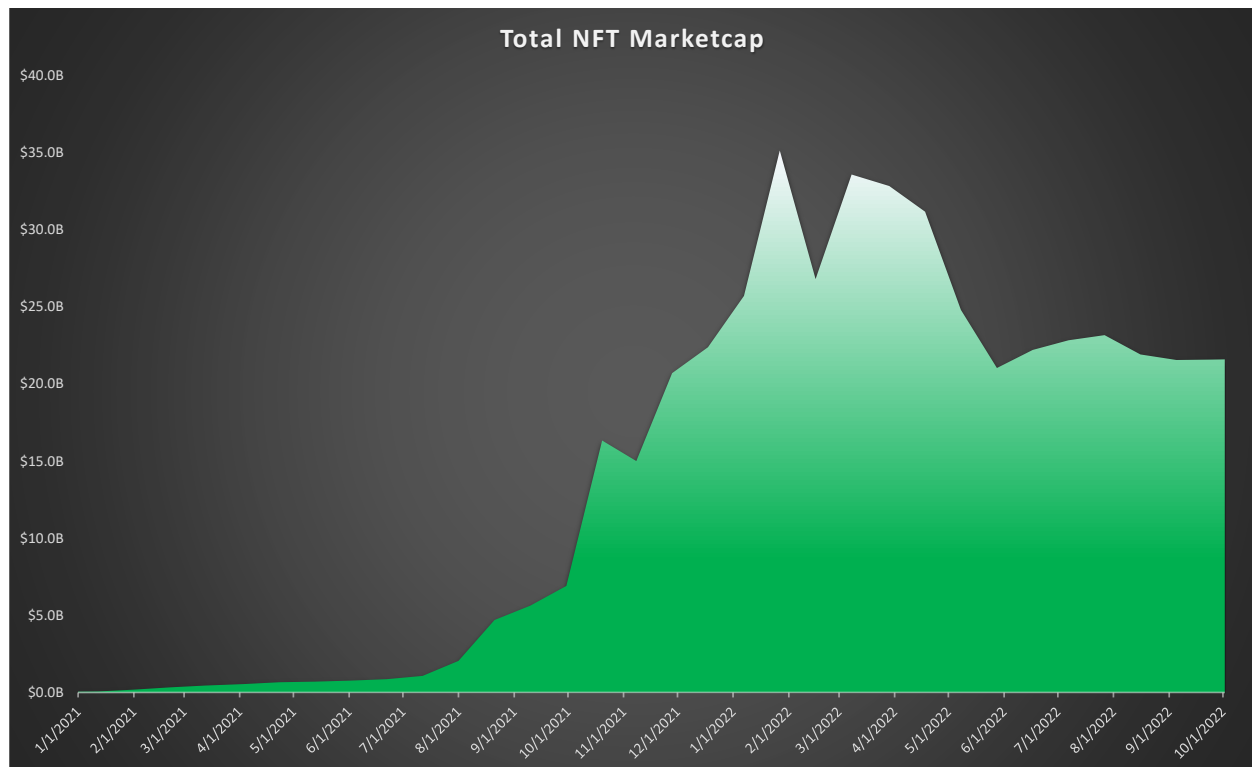
Source: NFTGo as of 10.2.22

While the idea of digital goods is not new, much of the excitement behind NFTs is due to the fact that they completely change the underlying structure of the entertainment industry.

Historically, content has been *owned* by centralized third parties and *rented* to consumers.

For example, if you bought an in-game asset (such as the ultra-rare, $16,000 Dragon Slaying Sabre in the game *Age of Wulin*), you would need permission from the developer to sell it and you likely wouldn't be able to transfer it to other games. In addition, the gaming studio could easily choose to arbitrarily restrict access to your items and / or decide to charge you enormous fees.

NFTs change the game because – for the first time in history – **they allow artists and consumers to truly own their digital goods**. This eliminates the need for centralized third-parties and provides substantial benefits to all stakeholders.

_____

_____

Chapter 22: Problems with Centralized Asset Ownership

The entertainment industry has long been dominated by centralized entities.

The original reason for this was related to the difficulties of distributing content. For example, if a band wanted to sell their music, they would have to rely on a record company to record it, turn it into a physical record and then ship it to a record store where consumers could buy it.

As such, in the 20th century we saw the rise of several entertainment-focused conglomerates such as:

- **Movie & TV Studios**: Disney, NBCUniversal, Paramount, Warner Media and Sony
- **Record Labels**: UMG, Sony and Warner Music Group
- **Video Game Developers**: Activision and Electronic Arts
- **News Organization**: News Corp. The New York Times Company, Daily Mail, etc…
- **Auction Houses**: Sotheby's and Christies
- **Book Publishers**: Penguin Random House, Harper Collins and Simon & Schuster
- **Internet Providers**: Comcast, AT&T and Verizon

Initially, many thought the internet would fix these problems through digital distribution, but it actually made them worse. As internet giants such as Facebook, Amazon, Microsoft, Apple, Google, Netflix and Spotify grew, they began to consolidate power, monopolize distribution and insert themselves into the value chain.

Today the internet giants control over 60% of distribution in several industries.

FAANGs Controls over 60% of the Digital Publishing, Music and Video Markets
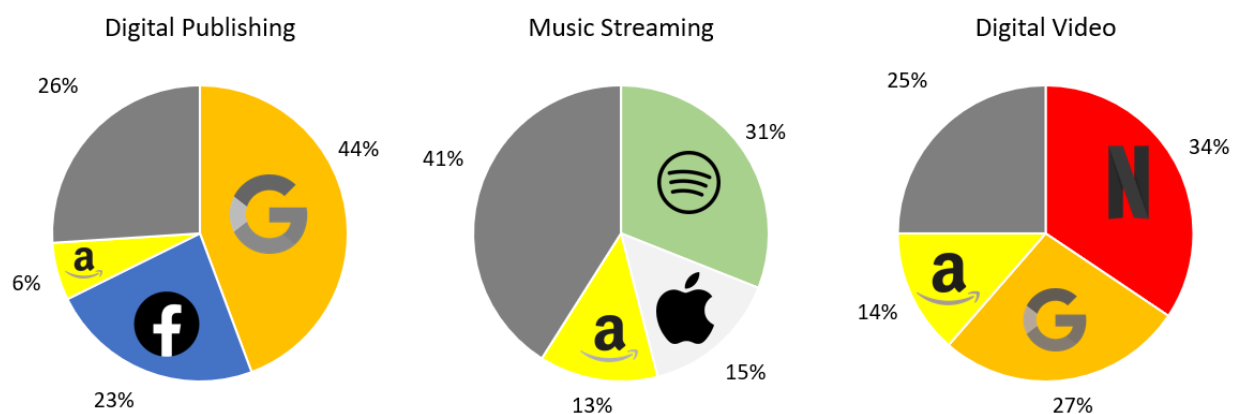
Source: Midia Research, Statista, Ebiquity

To be fair, a centralized internet does have several advantages – most notably the fact that it's very efficient – but these benefits also come at a severe cost to both artists and consumers, including:

_____

_____

- **Rent-seeking:** Intermediaries take a large cut out of an artist's revenue. After accounting for record labels, producers and streaming platforms, artists earn less than 12% on platforms such as Spotify. On the other end of the spectrum, the Apple Store can charge up to 30% taxes on every sale, which is almost certainly passed along to the consumer

- **Censorship:** Companies such as Twitter frequently ban users, and Apple banned Epic Games, the creator of the multi-billion dollar game Fortnite, from its App Store after a revenue dispute

- **Interoperability:** In their current form most online platforms aren't interoperable – you can't buy an Android app on Apple's App Store and you can't purchase an item of clothing in The Sims and wear it in Second Life

But what if there were a better way? What if we could keep the efficiency of the existing system but remove the threat of censorship, allow creators to keep their profits and guarantee interoperability between systems?

Fortunately, NFTs make that possible…

_____

Chapter 23: Benefits of Decentralized Asset Ownership

In the old world, centralized entities owned the content and rented it to users. For instance, after an artist created a song, she might sell it to the record labels, who would in turn license it to a platform such as Spotify who in turn would "rent" it to the user.

NFTs, on the other hand, allow artists to retain ownership of their work and sell it directly to the users. This is immensely powerful because it removes the intermediaries from all transactions.

Source: The Value Chain of the Open Metaverse on Not Boring

One of the biggest benefits to this is monetary, as cutting out the middleman yields **substantial financial benefits to both artists and consumers**.

For instance, after removing the cut taken by record labels, producers and streaming platforms, the average singer receives ~12% of total music sales. By removing the middleman and leveraging blockchain-based platforms such as Audius, this number could increase to over 90%!

_____

_____

NFTs also allow artists to experiment with new streams of revenue, including the ability to sell: 1) original works as collectibles, 2) unique album art, 3) tokens with real-world benefits such as access to shows and 4) memorabilia (such as Snoop Dogg's "Doggies" – digital avatars designed for the metaverse)

NFTs don't just benefit artists, they will also allow *consumers* to monetize content. For example, a user could purchase all or part of the rights to a song directly from an artist and then receive royalties every time someone streams it. They can even make money by playing video games and selling the assets they collect on the open market. For example, in late 2021 people in the Philippines were earning an average of $400 per month playing the blockchain game Axie Infinity – that's more than a local teacher, construction worker, security guard or office assistant!

In addition, many NFTs offer users benefits that well extend beyond possession of the underlying assets, such as: 1) access to a community (which can include anything from Discord membership to private party invites), 2) the right to receive royalties if someone wants to use their art for any reason, 3) the right to create and sell derivative works) and 4) the potential to receive an ownership stake and governance rights of the collection itself.

In addition to these monetary benefits, cutting out the middleman:

- **Eliminates Censorship**: The entertainment giants can no longer censor artists or consumers. Artists are free to upload any content, no matter how controversial, to any platform they so choose

- **Creates Interoperability:** Holders of an NFT truly own their content, which means they can use it to interact with other games, applications, or blockchains and they can also lend out their in-game assets, port them to another application, or gain access to real-world events

- **Transparent:** In contrast to the traditional system of royalty management – which is often complex and opaque - NFTs make it very easy to track the ownership and usage of digital assets, making it easy to determine exactly who gets paid and how much

- **Programmable:** Using smart contracts, NFTs can be programmed to automate payments based on the completion of user actions (such as streaming a song) and automatically approve licensing by users agreeing to preset terms and conditions

- **Lower Costs:**   NFTs can greatly reduce costs by automating many processes traditionally done by intellectual property lawyers, including: drafting patent, copyright and trademark contracts, interpreting complicated IP laws and enforcing rights across multiple jurisdictions

- **Instant:** Traditional art is tough to sell - it requires specialized brokers or auction houses, and even when the sale is made someone has to arrange shipping, storage, security and insurance to ensure safe delivery. Digital art, on the other hand, can be listed online, sold within minutes and delivered instantly

_____

_____

- **Liquidity:** NFTs allow for the creation of "IP markets", where things such as patents, copyrights, trademarks, brand names, etc… can be traded in real-time

Finally, and perhaps most importantly, breaking down the barriers between artists and consumers may usher in a new era of collaboration. Although users have long created derivative works including fan fiction, remixes, etc… it's been difficult to monetize them. By transferring ownership and allowing users to profit from their creations, NFTs could unlock new forms of cooperation that allow artists and fans to merge ideas, build off each other's efforts and create new forms of interactive content.

_____

Chapter 24: History of NFTs

NFTs have existed in some form since 2014, but they experienced most of their growth in two distinct periods: late 2017 and early 2021.

The first "NFT boom" occurred in late 2017, a year that saw the release of Cryptopunks, CryptoKitties and OpenSea. CryptoKitties, in particular, helped bring attention to the space by nearly shutting down the Ethereum network due to its popularity. For the next several years, the NFT market faded into the background as other applications, such as DeFi, gained popularity.

This all changed in early 2021, with the combination of three events – the sudden spike in the popularity of NBA Top Shot (which did >$200 million in February), Beeple's sale of his digital work *Everydays* for $69 million and the launch of the Bored Ape Yacht Club.

These three events helped catalyze an unprecedented bull market that peaked at $38.6 billion in January 2022 – nearly 600x growth from the previous year.

Notable moments in NFT history include:

- **May 2014**: The first known NFT, "Quantum", was created on the Namecoin blockchain

- **September 2016**: The first Rare Pepes are minted

- **June 2017:** Larva Labs launches a collection of 10,000 Cryptopunks. Punks are seen by many as the "OG" NFT asset and long held the title as the most valuable

- **November 2017:** CryptoKitties are first launched, causing the Ethereum network to reach all-time highs in the number of transactions and greatly increasing gas prices

- **December 2017:** OpenSea launches as one of the first decentralized marketplaces for NFTs

- **March 2018:** Axie Infinity, the most popular Play-to-Earn game and top selling NFT, is launched

- **January 2020:** Decentraland, one of the first "metaverses", launches

- **November 2020:** Art Blocks launches, officially becoming the go-to source for generative art NFTs

- **February 2021**: NBA Top Shot records over $200 million in sales in February alone, arguably kicking of the 2021 NFT boom

_____

_____

- **February 2021:** The musician 3Lau sells a collection of NFTs for nearly $12 million

- **March 2021:** Kings of Leon becomes the first band to release an NFT album

- **March 2021:** Jack Dorsey sells his first tweet ever as an NFT for over $2.9 million

- **March 2021:** Beeple sells his *Everydays: The First 5,000 Days* NFT for $69.3 million

- **April 2021:** Yuga Lab introduces its collection of 10,000 Bored Apes, which would eventually become the most valuable NFT

- **August 2021:** Bored Ape Yacht Club holders are gifted with two Mutant Apes and one Bored Ape Kennel Club (a dog)

- **November 2021:** The Sandbox launches its alpha version, eventually becoming the second most valuable virtual world

- **January 2022:** LooksRare forks OpenSea's code in a "vampire attack" and sells over $100M in its first day live

- **January 2022:** Azuki launches a collection of 10K NFTs, doing over $300M of transactions in their first month

- **March 2022:** Bored Ape Yacht Club launches ApeCoin, a token designed to power the platform's upcoming metaverse known as "Otherside"

- **April 2022:** Proof.xyz launches Moonbirds, which shatters previous records with $364.8M of sales in its first five days

- **May 2022:** Bored Ape Yacht Club nets $561M in **one night** by selling land deeds for "Otherside", which almost instantly becomes the most valuable virtual world (the sale also cost users over $100M in fees, creating a decent amount of backlash)

- **September 2022**: Starbucks announces that it will launch an NFT-based loyalty program

Despite this massive growth, the value of all NFTs still remains around 2% of the total market cap of cryptocurrencies.

_____

_____

Chapter 25: How do NFTs work?

Non-fungible tokens function as the goods of a decentralized economy.

While the term may sound confusing, one of the easiest ways to visualize an NFT is as a digital "record of ownership". In many ways it's like the deed to a house, a car's title or an artwork's certificate of authenticity.

Instead of a physical piece of paper you can hold, however, this "certificate" is recorded on a blockchain, where it is linked to your digital address. This not only guarantees the legitimacy of the asset, but also proves that you own it.

Like real-world assets, NFTs can be bought, sold, traded and consumed via smart contract platforms.

<u>The Structure of an NFT: The "Title" to an Asset Held on a Third-Party Server</u>

Digital Wallet　　　　　　**Blockchain**　　　　　**Third-Party Server**

Owner's Address　→

NFT Metadata
1. **Unique ID**
2. **Description of NFT**
3. **Link to Location of NFT**

←　NFT's Address

NFT Art
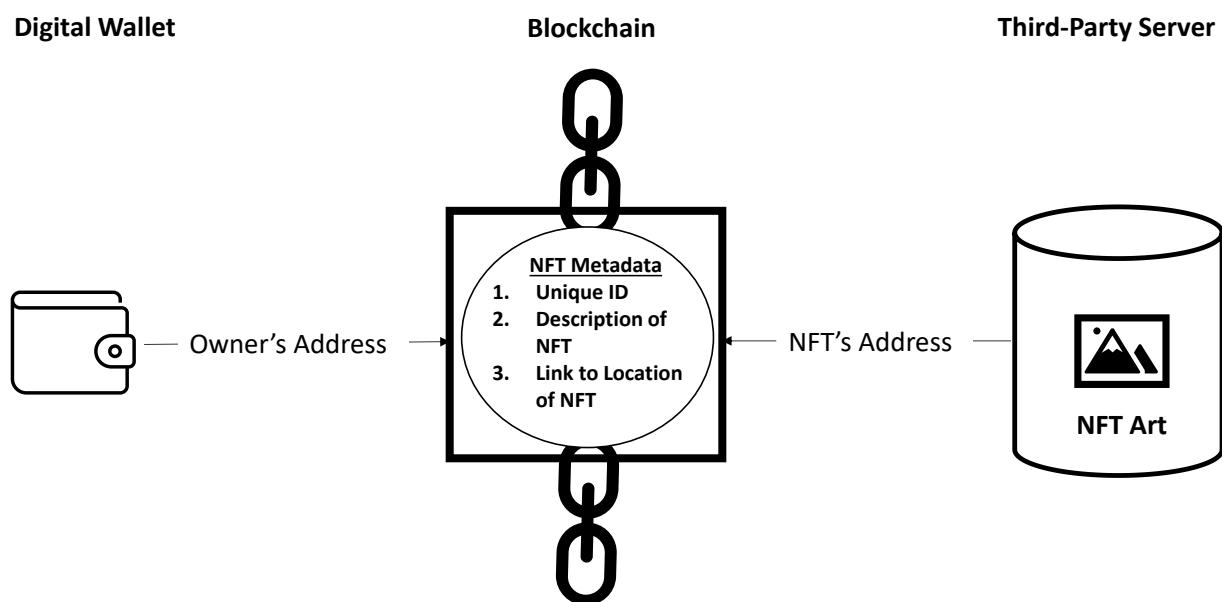
Notable assets that have been tokenized as NFTs to date include digital art, virtual land, music, membership rights, intellectual property and virtual goods in online games.

Contrary to popular belief, most NFTs don't actually host the underlying asset (art, music, etc…) on a blockchain, as this would be extremely expensive (i.e. storing even a modest picture could cost thousands of dollars). Instead, the assets themselves are generally stored a separate server, and the NFT contains a link that *points* to the address of this database (or, as one expert said, an NFT is like "directions to the museum").

_____

_____

To understand how NFTs work, it's helpful to understand three concepts: 1) what is a token? 2) how does a token work? and 3) what makes a token "non-fungible"?

What is a token?

A token is a digital asset that provides its owners with some form of economic value. This value can come in a variety of forms – a token can serve as a currency, it can provide benefits such as voting or ownership rights, it can represent digital assets such as online art, music or virtual land and it can even be tied to a physical commodity such as dollars, gold, real estate or oil.

Like traditional assets, tokens can be bought, sold, traded and even consumed. Unlike the dollar or gold, however, tokens do not have a physical form.

Instead, a token is really nothing more than a long string of numbers that is owned by a wallet address (which is another long string of numbers and letters). This relationship is recorded on a blockchain.

So when you trade tokens or NFTs, you're basically just moving this number to different addresses.

While this may sound scary, this is exactly how most banks work today (over 90% of money exists only online).

There are Many Different Types of Tokens
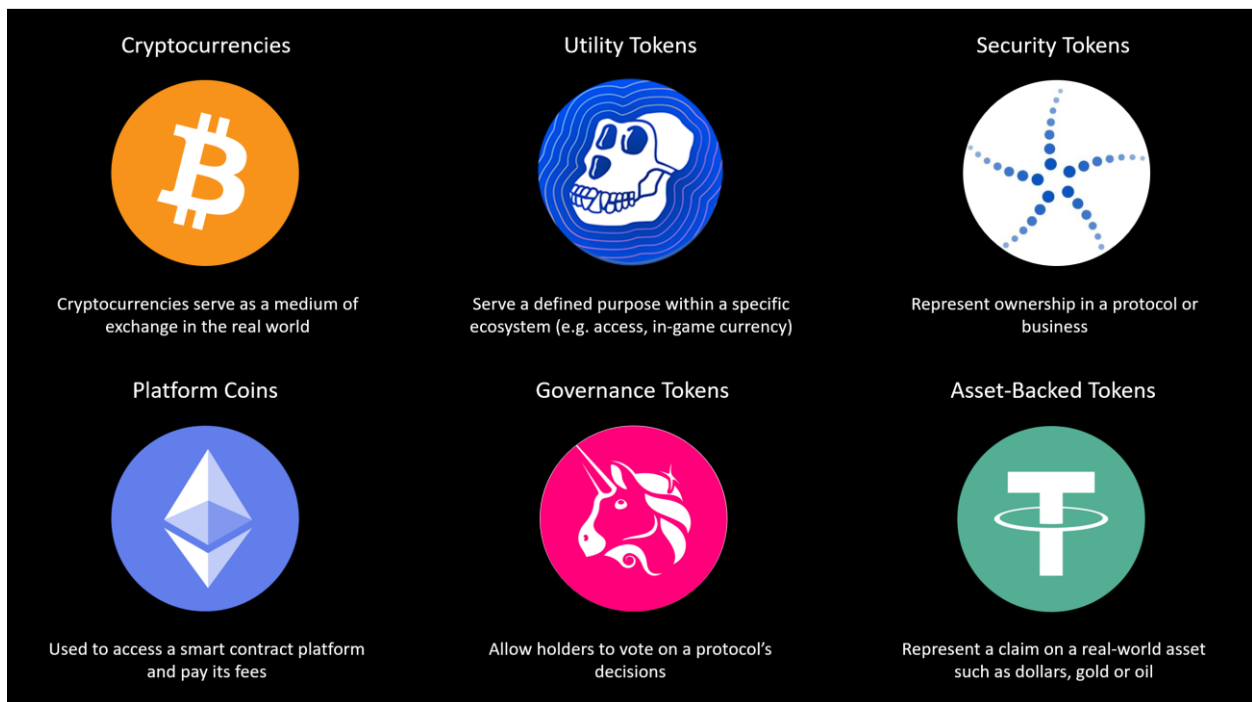
There are multiple different types of tokens including:

_____

- **Cryptocurrencies**: Cryptocurrencies are designed to serve as a medium of exchange in the real world. Bitcoin is the most famous example of a cryptocurrency coin
- **Platform**: Platform coins are needed to access a smart contract platform and pay its fees. Ethereum is the most prominent example of a platform coin
- **Utility**: Utility tokens serve a defined purpose within a specific ecosystem, such as allowing access to a product or service and / or serving as a medium of exchange within a virtual world.   The Bored Ape Yacht Club's ApeCoin is an example of a utility token
- **Governance**: Governance tokens give holders the right to vote on a protocol's decisions. Uniswap's UNI token is the most prominent example of a governance token
- **Security**: Security tokens are the crypto equivalent of stocks in that they represent an ownership stake in a protocol or business
- **Asset-Backed**: Asset-backed tokens represent claims on real-world assets such as dollars, gold, real estate or oil. The most popular form of asset-backed tokens are stablecoins

You may have noticed that I substituted the word "token" for "coin" in a few cases – this was intentional. While the two assets are similar on a fundamental level as they both can store value and process payments, the terms are used differently in the Web3 space.

In particular, a "coin" is a digital asset with its own blockchain (such as Bitcoin or Ethereum) where a "token" operates on another protocol's blockchain (such as the Uniswap and ApeCoin tokens, which operate on Ethereum).

How does a Token Work?

Tokens are secured by cryptography and operate on smart contract platforms using the same three elements discussed in Chapter 10 and Chapter 16 – decentralized ledgers, digital keys and consensus mining. This makes them programmable, permissionless, trustless and transparent.

_____

<u>Tokens Live on Smart Contract Platforms</u>

Source: [Towarddatascience](#)

Smart contract platforms are responsible for creating, storing, authenticating, transferring and standardizing tokens:

- **Creation**: Tokens are created by a smart contract (in the case of NFTs, each token is given a description and unique ID number)
- **Storage**: Tokens are stored on a smart contract platform's native blockchain
- **Authentication**: Ownership is verified through digital key cryptography
- **Trading**: Transactions are executed by the platform's miners
- **Standards**: Smart contract platforms create the rules that allow tokens to function seamlessly across multiple protocols

In exchange for performing these services, token holders pay a fee to the smart contract platform. For example, if you wanted to trade a token on the Ethereum network, you would need to spend ETH, the platform's native coin.

What makes a token "non-fungible"?

The major difference between an NFT and traditional token is a concept known as "fungibility". While it sounds like a scary word, "non-fungible" is really a fancy way of saying "unique". For example:

- **Fungible assets** are <u>not</u> unique, and you can easily swap them for another asset. Currency (both traditional and crypto) is a great example of a fungible asset as you can always swap one dollar bill for another dollar bill or one Bitcoin for another Bitcoin

_____

- **Non-fungible assets**, on the other hand, are unique, and therefore cannot be directly swapped for other assets. Most assets in life – art, real estate, shoes, couches, watches, etc… – are non-fungible (i.e., you can't freely trade a shoe for a house)

- **Semi-fungible assets**, like concert tickets, lie somewhere in between. While any ticket could theoretically be swapped for any other ticket to the same concert, you couldn't swap it for a ticket to *another* concert

<u>Fungible vs. Non-Fungible. Vs. Semi-Fungible Tokens</u>
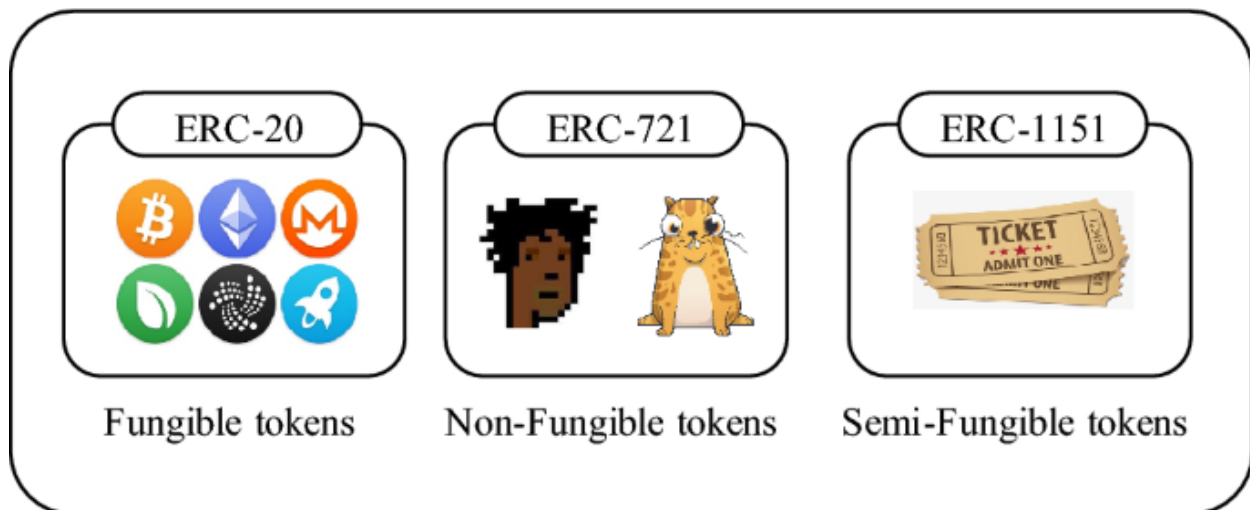
Source: <u>Nature.com</u>

From a technical standpoint, fungible and non-fungible tokens are actually quite similar. They both contain functions to check the supply and balance, transfer tokens and approve transactions. The main difference is that non-fungible tokens each carry a unique ID, whereas fungible tokens do not (for Ethereum's ERC-721 standard, this is known as a "uint256" ID)

_____

Chapter 26: Overview of the NFT Market

According to NFTGo, as of early October 2022, the market capitalization of the NFT space is $21.6B, or around 2% of the crypto space as a whole.
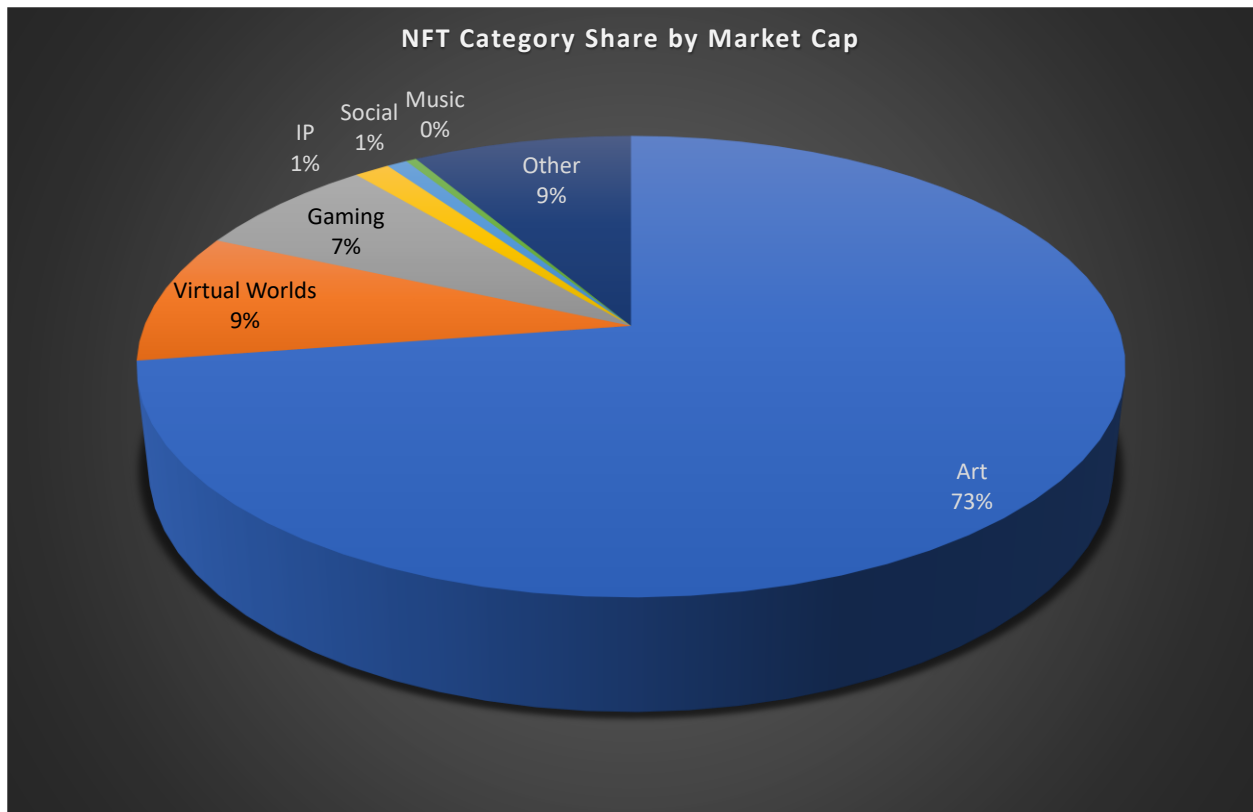
Source: NFTGo as of 10.2.22

The space is broken down into 6 key verticals which include:

- **Art:** Digital art, profile pics and collectibles
- **Virtual Worlds:** Virtual land and goods
- **Gaming:** Play-to-Earn games
- **Intellectual Property:** Patents, trademarks, copyrights, domain names, etc…
- **Social:** Online social clubs and access NFTs
- **Music:** Recorded music and memorabilia

A more detailed analysis of each category is provided below.

_____

_____

Chapter 27: Digital Art

What are Digital Art NFTs?

Digital art NFTs – often affectionally called JPEGs by the community – are by far the largest category in the burgeoning NFT market. They are valued at almost $20 billion and represent 73% of the total value and over 75% of the total volume of all NFTs. That's why when most people hear the word "NFT", they immediately think of a JPEG.

The digital art space has recorded several high-profile sales in the last year, including:

- **Beeple:** *Beeple's Everydays: the First 5000 Days* – a digital mosaic of 5,000 individually crafted pieces –   sold for $69.3 million in 2021

- **Art Blocks:** Forty Art Blocks projects, including several Ringers, Fidenza and Chromie Squiggles, have sold for over $1 million

- **Crypto Punks:** Sixty-eight Crypto Punks have sold for over $1 million with Crypto Punk #5822 going for $23.7 million in February 2022

- **Bored Ape Yacht Club:** Nineteen avatars from the Bored Ape Yacht Club have sold for over $1 million. The collection also boasts the highest floor price (i.e. the minimum price at which you can buy an asset), ranging between $100K and $400K for much of 2022.

- **Mutant Ape Yacht Club:**   Several assets from the Mutant Ape Yacht Club (BAYC's sister project) have sold for over $1 million with one "Mega Mutant Serum" selling for $5.8 million in January 2022

- **Azuki:** The Azuki collection was launched in January 2022 and obtained a floor price of over $120K within 3 months. In addition, Azuki granted all holders two additional assets valued at nearly $20K each in early April 2022 (representing an almost 50x return for original holders).

- **Top Shot:** NBA Top Shot has recorded over $1 billion sales, boasts nearly 700K collectors and has sold over a dozen individual moments for $100K+

_____

_____

Selected NFT Sales in 2021 - 22

Beeple's Everydays: The First 5000 Days: $69.3 Million
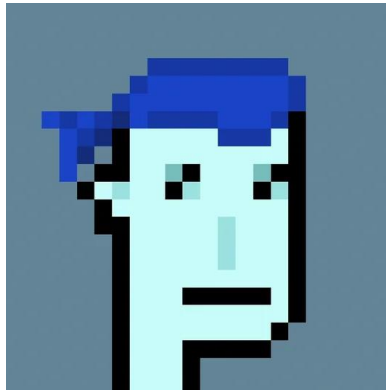
CryptoPunk #5822: $23.7 Million

Mega Mutant Serum #69: $5.8 Million

Although at first glance it may seem odd that people are paying tens of thousands to millions of dollars for pictures of cartoon apes, it's not that strange when you consider the scope of the traditional art market.

Why are Digital Art NFTs important?

Art is an underestimated and often misunderstood asset class. According to crypto research firm Messari, the total value of artwork across the globe is nearly $2 trillion, and the industry does over $50B in revenue per year.

Perhaps more importantly, art has proven to be an outstanding investment: it has outperformed the S&P 500 over the past 25 years, has little correlation with other asset classes, and it performs especially well in times of inflation.

_____

_____

Contemporary Art has Outperformed the S&P 500 Over the Past 25 Years
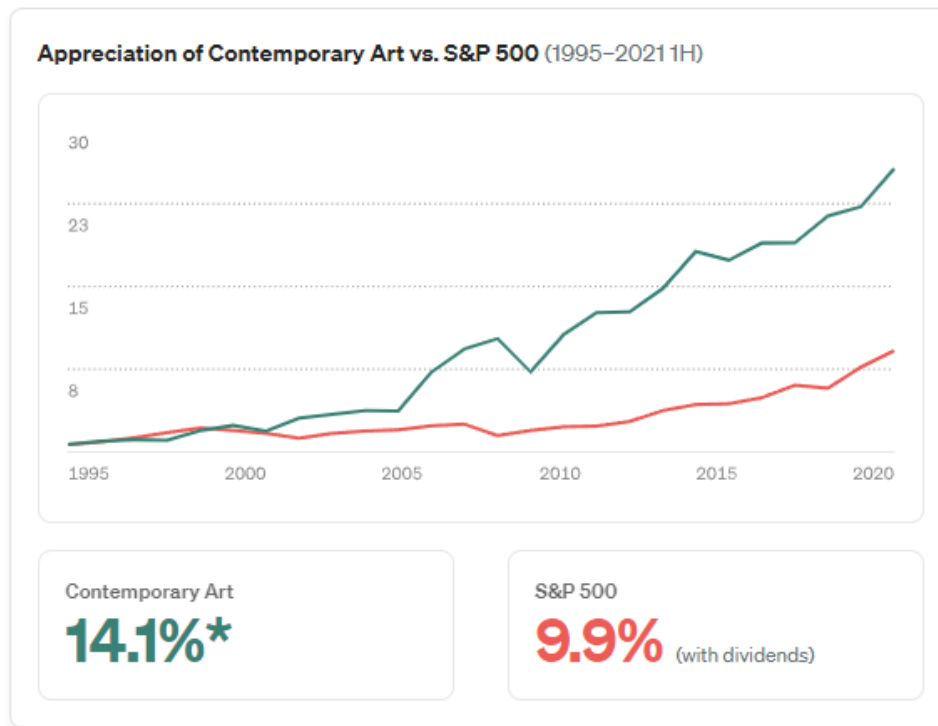
Source: Masterworks.io

Unfortunately, the traditional art market is antiquated and plagued by numerous problems. Not only are fewer than 20% of works sold online, but the industry also suffers from illiquidity, fraud and is notorious for the paltry economics received by creators (there's a reason for the "starving artist" cliché…).

NFTs have the potential to fix many of these problems and several experts believe they could represent art's "Uber moment", catalyzing a 10-fold increase in industry sales. Indeed, proponents argue that NFTs will:

- **Increase Access**: There are currently fewer than 10,000 serious art buyers globally and these collectors tend to be older (average age of 59) and male. Given their ubiquitous access and lower average price point, many researchers believe that NFTs have the potential to grow the universe of buyers by 100x and spawn a demographic shift to a younger and more diverse crowd

- **Enable New Art Forms**: Historically, there was no market for digital art because it was impossible to separate the "owner" of a work from someone who simply made a copy. NFTs have solved this problem, not only creating the first market for digital art but also unlocking the potential for future art classes that we haven't even started to dream up (e.g. programmable art that could change color as the weather or seasons change)

_____

- **Eliminate Fraud**: Fraud is rampant in the art world – it is estimated that [over 50% to 70% of art is fake]() and dealers often embellish a work's record of ownership (known as "provenance") in an attempt to increase the price. NFTs can eliminate both problems, using cryptography to guarantee authenticity and the immutable nature of the blockchain to assure provenance

- **Increase Liquidity**: Art is notoriously illiquid – it requires specialized brokers or auction houses, and even when the sale is made someone must arrange shipping, storage, security and insurance to ensure safe delivery. Digital art, on the other hand, can be listed online, sold within minutes and delivered instantly

- **Make Artists Richer**: While there are several factors limiting an artist's ability to earn a living, one of the biggest is the absence of royalties. Unlike other entertainment markets such as music, film and TV, artists do not receive a cut of sales on the secondary market. Because all NFT sales can be easily tracked and programmed to pay a cut of secondary sales to artists, they will likely usher in an entirely new, royalty-based, business model that will undoubtedly enrich artists

- **Increase Consumer Utility**: Many NFTs offer consumers benefits that go well beyond holding traditional art, including: 1) access to a community (which can include anything from Discord membership to private party invites), 2) ownership of the IP (i.e. the right to receive royalties if someone wants to use your art for any reason *and* the right to create and sell derivative works) and 3) potential to receive an ownership stake and governance rights of the collection itself. As such, many NFT buyers feel like they're purchasing a piece of art + a country club membership + the IP rights to the next Spiderman + shares of stock in the next Marvel

Finally, NFTs can be an extremely effective display of wealth and status. While this may seem gauche – it's an undeniable part of human psychology (and perhaps one of the reasons that Bernard Arnault, the Chariman and CEO of Louis Vuitton, is one of the richest men in the world).

<u>Key Players in the Digital Art Space</u>

For the purposes of this report, we'll divide digital art into three categories:

- **Art**: This category includes manmade digital art (such as Beeple's *Everydays*) and generative art, which is art made by computers (such as Art Blocks)

- **Avatars**: Includes art such as the Bored Ape Yacht Club that is intended to be used as a profile picture on Twitter, Facebook, Discord and / or Instagram (and eventually as one's "avatar" in the Metaverse)

- **Collectibles**: Includes virtual memorabilia such as NBA's Top Shot, which creates virtual trading cards of memorable moments, such as a game-winning dunk by LeBron

_____

_____

Avatars are the Largest Category of the Digital Art Market at Over 70%
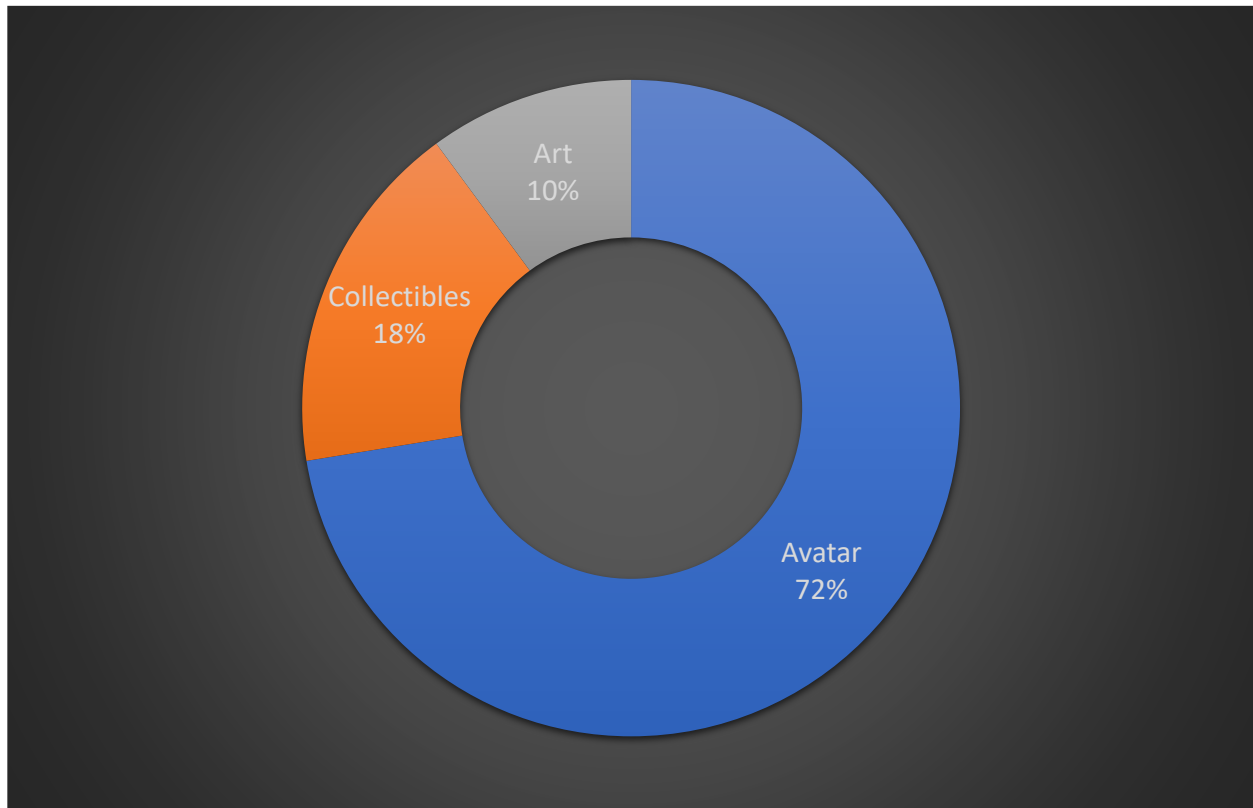
Source: NFTGo as of 10.2.22

More on these three models is below.

Avatars

Avatars are far and away the most popular category of NFT, representing 72% of digital art and over 50% of all NFTs.

Their most immediate use is as a profile picture on social media sites such as Twitter, Instagram or Discord – in fact, that's why they are often called PFPs for "Profile Picture" or "Picture for Proof", depending on whom you ask.

My Twitter PFP at the Time of Writing

But there's actually a lot more to these avatars than first meets the eye, as we will see when exploring one of the most popular PFP projects, The Bored Ape Yacht Club.

The Bored Ape Yacht Club is a collection of 10,000 pictures of apes. It was created in 2021 by parent Yuga Labs.

Apes are created using a process known as generative art. This means that the artists created several "templates" (e.g. different expressions, fur colors, hats, earrings, eyes) and layer these templates on top of one another with a computer program to create 10,000 works – each unique in its own way.

_____

<u>The Bored Ape Yacht Club</u>
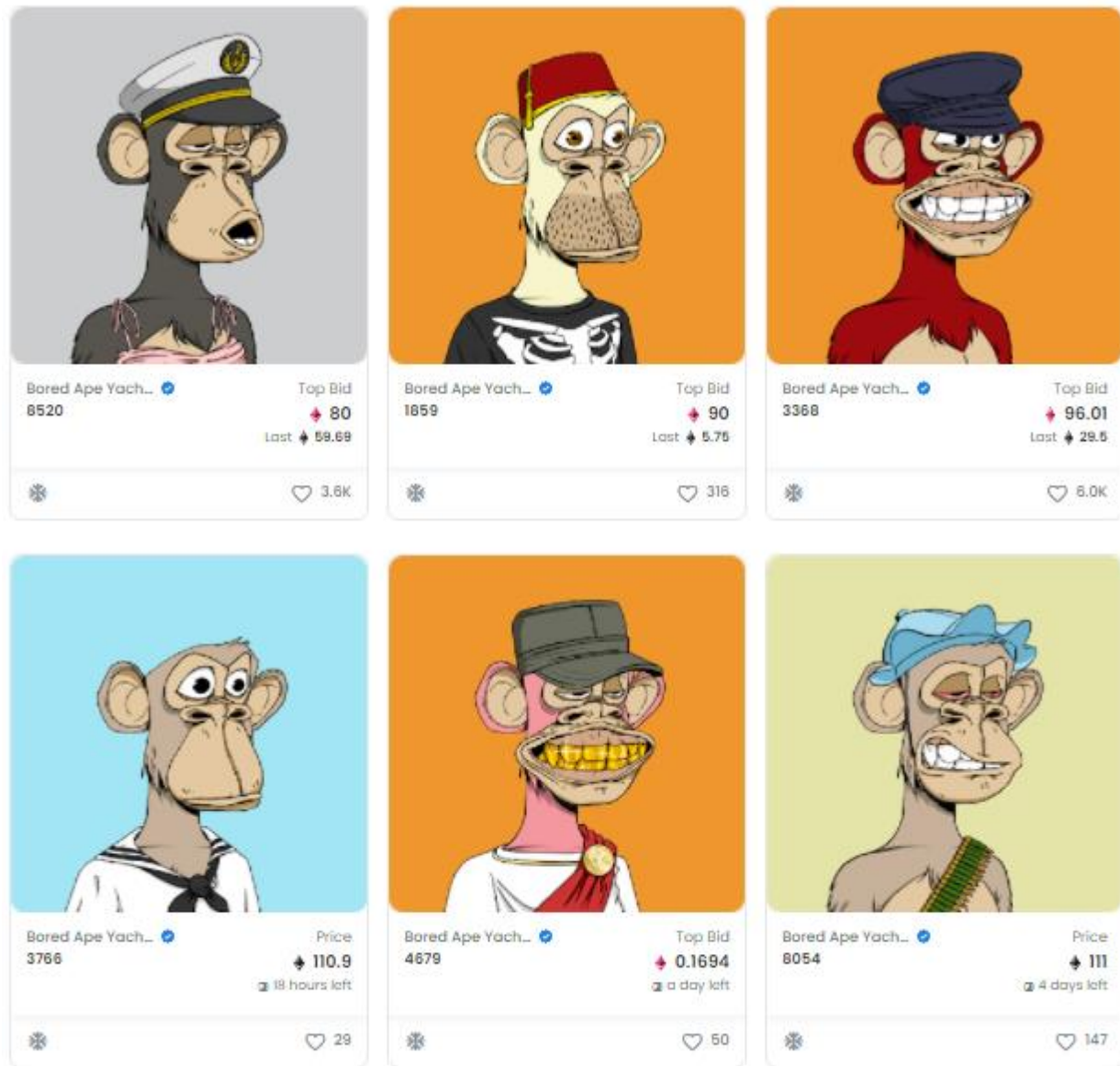
Source: OpenSea

At the time of writing, the cheapest apes sell for approximately $100K (down from $400K in April 2022!), while the most expensive have sold for millions. The Bored Ape Yacht Club community also includes 20,000 Mutant Apes, 10,000 Bored Ape Kennel Club dogs (to keep the apes company!), its own propriety token known as APE and a decentralized virtual world known as the "Otherside".

While on the surface each ape can be thought of as a piece of art, there are several indirect benefits to owners that include:

_____

_____

- **Access to an exclusive community**: The Bored Ape Yacht Club (BAYC) grants members access to its private Discord group, hosts members-only parties and has plans to build a physical clubhouse

- **Airdrops, Dividends and Distributions**: All original holders received two free Mutant Apes and one Bored Ape Kennel Club dog in 2021, and up to 15,000 APE tokens and three pieces of Otherside metaverse land in 2022. At their peak in April, these free distributions were worth over $350K. Combined with the value of the original APE at the time, anyone who participated in the original mint in April 2021 for ~$200 would have had over $750K in assets (assuming they held). **That's nearly a 4,000x return in one year!**

- **Ownership of the IP**: Most projects grant owners exclusive IP rights, allowing them to create and sell derivative works and receive royalties if someone wants to use their avatar in a game, music video or marketing. This could be quite lucrative, as one BAYC holder partnered with CAA for representation, another launched their own music group in partnership with UMG and the project is in talks to create a play-to-earn game, which could leverage the assets from multiple users

- **Free ApeCoin:** ApeCoin is the official token of the Bored Ape Yacht Club ecosystem. It is intended to be used for payments in the Otherside as well as for purchases of real-world merchandise. There are 1 billion ApeCoin tokens, and 150 million of them were originally airdropped to Bored Ape, Mutant Ape and Kennel Club holders. In addition, there are rumors that BAYC holders will be able to "stake" their assets to earn more tokens

- **Ownership of ApeCoinDAO**: Ownership of APE tokens also grants holders governance rights of ApeCoinDAO, the entity responsible for governing the ApeCoin token

Interestingly, Yuga Labs itself is quickly becoming a powerhouse in the NFT community. The project recently received funding from A16Z at a valuation of $4B and, according to a leaked pitch deck, It generated nearly $140M in revenue in 2021 at >90% margins and expects to generate over half a billion in 2022. In addition, the project has a notable social media presence with nearly a million Twitter followers and is held (or has been held) by several celebrities including Justin Bieber, Serena Williams, Jimmy Fallon, Shaq, Steph Curry, Neymar Jr., Eminem, Tom Brady and Snoop Dogg.

_____

Notable Bored Ape Yacht Club Holders

In addition to the ecosystem expansions listed above, the studio purchased the rights to CryptoPunks and Meebits from Larva Labs in March 2022. This gives Yuga the rights to almost 50% of all avatars! (but remember that due to the decentralized nature of Web3, they don't actually "own" this IP – the NFT holders do)

As you can see, digital art avatars are shaping up to be so much more than merely "art". In many ways, JPEGs can be considered "art *plus*", and holders of these assets often hope they're buying the next Picasso + membership at Augusta + the IP rights to Spiderman + a share of stock in Marvel.

In addition to the Bored Ape Yacht Club, there are several other high-profile avatar collections including Crypto Punks, Meebits, Mutant Ape Yacht Club, Clone X, Moonbirds and Azuki.

_____

_____

Market Value of Selected Avatar Collections
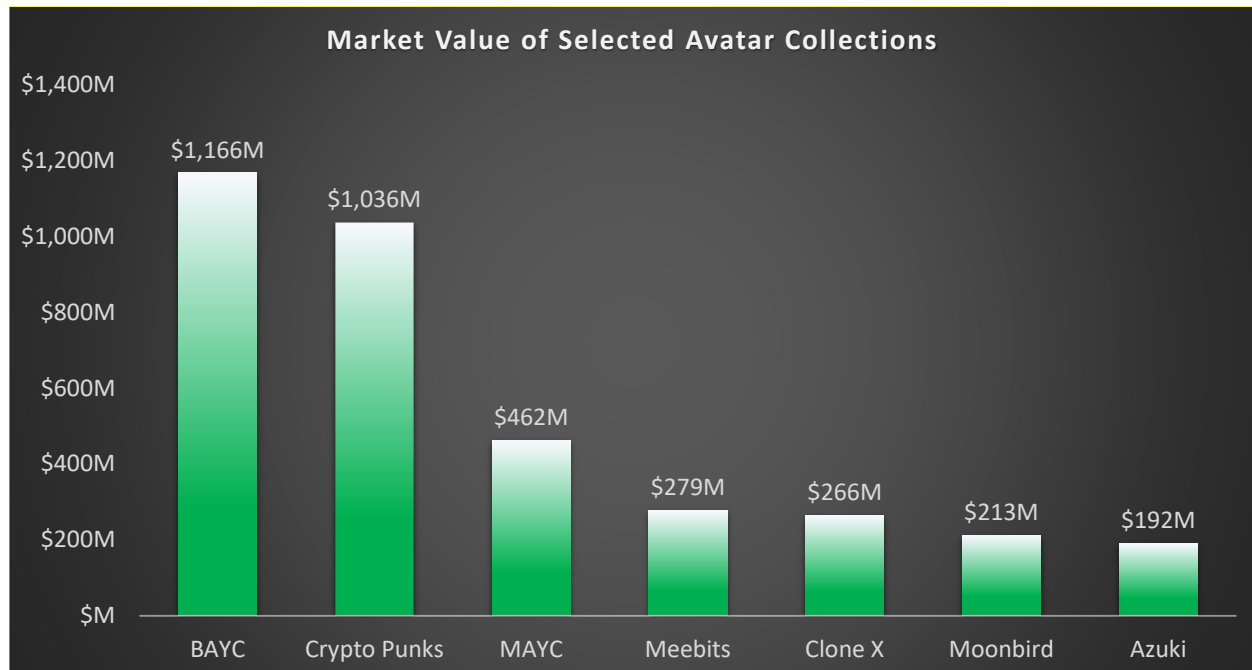
Source: [NFTGo](#) as of 10.2.22

Collection	Image	Total Value	Floor Price	Description
Bored Ape Yacht Club		$1,166M	$104K	The Bored Ape Yacht Club is Yuga Lab's flagship project, representing 10,000 unique avatars of apes.
Crypto Punks		$1,036M	$82K	Crypto Punks were one of the first NFT projects launched by Larva Labs in 2017. They are simple 8-bit images and part of a collection of 10K. The project has since been acquired by BAYC parent Yuga Labs
Mutant Ape Yacht Club		$462M	$20K	The Mutant Ape Yacht Club is the sister project to The Bored Ape Yacht Club. In August of 2021, each BAYC holder received two free "serums", which could be used to generate two unique Mutants

_____

_____

Meebits		$279M	$4K	Meebits represent a collection of 20,000 unique 3D characters. They were originally created by Larva Labs but acquired by Yuga Labs along with Crypto Punks
Clone X		$266M	$9K	Clone X is a collection of 20K 3D avatars created by the RTFKT (pronounced "artifact") studio which was acquired by Nike in December 2021
Moonbirds		$213M	$13K	Moonbirds is a collection of 10K PFPs launched by Proof.xyz. They provide access to the Proof community and shattered previous records by selling over $350M in the first five days after their launch in April 2022
Azuki		$192M	$12K	Azuki is a collection of 10K avatars created in with an "anime/manga" style. It is notable in the ecosystem for its explosive growth in 2022.

_____

Collectibles

Collectibles are the second most popular category of digital art, representing 17% of the sector and 13% of all NFTs.

There are several categories of collectibles, but one of the most popular is proving to be sports. Sports NFTs may provide an ideal venue for onboarding "normies" into crypto, given the rabid fanbase and high degree of overlap with the $30 billion fantasy sports / trading card market. Indeed, we have seen several notable projects in the space – such as UFC Strike, NFL All La Liga and cricket's FanCraze – and Deloitte estimates that 4 to 5 million people will purchase sports NFTs in 2022, generating revenue of over $2 billion.

One of the top sports collectibles is a project known as NBA Top Shot, which was formed as a partnership between the NBA and Dapper Labs, the company that created Cryptokitties.

The platform allows users to collect and trade "moments" – video clips of specific game highlights with relevant information such as statistics about the game and players featured. In short, they're the modern equivalent of baseball cards.

NBA TopShot has recorded over $1B in sales to date, peaking at nearly $225M in February 2021. Prominent moments on sale at the time of writing include:

Source: NBA Top Shot

_____

Art

Art is another popular category of NFT, representing 10% of the total digital art market and 7% of all NFTs.

Perhaps the most famous example of digital art is Beeple's *Everydays – The First 5,000 Days*, a collage of 5,000 digital images that sold for $69M in 2021. The work was notable because it was the first purely digital work sold by a major auction house.

Beeple's Everydays Sold for $69 Million in 2021

_____
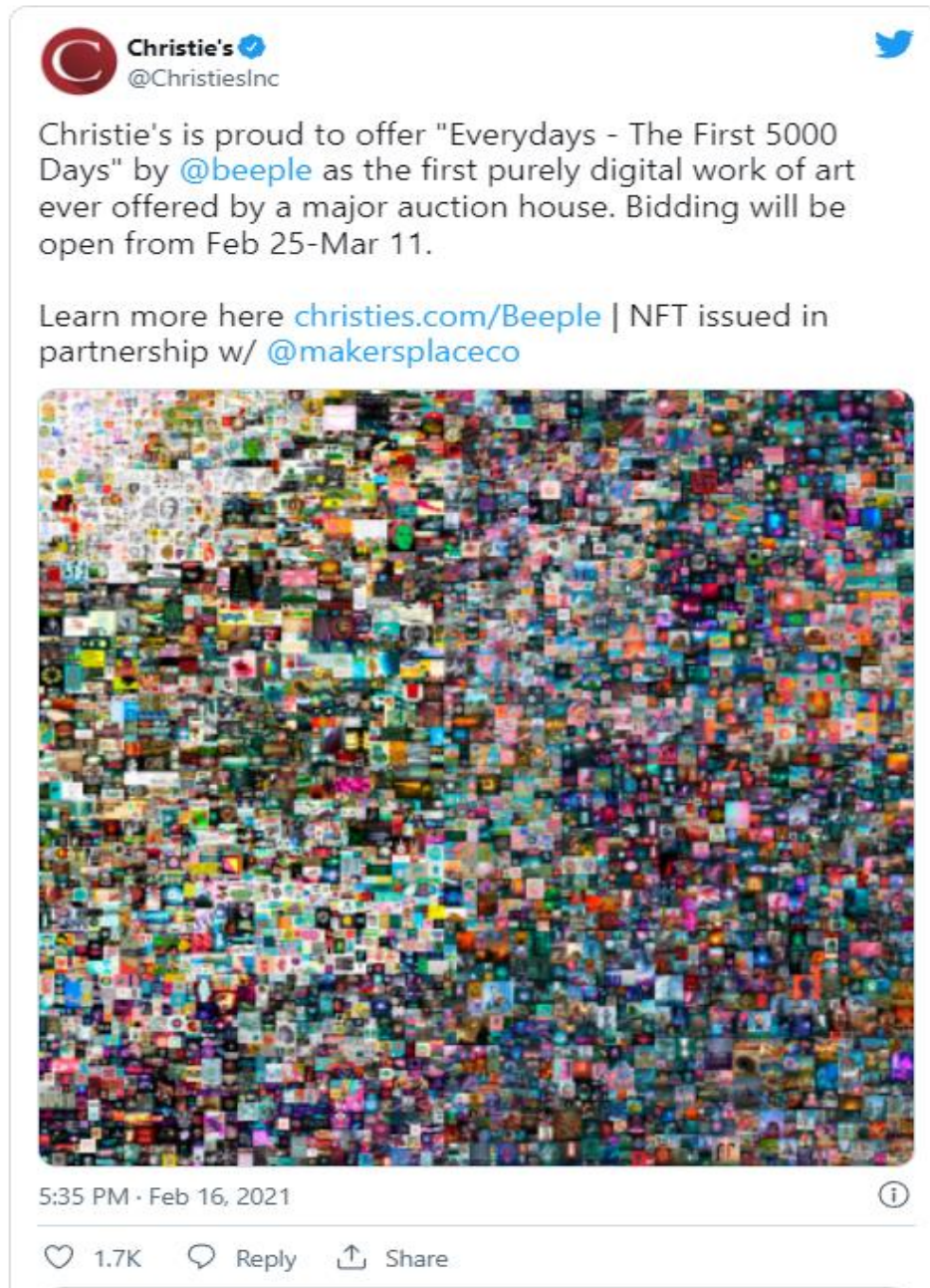
While the sale of *Everydays* was groundbreaking, it's likely just the tip of the iceberg, as artists are using the functionality of smart contracts and NFTs to experiment with new designs.

One of the most popular is known as generative art – art made in partnership with a computer.

Unlike traditional art, generative artists don't directly create their works. Instead, they write a software program that defines an acceptable "universe" of artistic elements such as shapes, colors and basic geometries.   When this code is executed, the computer then randomly assembles these elements to create distinct works.

As such, each piece is unique and neither the artist nor the buyer has any idea what it's going to look like until the process is complete.

This represents an important evolution – while digital artists have long used computers as a ***medium*** to make art (much like a painter would use oil or a sculptor clay), generative art takes this a step further and leverages the computer as a ***co-creator***.

Like Monet's impressionism in the late 19th century, Picasso's cubism in the early 20th and Warhol's Pop Art in the 60s, many argue that generative art best captures the zeitgeist of our time – one where the line between human and machine is beginning to blur.
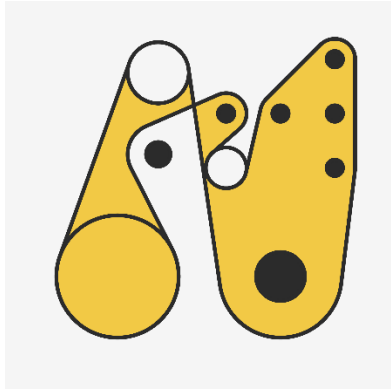
One of the most popular platforms for generative art is Art Blocks, which allows artists to create and sell their works. Popular collections include:

- **Ringers**: A series of 1,000 generative art NFTs created by Dmitri Cherniak
- **Fidenza**: A curated collection of 999 works produced by Tyler Hobbs
- **Chromie Squiggles**: An art collection created by Snowfro, a Mexico-city born technologist and generative artist

To date, the platform has recorded over $1B in sales including:.

Asset	Image	Price
Ringers #109		$6.9M

_____

_____

Ringers #879		$5.6M
Fidenza #313		$3.2M
Chromie Squiggle #4697		$2.8M

_____

Fidenza #77		$2.7M
Chromie Squiggle #7583		$2.7M

_____

Chapter 28: Virtual Worlds

What are Virtual Worlds?

Often called "metaverses", virtual worlds are online, immersive 3D spaces.

Using an avatar – a graphical representation of their persona– users can explore these virtual worlds, interact with other users, create and trade digital goods, participate in meetings, attend events, play games and build in-world objects and landscapes.

Although many virtual worlds are currently PC and / or mobile-based, it is expected that most will transition to virtual and augmented reality as the technology continues to mature.

Justin Bieber Hosting a Concert in the Metaverse
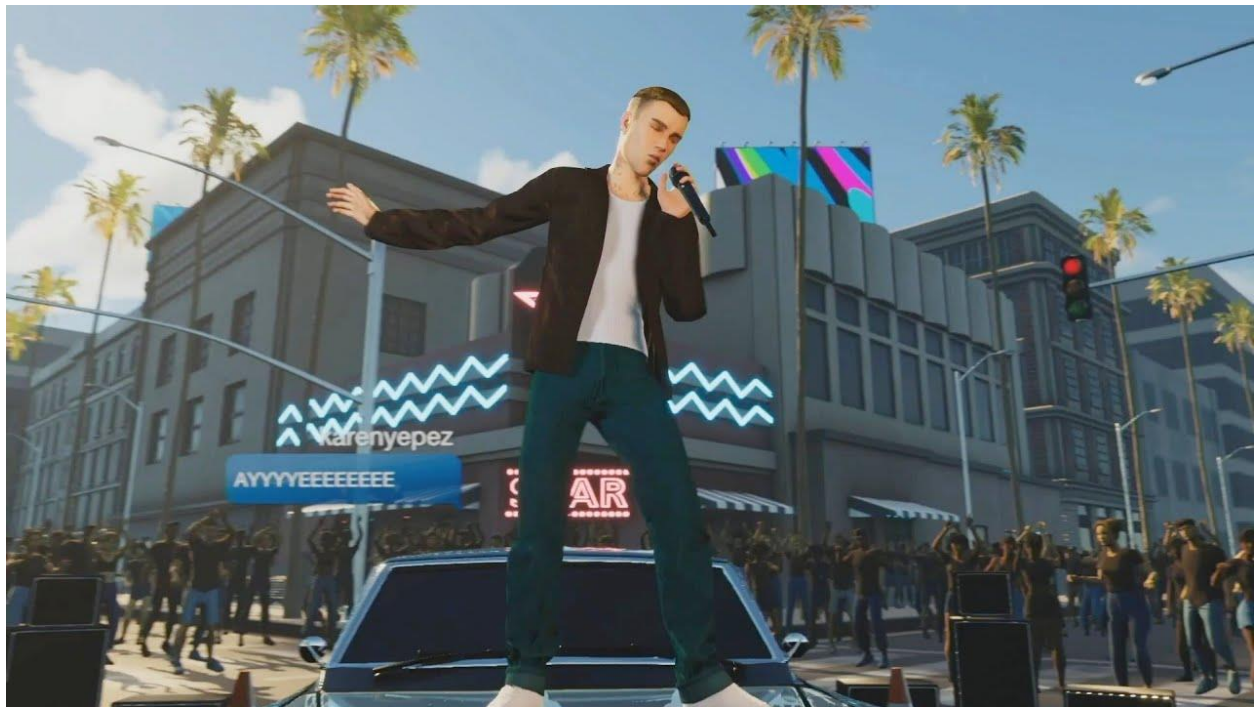
Source: Youtube

Virtual worlds host their own self-sufficient economies which include:

- **Land** which can be bought, sold, rented and developed
- **Digital Goods** which can be consumed and traded
- **Native currencies** to buy and sell goods and services

While companies such as Meta (formerly Facebook) are making a strong push into the space, there is a sizable constituency hoping to create a user-owned and decentralized metaverse using NFTs to represent land and goods and cryptocurrencies as the native currency.

_____

_____

The virtual worlds category has recently overtaken gaming to become the second largest category of NFTs, representing 9% of market value and 6% of all volume.

To date, users have spent nearly $2.5B on digital land and in-game items in the metaverse, and many researchers believe the space represents a multi-trillion dollar opportunity (with some projections ranging as high as $30 trillion!)

What are the Benefits of Decentralized Virtual Worlds?

Virtual worlds will offer numerous benefits to the consumer, including the ability to facilitate remote work, allow virtual doctor visits, create engaging and immersive games and generally just provide a "fantasy world" for us to escape reality and become anything we want to be.

One of the greatest threats to the metaverse is control by a digital monopoly. We have already seen the dangers of a centralized internet, and these threats have the potential to turn into a nightmare scenario as we move more of our lives online.

Indeed, if we aren't careful, companies such as Facebook, Amazon, Microsoft, Apple, Google could gain even more power in the metaverse and form "digital dictatorships", levying heavy taxes on usage and exercising absolute control over what we can and cannot do.

Fortunately, using blockchain technology, we can create a decentralized metaverse, where ownership remains with the community – creators, consumers and developers.

This would have several benefits including:

- **Fair economics**: The Apple store currently charges participants up to a 30% tax on every sale. Eliminating the middleman would allow creators to sell directly to consumers without having to pay outrageous fees like these

- **Permission-less Access**: Facebook notoriously shut down its most popular game Farmville over a disagreement in economics. Decentralized virtual worlds would eliminate this threat, as users can't be banned or restricted access in any way, can't be shut down and anyone can access them at any time

- **Reduced Censorship**: Platforms such as Twitter have full control over the decision to ban or censor users, and unfortunately they are exercising this power more and more frequently. Decentralized worlds, by contrast, would eliminate censorship, allowing users to upload any content – no matter how controversial – to any platform they choose

- **Interoperability**: In their current form, virtual worlds are not interoperable – you can't buy an item of clothing in The Sims and wear it in Second Life. An open metaverse, on the other hand, would allow users to freely transfer their virtual goods from one world to the next. For instance, if you bought a flaming sword in World of Warcraft, you could theoretically use it in Farmville (🤓)

_____

_____

How do Decentralized Virtual Worlds Work?

To understand how virtual worlds work, let's look at one of the largest players – The Sandbox.

The Sandbox is a user-generated, 3D virtual world that allows users to own land, design characters and create and host their own play-to-earn games. While the project was originally created in 2012, it was acquired by Animoca Brands in 2018 for use as a blockchain-based gaming metaverse. The alpha version of The Sandbox was launched in late November 2021.

In many ways the platform functions like The Sims or Second Life, with one key difference – **users maintain full ownership of their characters, land, games and virtual goods**.

The Sandbox's virtual economy is powered by several core tokens including:

- SAND: The platform's native in-game currency that is used for all transactions within the world
- LAND: NFTs representing plots of digital real estate within the Sandbox Metaverse
- ASSETS: NFTs representing digital goods such as characters, animals, vehicles, buildings, etc…
- GAMES: Play-to-Earn games created and hosted by users

<p align="center">Core Tokens in The Sandbox</p>

<p align="center">Source: <u>The Sandbox via Medium</u></p>

Let's take a deeper look into each of these tokens…

SAND

The Sandbox's virtual economy is powered by its native currency known as SAND. SAND is an ERC-20 (fungible) token with a variety of uses, including:

- **Purchases:** As the in-game currency for The Sandbox, SAND can be used to play games, purchase assets and land, customize and upgrade their characters, buy equipment, etc…

_____

_____

- **Staking:** Holders can stake SAND to earn passive income

- **Governance:** SAND also functions as a governance token, allowing users to vote on decisions impacting The Sandbox ecosystem

As of October 2nd, 2022, there are currently 1.5 billion tokens available out of a maximum total supply of 3 billion. The current fully-diluted market capitalization of SAND is $2.6B.

LAND

The Sandbox contains NFTs representing 166,464 plots of LAND which can all be fully owned by users and traded much in the same way as physical real estate.

<u>Developed Plot of Land in The Sandbox</u>

Source: [Metaverse Properties](#)

Like in the real world, owners can also build whatever they want on their property, and we have already seen several commercial enterprises created on the system, including:

_____

_____

- **Casinos:** The Sandbox has several virtual casinos

- **Concert Venues:** Warner Music Group is launching a metaverse concert hall in partnership with Snoop Dogg

- **Cultural Venues:** Several Hong Kong investors have joined to build "Mega City", a cultural hub showcasing art, film, music and gaming

- **Nightclubs:** The Sandbox boasts several nightclubs

- **Retail Stores:** Gucci purchased land in February 2022 to create an online store

- **Sports:** HSBC recently bought a plot of land to construct a virtual sports stadium

- **Virtual Offices:** The government of Dubai has purchased a plot of land in The Sandbox to build a virtual headquarters for its Virtual Assets Regulatory Authority

Multiple plots of LAND can also be combined to form ESTATES.

ASSETS

ASSETS are the native digital goods of The Sandbox. They can include anything that will populate the platform's virtual world, including characters, equipment, outfits, buildings, etc…

Sample of Assets in The Sandbox

Source: [The Sandbox via Medium](#)

_____

_____
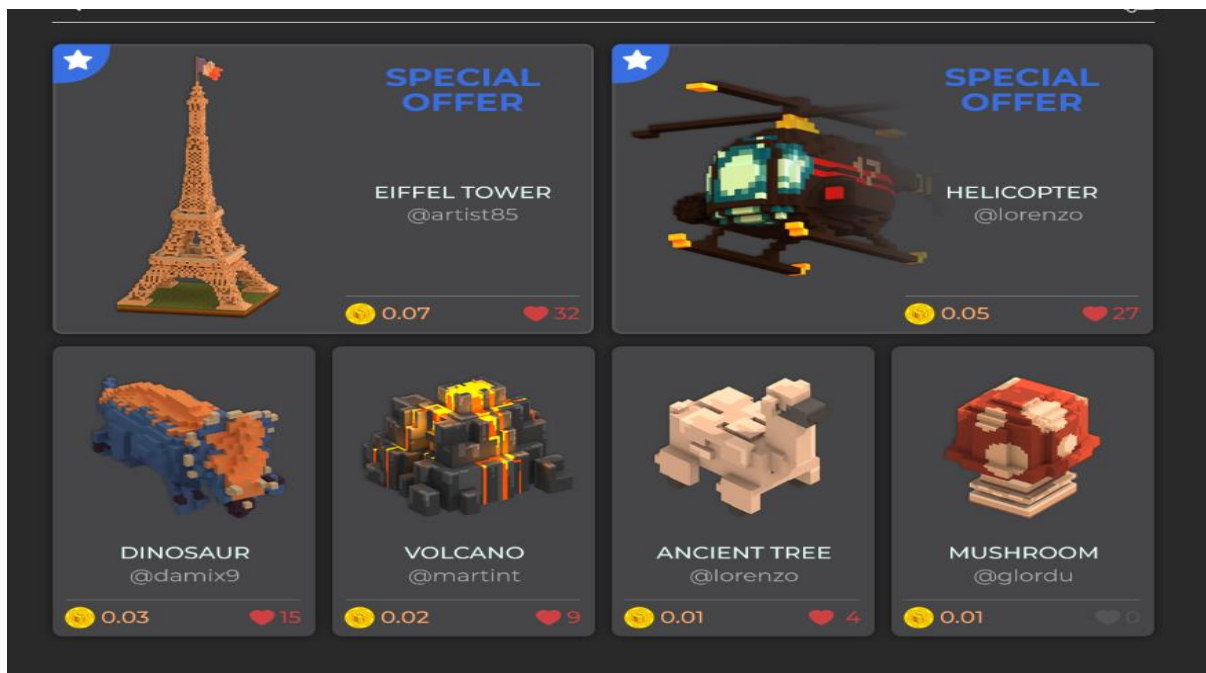
All ASSETS are represented as ERC-1155 ("semi-fungible") tokens, allowing users to create unlimited copies of a given piece.

GAMES

One of the key features of The Sandbox is that it allows users to create and host 3D, play-to-earn games on LAND that they own (or rent). To create a game, users have access to three tools.

- VoxEdit: A program that allows users to create 3D virtual assets to populate the game such as characters, animals, structures, foliage, etc…
- Marketplace: A decentralized platform that allows creators to buy and sell existing assets for use in the game
- Game Maker: A simple editor that allows users to create games without needing to know how to code

Three products in The Sandbox ecosystem

VoxEdit	**Marketplace**	**Game Maker**
VoxEdit: a tool used to create NFT game assets.	A marketplace: where you may sell and acquire those assets.	Game Maker: a program that allows gamers to create their games without knowing how to code.

Source: Cointelegraph

Once created, creators can invite other users to play the game and also monetize it in any way they see fit – they can charge other users to play, sell the NFT ASSETS required to play the game or even sell the game itself.

While some describe The Sandbox itself as a game, it is more accurately described as a collection of user-generated games.

_____

_____

Traction

Although activity has slowed in the bear market, The Sandbox has nonetheless achieved impressive traction, garnering nearly 3.5M users and generating over $500 million in sales volume to date.

In addition, the project has recorded over 165 high-profile partnerships with individuals and companies such as Snoop Dogg, Adidas, The Walking Dead, The Smurfs and Atari. The project recently raised $400M at a $4B valuation and notable investors include Softbank, Liberty City Ventures and Samsung Next.

Who are the Key Players in the Virtual World Ecosystem?

In addition to The Sandbox, there are several other notable projects including Otherside, Decentraland, NFT Worlds and NEO Tokyo.

Total Volume of Metaverse Projects

Otherside	$1,302M
The Sandbox	$564M
Neo Tokyo	$254M
Decentraland	$225M
NFT Worlds	$166M
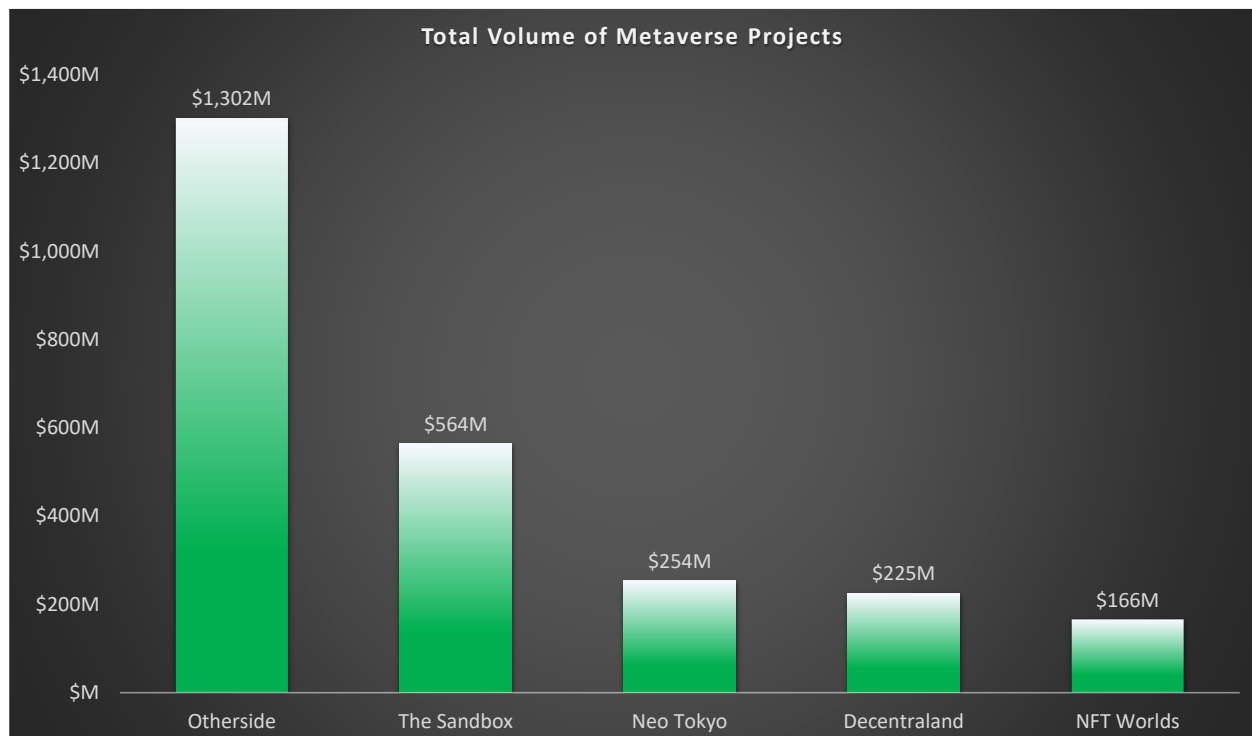
Source: Nonfungible as of 10.2.22.

_____

_____

Virtual World	Volume	Description
	$1,302M	Otherside is the Bored Ape Yacht Club's metaverse project. While the virtual world has yet to launch, it instantly became the most valuable virtual property after its "deed" sale on April 30th 2022
	$564M	The Sandbox is the second largest virtual world with over half a billion in total volume
	$254M	Described as "Blade Runner meets Anime", Neo Tokyo is a relatively recent project based on the 1978 dystopian thriller of the same name. Users can purchase identities, item caches and land deeds for the upcoming virtual world
	$225M	Decentraland is one of the oldest virtual worlds. The project has 90,601 parcels of land
	$166M	NFT worlds has 10,000 parcels and is built to be compatible with the popular game Minecraft

_____

_____

Chapter 29: Gaming

What are Play-to-Earn Games?

Play-to-Earn ("P2E") gaming is a business model that allows users to earn in-game goods and / or tokens by playing a game, and then sell those assets on the open market to earn real-world income.

This represents a disruptive evolution over legacy gaming business models such as pay-to-play and free-to-play:

- **Pay-to-Play Games**: The earliest games, such as World of Warcraft and Grand Theft Auto, charged users an upfront fee for playing
- **Free-to-Play Games**: Popularized in the 2010s, the "freemium" model used by games such as Fortnite and League of Legends allowed anyone to play for free, but generated revenue through in-game sales and upgrades

Play-to-Earn Gaming Represents a Significant Evolution in the Gaming Industry
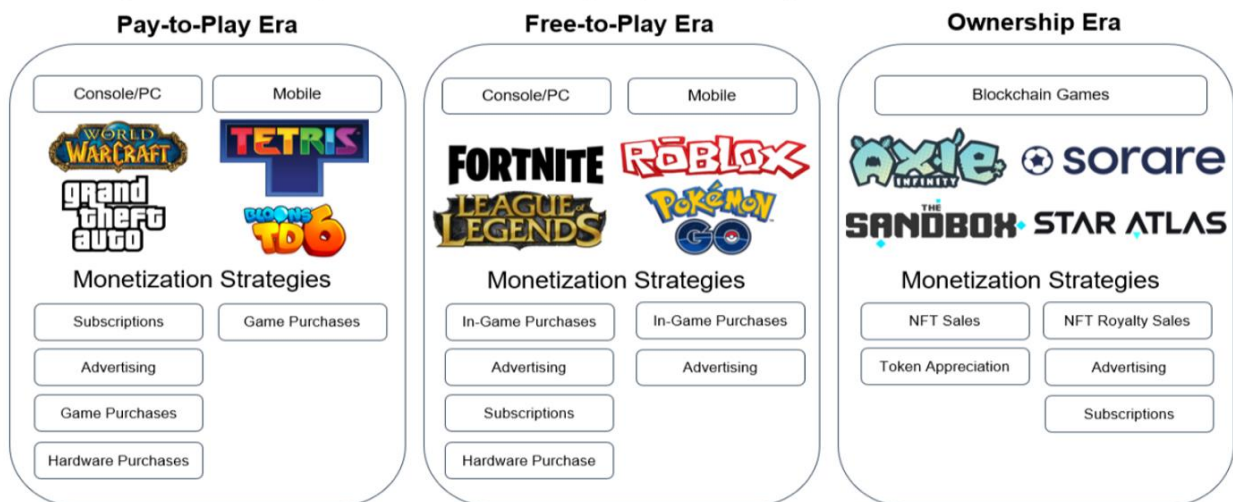
Source: Messari

The P2E business model is now only feasible at scale due to the unique properties of NFTs, which allow users to truly own their assets, transfer them freely and sell them anywhere they wish.

P2E models have blossomed over the last year and some games, such as Axie Infinity, were generating an average income of $400 per month for users in late 2021.   As such, these games have been especially popular in countries with lower incomes, such as the Philippines, where

_____

_____

grandmothers, taxi drivers, teachers, etc… were quitting their jobs because they could earn 2-3x the local minimum wage by playing the games.

Gaming is the third largest NFT category by market value (representing 7% of the market) and second largest by volume (representing 7% of all-time volume).

<u>What are the Benefits of Play-to-Earn games?</u>

Gaming is *big* business. According to <u>NewZoo</u>, there are currently over 3 billion gamers in the world representing nearly $200B in yearly revenue. This makes it the second largest category of entertainment behind TV (and some researchers, such as <u>Bitkraft</u>, believe that this estimate is conservative, and that the gaming industry may be worth nearly $350B). Gaming is also the fastest growing sector in the traditional entertainment market with a CAGR of over 10%.

<u>The Gaming Industry is Expected to Earn Over $250B in Revenue by 2026</u>
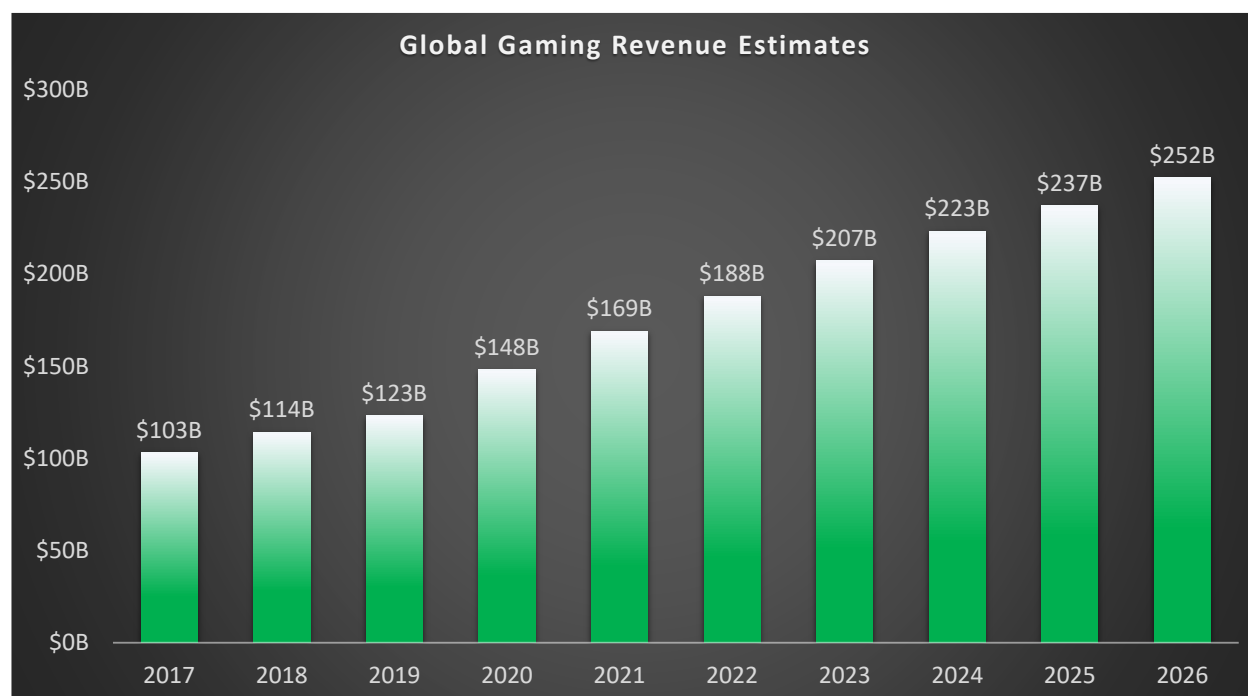
Source: <u>Statista</u>

Some games, such as Fortnite, <u>earn over $5B per year</u>, easily dwarfing most entertainment assets.

Unfortunately, the industry is plagued by a significant issue – it's dominated by a handful of developers such as Sony, Tencent, Nintendo, Microsoft, Activision, Electronic Arts and Epic Games that have full ownership of all in-game content. This creates several problems: i) they control the economics and can prevent users from selling goods, ii) they can revoke access to digital goods at any time and iii) in-game assets are rarely interoperable with other platforms.

NFTs represent a major transformation in gaming because they allow players to earn and retain full ownership over their digital assets. This creates several immediate advantages including:

_____

- **Monetization**: Players can choose to sell, rent or trade their in-game currency, account name, skins, in-game land or any other asset on the open market for real-world cash

- **Facilitation of virtual economies**: Ownership of assets will likely lead to the development of intricate virtual economies, complete with entire financial systems that support asset trading, lending and borrowing, rental, insurance, etc…

- **Reduction in Censorship**: Developers can no longer block or revoke access to a player's assets (ironically, it's been said that Ethereum was created because Vitalik Buterin was mad that World of Warcraft made his wizard less powerful)

- **Interoperability**: Assets will become fully interoperable, meaning that users can freely move them between games. They will also become composable, meaning that they can users can combine assets from different games in unique and interesting ways

- **Programmability**: Since NFTs are essentially software on blockchain networks, users can choose to modify them in any way they see fit. This will likely lead to new and exciting outcomes as players experiment with derivative work and user-generated functionality

As stated previously, these benefits represent a significant evolution over traditional industry models, and have the potential to drive massive growth in Play-to-Earn games

How do Play-to-Earn Games Work?

To understand the mechanics of Play-to-Earn gaming, let's look at the most popular blockchain game, Axie Infinity, which has generated over $4B in sales.

The company was founded in 2018 and it hosts a Pokemon-inspired game that allows players to collect, raise and battle creatures called "Axies". Every Axie is different, has unique strengths and weaknesses and is represented by an NFT.

In order to play, users must purchase three Axies. Although prices have dropped significantly, at the peak of the game's popularity, this could cost users hundreds to thousands of dollars.

_____

<u>A Triplet of Axies</u>
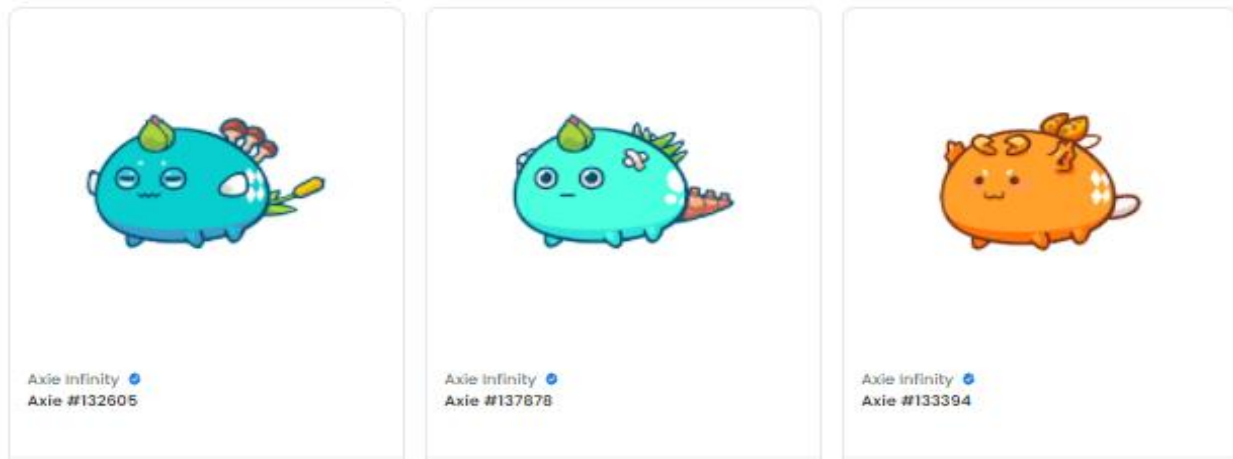
Upon purchasing their Axies, players can use them to:

- **Adventure**: Adventures are a single-player mode where users can battle against computer-controlled opponents to earn Smooth Love Potion (SLP) tokens

- **Battle**:   Battles are direct combat with other players. While victories offer more SLP rewards, they are often generally much harder to obtain.

- **Breed**: Players can breed two Axies to create a baby Axie, which can be trained and eventually used to adventure, battle and breed

Like most games, Smooth Love Potion tokens can function as an in-game currency, and users can spend them to breed new Axies. Unlike traditional games, however, SLP can also be sold for real cash.

Similarly, while the newly bred baby Axie NFTs can be used to play the game, they also can also be sold on the open market.

These avenues for real-world monetization represent a paradigm shift in the gaming industry and form the core of P2E gaming. Indeed, users in the Philippines – Axie's most popular market – reported an average income of $400 per month in late 2021 (more than the average salary for a teacher, construction worker or security guard)

<u>Who are the Key Players in the Play-to-Earn Gaming Industry?</u>

In addition to Axie Infinity, other notable games include Loot, Sorare, Parallel Alpha, Crabada, Farmers World and Zed Run.

_____

_____
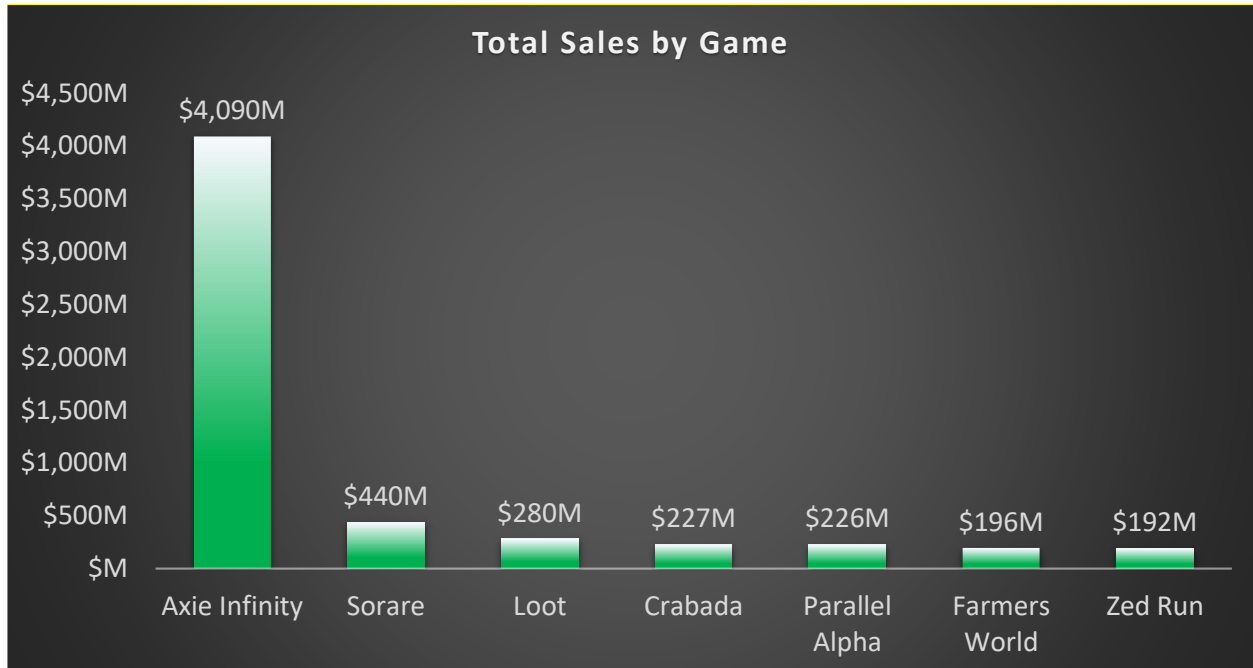
Total Sales by Game

Source: Cryptoslam.io as of 10.2.22

Game	Total Sales ($M)	Description
	$4,090M	Axie Infinity is the largest P2E game with over $4 billion in sales
	$440M	Sorare is a fantasy football (soccer) game that was founded in 2018
	$280M	Loot for Adventurers is not a game per se, but a collection of digital items such as weapons, armor, jewelry, etc… that players can use in other games
	$227M	Crabada is a P2E game on the Avalanche network. Players can collect, breed and battle a collection of ill-tempered hermit crabs from a variety of clans

_____

_____

	$226M	Parallel Alpha is a sci-fi themed card game, where players collect assets and use them to battle other players
	$196M	Farmers World is a social game that allows players to grow, harvest and trade a variety of crops
	$192M	Zed Run is a digital horse racing game that allows players to breed, buy, sell and race their horses

Play-to-Earn Gaming Infrastructure

Perhaps the biggest criticisms of play-to-earn games is that they often require a considerable upfront investment – users may have to purchase hundreds to thousands of dollars in NFTs just to play a game. This creates significant barriers to entry and may prevent wider adoption in some of the space's most lucrative markets.

One company working to solve this problem is a project known as Yield Guild Games (YGG).

Founded in 2020 by Gabby Dizon, Yield Guild is a community-owned co-op that purchases and collects in-game assets, such as NFTs, digital assets, parcels of land, etc… The organization then rents or loans these assets out to gamers, who use them to play the game and earn rewards. As such, the platform earns revenue on the appreciation of the NFTs and also receives a cut of its members earnings.

Yield Guild Games Portfolio of NFTs

_____

Source: Messari as of January 15th, 2022

To maximize revenue, YGG is organized into several smaller groups (for each game or geographic region) that:

- Provide training to new members
- Serve as a forum to share tips, strategies and best practices
- Allow players to work together in-game to collaborate on missions to maximize earnings

YGG is structured as a DAO and co-owned by members through the YGG token. This creates a powerful incentive for all stakeholders to work together to maximize the value of the organization.

To date, the project currently supports multiple games including:

- Axie Infinity
- Ember Sword
- Delta Time
- Guild of Guardians
- Illuvium
- League of Kingdoms
- The Sandbox
- Star Atlas

The organization has over 27,000 members (called "scholars") and is backed by A16Z, Jump Capital and Crypto.com Capital.

Yield Guild is one of the vanguards of an exciting new field known as GameFi – a concept that combines decentralized finance with play-to-earn gaming, making it easier for players to obtain

_____

_____

funding, monetize assets and share earnings. Other notable players in this space include Merit Circle, GuildFi, AvocadoDAO and GameFi.
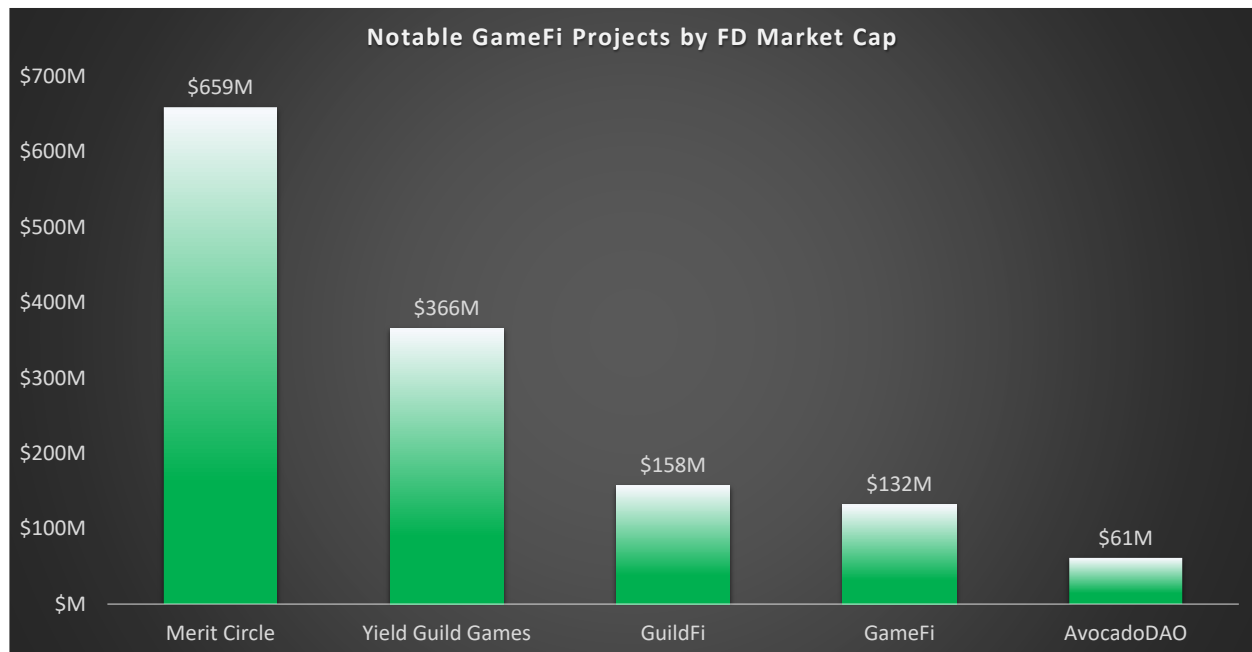
Source: Coinmarketcap as of 10.2.22

Project	FD Market Cap	Description
Merit Circle	$659M	As of 10.2.22, Merit Circle was the largest guild by market cap (recently overtaking YGG). It has 3,750 members, $115M AUM, supports 50 games and has earned over $2M
Yield Guild	$366M	Yield Guild Games is one of the oldest and largest gaming guilds and has historically commanded the highest market cap in the space

_____

_____

	$158M	GuildFi was launched in October 2021 and supports several popular games including Axie Infinity
	$132M	GameFi is backed by Polygon and Animoca Brands
	$61M	AvocadoDAO was launched in 2021 and is backed by A16Z, Solana Ventures, Three Arrows Capital and Polygon Studios. It has 11K scholars and supports 45+ assets

_____

Chapter 30: Social

What are Social NFTs?

Social NFTs grant owners access to exclusive communities, experiences or goods.

While we are still in the earliest stages of development, several potential use-cases for social NFTs are emerging. Some of the more popular proposals include:

- **Social Clubs** (e.g. Country clubs, private members clubs, community organizations)
- **Charities** (e.g. Education, health, environmental)
- **Investment Clubs** (e.g. VC / PE / Hedge Funds, NFT collectors groups)
- **Artist's Guilds** (Film studios, publishers, news organizations, records labels, game developers)
- **Worker Collectives** (e.g. digital unions, talent agencies, consulting firms)

Although the use-cases of social NFTs are broad, most tend to share three important criteria. They are: 1) organized around a single purpose, 2) share a treasury raised from early NFT sales and 3) often structured as DAOs.

The total market capitalization of Social NFTs is ~$200M (or ~1% of the NFT market) but they are poised to grow as a replacement for both in-person social organizations and online, "Web2", social networks.

What are the Benefits of Social NFTs?

Social clubs are obviously not a new phenomenon. For most of history, we've been joining guilds, salons, country clubs, exclusive houses, etc… to gain a host of benefits such as networking, knowledge sharing, status, etc…

Social NFTs are unique in that they allow members to form organizations that retain the advantages of traditional clubs while adding several new features. Because these organizations are often structured as DAOs (which we will discuss more in Part 6), they enable:

1. **Democratic decision-making**: Unlike many legacy organizations, Social DAOs have a flat structure with little to no management hierarchy. Each NFT holder has a vote, allowing the organization to leverage the collective wisdom of the group

2. **Direct economic incentives**: Social DAOs have the ability to create their own native currency. As such, they can directly compensate members who help with sales & marketing, recruiting, operations, financial management, development, community management, etc…

3. **Liquidity:** Many traditional clubs restrict the transfer or sale of membership. Even when permitted, it's generally difficult to find willing buyers or agree upon a fair price.   Social

_____

_____

NFTs, on the other hand, are extremely liquid – they are generally traded on a variety of platforms such as OpenSea and LooksRare, and prices are updated in real-time.

4. **Transparency:** Every vote made and every dollar spent by a social DAO is permanently recorded on an immutable blockchain, making it easy to budget, track spending, detect fraud, audit member contributions and measure performance.

5. **Efficiency:** Although distributed organizations have their challenges, the ability for real-time communication and the automation of processes make DAOs extremely fast. In addition, the elimination of traditional management structures can greatly reduce overhead.

How do Social NFTs work?
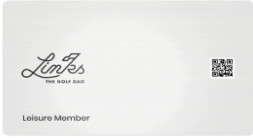
To understand how Social NFTs work, let's look at one of the hot new projects in the space – LinksDAO.

LinksDAO is a decentralized autonomous organization that plans to create a modern version of the country club by selling NFTs to crowdfund the purchase of a Top 100 golf course.

The DAO was founded in 2021 by Mike Dudas (founder, 6th Man Ventures), Jim Daily (president, Teads) and Chris Maddern (co-founder, Button). It raised over $10M in 48 hours through the initial sale of 6,363 "leisure membership" and 2,727 "global membership" NFTs that offer holders rights to purchase membership to the club, governance rights in the DAO and access to golf outings, discounts on tee times, exclusive merchandise, etc….

_____

_____

LinksDAO NFTs

Leisure Membership NFT
6,363 total

Enjoy the perks of LinksDAO including...

✓ The right to purchase a membership at the 1st physical club LinksDAO acquires

✓ Governance rights via $LINKS token, launching in early 2022

✓ Access and discounts on golf tee times, packages, leisure products, merch, and more

✓ Access to members-only Discord channels, including guest appearances by golf, sports, business, and celebrity luminaries

✓ Entry into the LinksDAO fantasy golf league

✓ More to come!

0.18 ETH

Select Quantity

| 1 | ⌄ | **Connect Wallet** |

Global Membership NFT
2,727 total

All the perks of a Leisure Membership plus...

✓ 4x the governance rights via $LINKS token, launching in early 2022

✓ The right to purchase two individual memberships or one family membership at the 1st physical club LinksDAO acquires

✓ Access to official LinksDAO IRL events such as golf outings and trips (first planned event will be in early 2022 at a Major Championship-quality course)

✓ Access to club reciprocity with other Global Members who opt-in to participating

✓ More to come!

0.72 ETH

Select Quantity

| 1 | ⌄ | **Connect Wallet** |

Source: Perfectputt.substack

Purchasing and running a golf course is no small feat, so the company has outlined a detailed roadmap:

- **Early 2022**: Proceeds from the initial offering will be used to build the DAO and organize the community. This includes hiring a Chief DAO officer, location scouts, product & engineering support, marketing personnel and legal, compliance and accounting teams
- **Mid 2022**: The community will identify potential clubs, vote on which one they'd like to acquire and use funds from the treasury to acquire a golf course
- **Late 2022 – Early 2023**: The first LinksDAO club location will open
- **2023 & Beyond**: The community will continue to expand to additional locations, creating a global "country club"

LinksDAO boasts a passionate community – it has over 15K Discord members and has hosted real world events such as a members-only tournament at SXSW. What makes the project especially interesting is that it's expanding the crypto ecosystem by introducing NFTs to the general public (i.e. "normies"). It has a very clear and understandable value proposition – membership to a golf club – and, as such, roughly one-third of the participants in the initial sale were first time NFT buyers.

_____

_____

On May 25th, 2022, LinksDAO announced a partnership with Callaway.

Who are the Key Players in the Social NFT ecosystem?

In addition to LinksDAO, other social NFTs include Squid DAO, Metahero Universe Planet Tokens, Hyperbearsclub, HeadDAO, Crypto Packaged Goods, City DAO Citizenship and IreneDAO.
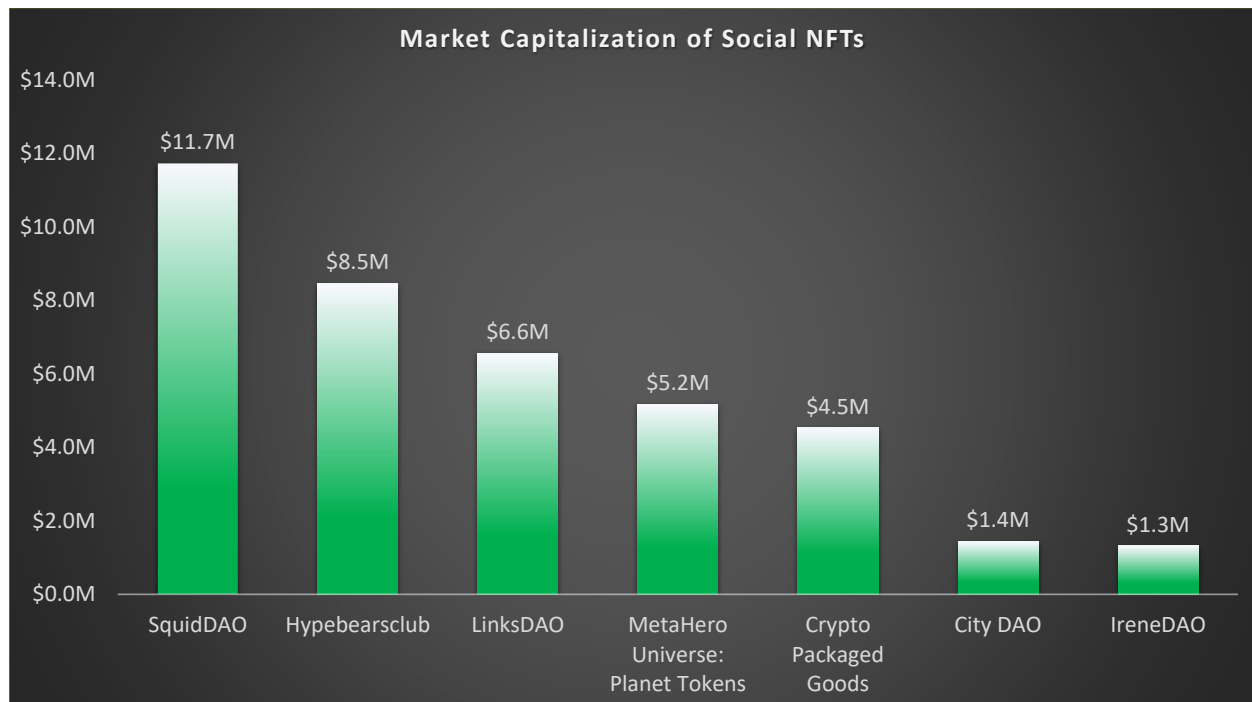
Source: NFTGo as of 10.2.22. While not in the top 10 by market cap, CityDAO and IreneDAO are included for illustrative purposes.

Project	Market Cap	Description
	$11.7M	Squid DAO is a community owned investment club. Owners of the NFT receive a claim on fees generated by the protocol as well as voting power over the ecosystem
	$8.5M	Ownership of Hyperbears – a collection of 10,000 PFPs that provides access to a members-only club with a variety of perks

_____

	$6.6M	Grants membership to LinksDAO, an organization formed to purchase and govern a country club
	$5.2M	Metahero Universe is a hybrid gaming platform and social network inspired by Punks Comic
	$4.5M	The Crypto Packaged Goods NFT provides access to the project's Telegram, which aims to be club focused on the intersection of crypto, consumer and Web3
	$1.4M	DAO organized to purchase and govern a real parcel of land in Wyoming
	$3.4M	Collection of risqué photos from Singapore influencer Irene Zhao. The NFT provides access to her fan club and has a much broader goal of disrupting the influencer and creator economy

Chapter 31: Music

What are Music NFTs?

Music NFTs are certificates of ownership for unique musical pieces such as songs, albums, lyrics and instrumentals. On the surface, they are similar to an audio file that one would purchase on iTunes.

What differentiates music NFTs is that they often offer the holder full ownership of the work and therefore exclusive rights to determine how it is used.

Although the category currently represents fewer than 0.4% of the NFT markets, there have been several notable developments in the last 18 months including:

- March 2021: Kings of Leon becomes the first band to release an album as an NFT
- April 2021: American artist Vérité auctions the perpetual master recording rights for the song "by now"
- October 2021: PleasrDAO purchases the NFT for Wu-Tang Clan's unreleased "Once Upon a Time in Shaolin" for $4 million
- November 2021: Universal Music Group partners with Timbaland to create a Bored Ape band
- December 2022: An unreleased Whitney Houston track sells as an NFT
- January 2022: Nas releases two singles on Royal that grant holders royalty rights
- February 2022: Coachella sells 10 lifetimes passes as NFTs (which were trading at $1M)
- March 2022: Snoop Dogg releases the first Death Row NFT mixtape
- June 2022: Pharrell Williams joins Doodles as its Chief Brand Officer

Given the large global fanbase of music aficionados and numerous developments in the space, many analysts are bullish on the long-term prospects of music NFTs.

What are the benefits of Music NFTs?

Owing to a shift to digital formats and the resulting explosion in piracy, the music industry experienced a steep decline from the early 2000s to 2014. Fortunately, digital and streaming markets matured during this time to stop the bleeding and reverse the trend.

Global Recorded Music Industry Revenues 2001-2019 (US$ Billions)
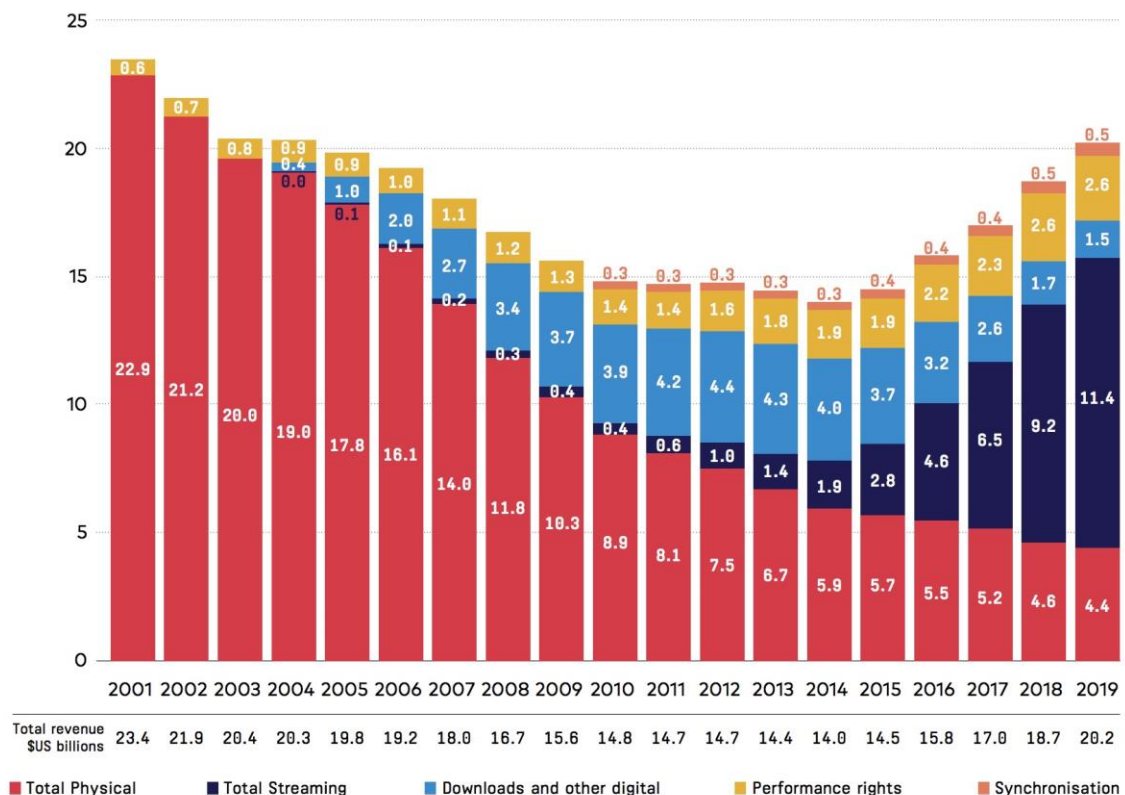
Source: Allaccess.com

Today, over 83% of music sales are streamed and the space is dominated by three players: Spotify (32% market share), Apple Music (16% market share) and Amazon (13% market share).

While these giants have undoubtedly provided value to the industry as a whole, these benefits have come at a heavy cost to artists, who now have yet another stakeholder to pay. Indeed, after the cut taken by distributors and record labels, the average musician only yields ~12% on their works.

Moreover, like any average, this figure is further skewed by the handful of larger artists with negotiating leverage – the typical musician makes much less. According to Venture Beat, the top 1% of artists receive 90% of streaming revenues and fewer than 0.8% make more than $50,000 per year.

_____

Recording Artists Capture Fewer Than 12% of Music Revenue
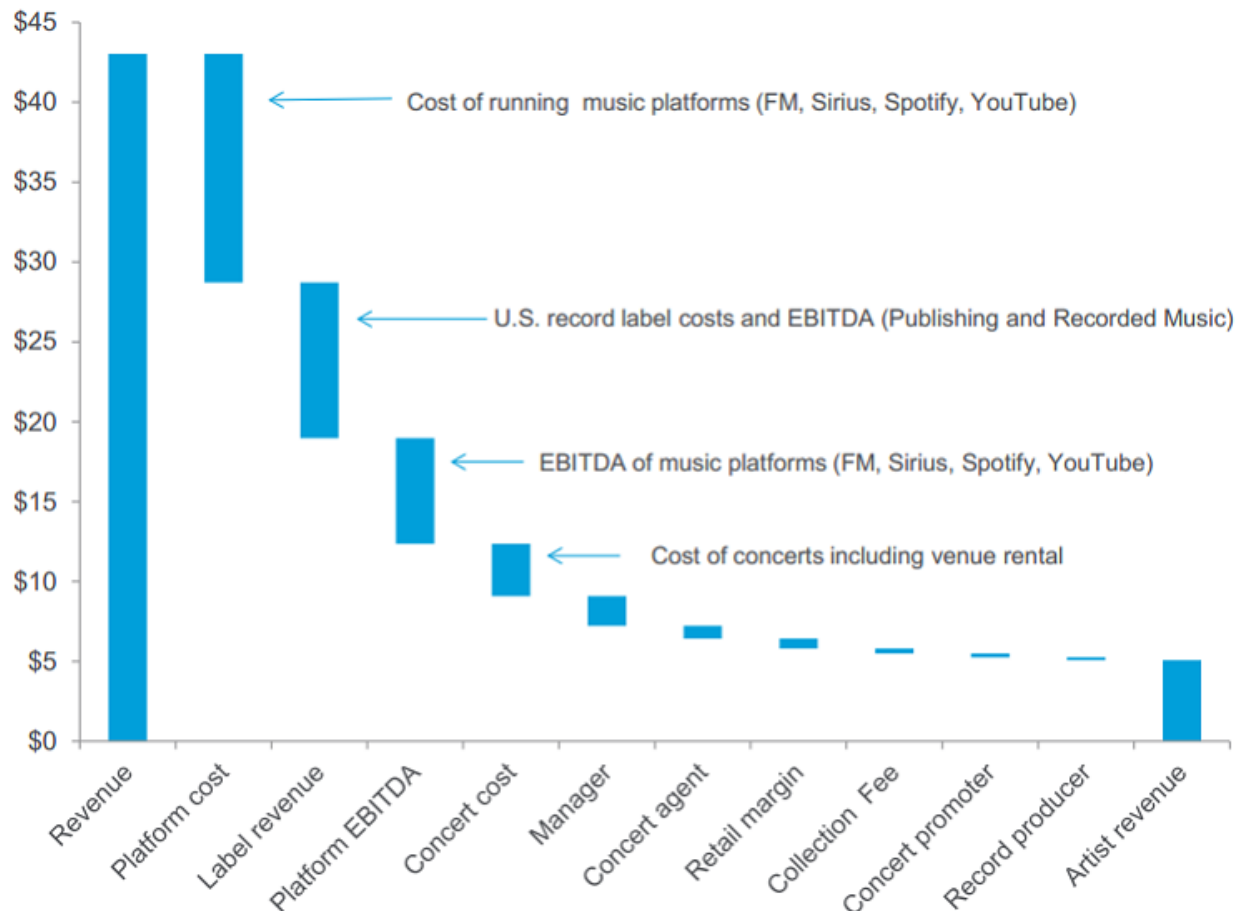
Source: CitiResearch, RIAA, Company Reports via Digital Music News

NFTs can buck this trend by cutting out the middleman and allowing artists to sell directly to consumers. This means the elimination of platforms, record labels and publishers – potentially increasing the artist's share to 90%!

In aggregate, Bankless estimates that selling music NFTs could yield an artist 7.5x more earnings than a year's worth of streaming on Spotify.

Music NFTs also offer substantial economic benefits to consumers. For instance, an artist could create an NFT of her work, sell it directly to fans who then could collect royalties every time the work is streamed.

In addition, music NFTs will likely improve the overall function music industry as they offer:

- **New Streams of Revenue**: Music NFTs will likely create the potential for an entirely new suite of products including digital memorabilia (such as Snoop Dogg's "Doggies"), NFT-based album art, concert tickets with perpetual royalties and collaborative works

_____

_____

- **Enhanced Consumer Benefits**: Owning music NFTs could entitle fans to exclusive access to parties, special shows, 1-on-1 interactions with artists and more

- **Irrefutable Provenance**: Musical works often have several owners and the details of these owners can be spread across dozens of physical contracts. Recording ownership on a blockchain eliminates this confusion and establishes a clear record of ownership

- **Transparency**: The current system for royalties is opaque and inefficient. NFTs make it easy to see who has streamed what and calculate payments accordingly

- **Censorship Resistance**: From Elvis to the Rolling Stones to N.W.A, censorship of music has been a long-standing problem. Decentralized platforms have the potential to eliminate censorship by allowing artists to upload any content, any time they want, no matter how controversial

Finally, Music NFTs will likely increase the incentives for collaboration between an artist and her fanbase. For instance, users could gain economic benefit from creating derivative works and remixes, or even building decentralized applications that incorporate a piece of work.

How Do Music NFTs work?

Explaining the mechanics of music NFTs is difficult because there are so many different types of assets.

Despite being only a few years old, we have seen several major categories emerge that include:

- **Digital Works:** Albums, songs, lyrics, etc… that have been made into an NFT

- **Generative Music:** Music that is created by computer algorithms, such as EulerBeats

- **Collaborative Works:** Although all music NFTs can be theoretically modified, remixed and sold, some – such as Snoop Dogg's "Dogg on it: Death Row Mixtape Vol. 1" – are designed specifically with this purpose in mind

- **Merchandise:** Including album art, special editions, digital avatars

- **Live-Event Tickets:** Concert tickets that can be programmed to include access to merchandise, food and beverages, etc…

Let's take a deeper look into each of these use-cases below…

Digital Works

One of the first, and most basic, iterations of music NFTs are as simple digital collectibles.

_____

_____

Artists can leverage the technology to create scarce digital representations of albums, songs, lyrics and even soundbites and sell them to superfans who are eager to collect these limited editions.

Although many music NFTs don't currently offer ownership or royalty rights, some platforms – such as Royal – are pioneering a new model that gives fans an economic stake in the works.

In January 2022, Nas raised over $560K in revenue selling royalty rights to two singles – "Ultra Black" and "Rare" – on Royal.

<u>Ownership of Nas's "Rare" Grants Holders up to 1.6% of the Song's Royalties</u>
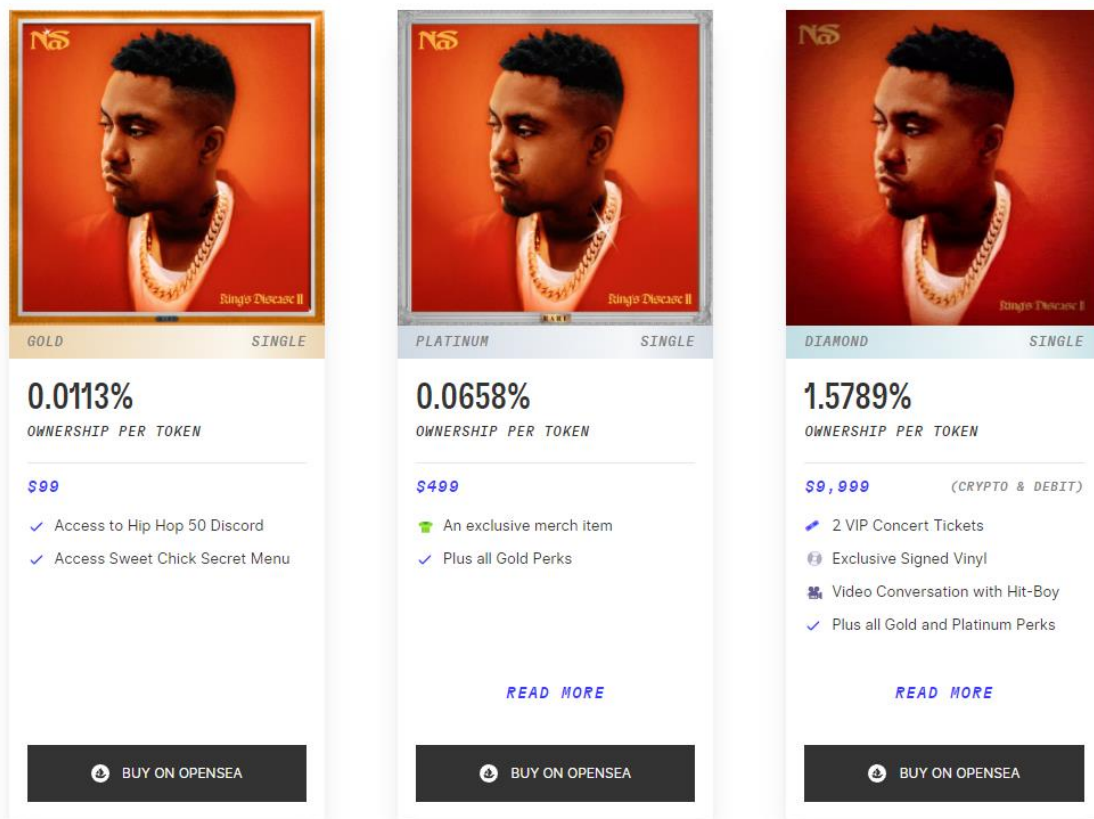
Source: Royal

Each NFT gives the buyer a percentage of streaming royalties for the song, ranging from 0.0133% for the "Gold" edition (~$99) to 1.5789% for the "Diamond" edition ($9,999). In addition, ownership of the NFTs comes with several additional perks that may include:

- Access to an invite-only Discord channel
- Exclusive merchandise
- VIP Concert Tickets
- Exclusive Signed Vinyl
- Video Conversation with Hit-Boy

_____

The collection consisted of 1,870 NFTs and sold out almost immediately, generating over $560K in revenue.

<u>Generative Music – EulerBeats</u>

Generative music is the recording industry's answer to Art Blocks. Like generative art, it is created by computer programs and random factors are introduced into the code to make each track unique.

EulerBeats is one of the earliest iterations of this new art form. It is a collection of 27 original tracks that are algorithmically generated using the Euler Phi function. Each track comes with 120 copies and its own unique digital album cover.

<div align="center"><u>EulerBeats Tracks</u></div>
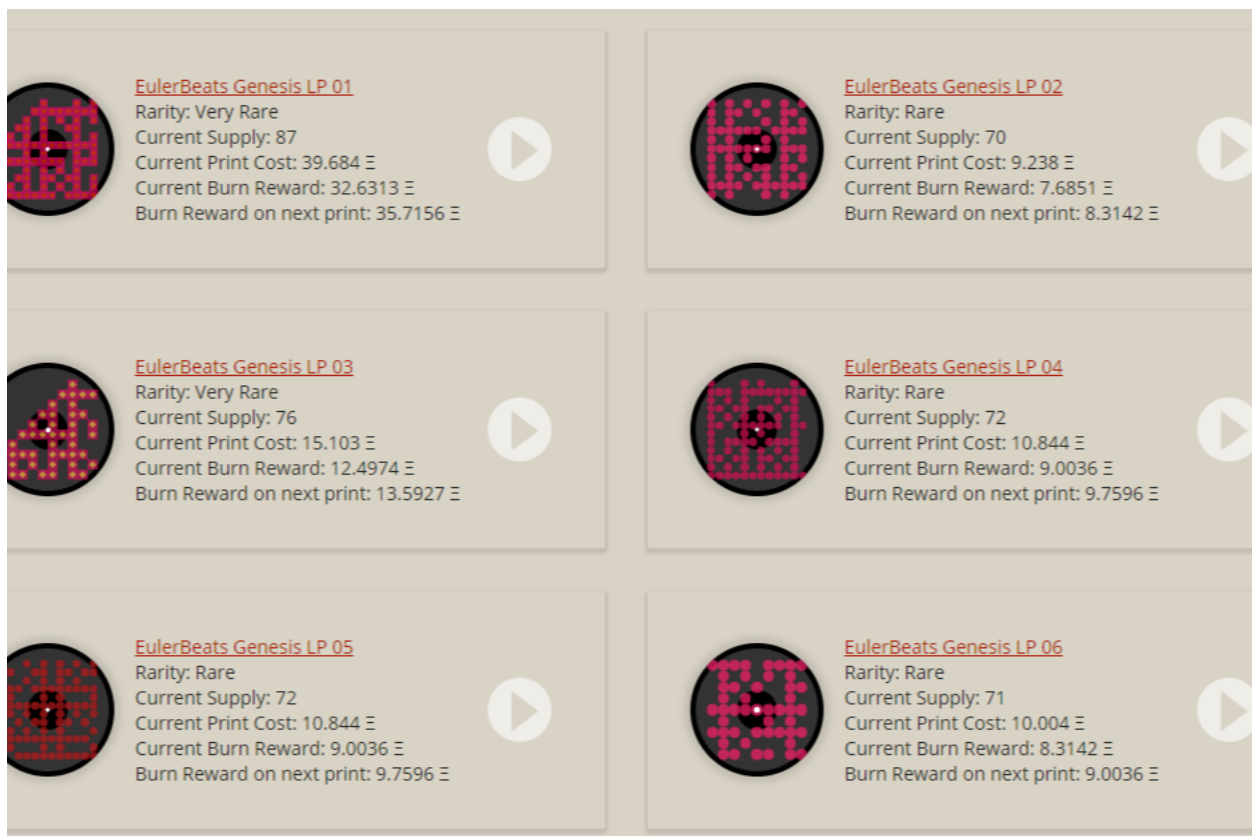
<div align="center">Source: <u>DappRadar</u></div>

Holders of EulerBeats own the full commercial rights to the music and receive an 8% royalty on every copy sold.

One interesting feature of EulerBeats is that all data (artwork + music) is stored entirely on-chain. Unlike other NFTs, which require third-party servers to host their content, EulerBeats will exist forever on the Ethereum blockchain.

_____

Collaborative Works – Snoop's Mixtapes

Another emerging category of music NFTs is collaborative works. Although most NFTs allow users the right to modify and sell derivative works, some are specifically created for this purpose.

One recent example is Snoop Dogg's "Dogg on it: Death Row Mixtape Vol. 1". Each NFT contains four audio files including:

- Vocals only
- Instrumentals only
- Instrumentals and hook, but without the verses
- The complete song

As such, purchasers have numerous options to create derivative works – such as creating their own instrumentals to go along with the vocals, using the instrumental to create their own rap or remixing the song in anyway they desire.

While it's unclear at this time whether users will be able to sell these derivatives (and if they'll have to provide royalties to Snoop), the ability to do so would be consistent with the NFT ethos. In fact, the description reads "Own it. Remix it. Master it."

Merchandise

The global market for music merchandise is nearly $4 billion, and it is estimated that artists often earn up to 35% of their income peddling hats, t-shirts, sneakers, etc…

_____

NFTs have the potential to expand this revenue base by allowing artists to monetize *digital* merchandise as well, selling limited edition album art, collectible editions, avatars, etc…

Once again, Snoop Dogg is a pioneer in this space, with multiple releases including:

1. Doggies: 10,000 programmable and playable avatars intended for use in the metaverse
2. Snoopverse Early Access Passes: Exclusive access to the "Snoopverse", the artist's own branded world within The Sandbox
3. Stash Boxes: "Goody" boxes that include a variety of random items such as music tracks, commemorative NFTs and even metaverse land parcels

<u>Snoop Dogg's "Doggies"</u>

Source: The Sandbox

Tickets

One particularly interesting use-case for NFTs is ticketing for concerts and other live music events.

We are already seeing traction in this area, artists Lupe Fiasco and Gucci Mane have sold blockchain-based tickets, and Coachella recently sold 10 lifetime passes (with VIP access) in the form of NFTs that are currently retailing for more than $1M on the secondary market.

_____

_____

$1M NFT Ticket for Lifetime VIP Access to Coachella

Source: Coachella NFT Marketplace

NFT tickets have several benefits including:

- **Less Counterfeiting:** It is estimated that up to 20% of second-hand tickets are fakes. NFTs could eliminate this problem by allowing purchasers to independently verify a ticket's legitimacy

- **Resale Potential**: NFTs can be coded to give an artist a percentage of every ticket resale, granting artists access to a multi-billion dollar market that has historically been dominated by scalpers

- **New Revenue Opportunities:** Tickets can be programmed to come with free food, drinks, concert merchandise, etc…

_____

_____

While the potential use-cases for NFT ticketing are vast and only beginning to emerge (it probably warrants an entire article) it is becoming clear that they are poised to disrupt the $25 billion live-music ticketing industry.
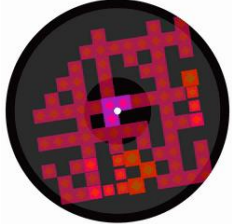
Who are the Key Players in the Music NFT Space?

As of October 2nd, 2022, the top selling music NFTs include WVRPS by Warpsound, The Orbs by BT, EulerBeats Genesis, EulerBeats Enigma, Kingship, Stickmen Toys, Audioglyphs, Dogg on it: Death Row Mixtape Vol. 1 and Snoop Dogg's B.O.D.R.
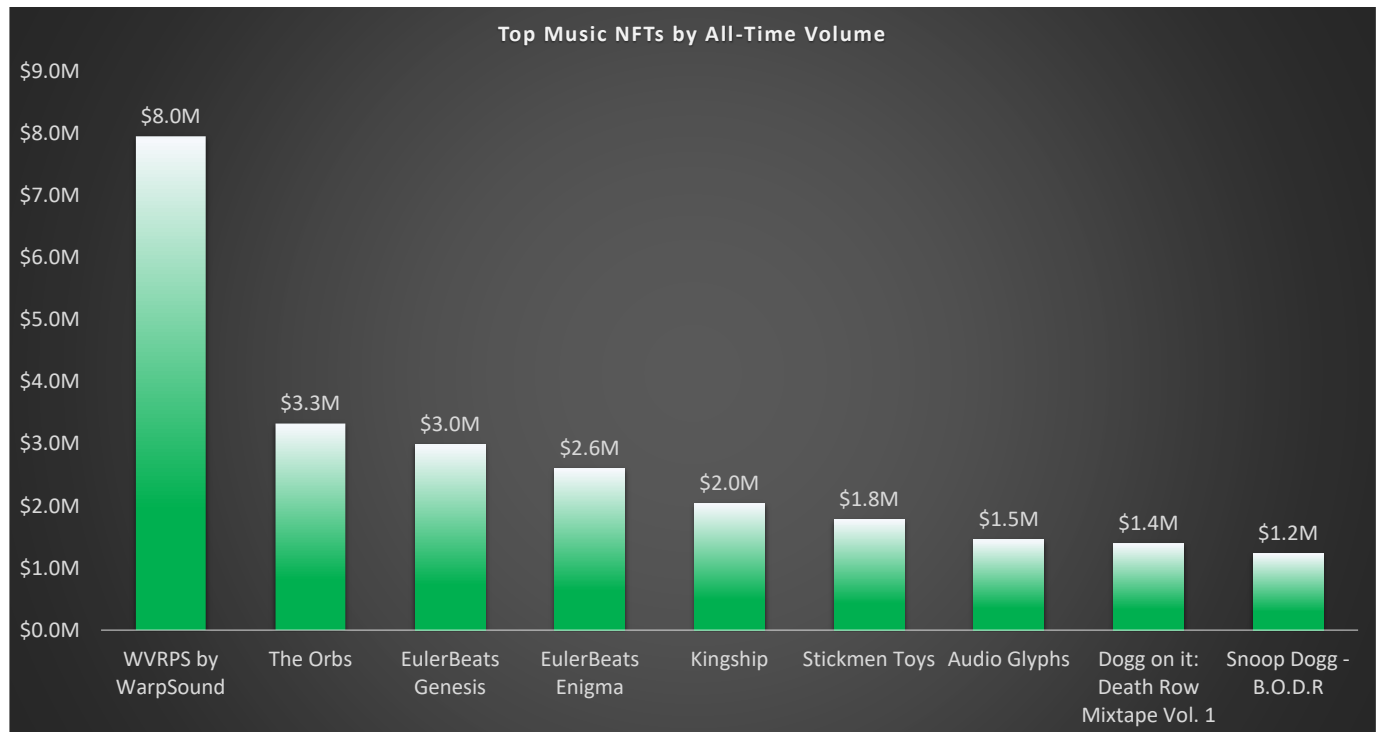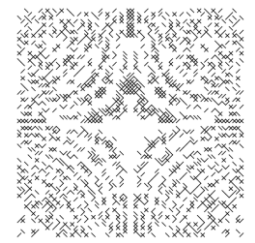
Source: OpenSea as of 10.2.22

Name	Image	All-Time Volume	Description
WVRPS by WarpSound		$8.0M	WVRPs are a hybrid generative PFP and piece of AI-composed music
The Orbs by BT		$3.3M	Collection of 3,333 audio-visual NFTs
EulerBeats Genesis		$3.0M	The original collection of EulerBeats consisting of 27 original tracks
EulerBeats Enigma		$2.6M	EulerBeat's second collection, 27 tracks generated from Euler's totient function

_____

Kingship		$2.0M	A collection of 5,000 NFTs that provides access to music, excusive content and token-gated experiences for the band "Kingship" (a group consisting of three Bored Apes and one Mutant Ape)
Stickmen Toys		$1.8M	A collection of 5,000 audio-visual NFTs from Warner Records UK and Bose
Audioglyphs		$1.5M	Collection of 10,000 NFTs that generate a unique, infinite stream of music
Dogg on it: Death Row Mixtape Vol. 1		$1.4M	Track of beats, a capellas and full songs from Snoop Dogg, designed to be remixed and fully owned by the user
Snoop Dogg - B.O.D.R		$1.2M	Collection of audio files and merchandise NFTs from Snoop Dogg's latest record

_____

Music NFT Infrastructure

Like the traditional music industry, infrastructure such as streaming services and marketplaces will be critical to the success of music NFTs.

One of the most popular infrastructure plays today is a project known as Audius.

Founded in 2018 by Forrest Browning, Ranidu Lankage, and Roneil Rumburg, Audius is a decentralized music streaming platform built on the Ethereum blockchain (in many ways it's similar to Spotify or SoundCloud).

Unlike traditional streaming services, however, the platform does not charge a fee – allowing artists to earn 90% of revenue vs. 12% on Spotify! (the remaining 10% goes to miners on the Audius Network)

<u>Artists Can Earn Nearly 8x More Using Audius</u>

Spotify

88% Spotify Platform Fee
Major Record Labels Cut
Back Office Services

12% Artist Share

Audius

10% Network Operators

90% Artist Share
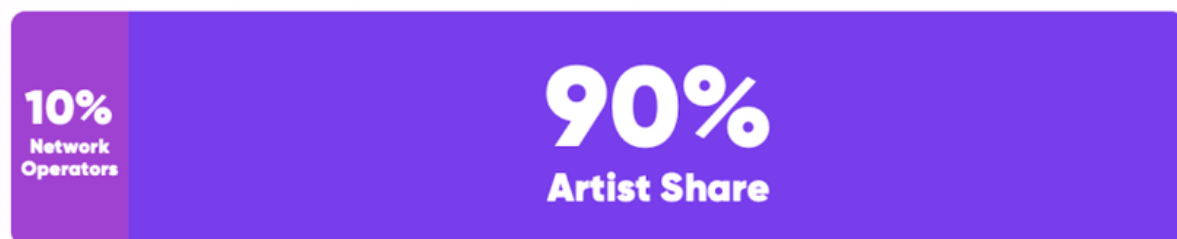
Audius Takes 0% of Streaming Revenue

Source: [Audius via Twitter](#)

The backbone of the Audius platform is a decentralized storage system known as AudSP (which is an extension of IPFS).

_____

In this system, artists upload their songs and then the data for each song is split up and stored across a global network of computers called content nodes. When a user wants to stream a song, these pieces are sent back to the user and reassembled.

Audius also employs another type of node – known as a discovery node – that indexes the AudSP ledger and makes it easier for users to find songs.

The platform is powered by the native ERC-20 token AUDIO, which provides:

- Security: Both content and discovery node operators are compensated with AUDIO, receiving up to 10% of the platform's revenue
- Staking: Artists and users can get premium features by staking the token
- Governance: Tokens grant governance rights, allowing holders to make proposals, participate in strategy and vote on important issues affecting the platform

As of December 2021, Audius hosted over 100,000 artists and 6 million monthly users.

While still early, the music infrastructure space is booming. Other notable decentralized streaming services include Emanate, Opus and BPM. In addition, there are also several music-specific NFT marketplaces such as Catalog, Royal, Decent and Sound.xyz.

_____

_____

Chapter 32: Intellectual Property

What is NFT IP?

In the NFT world , "IP" refers to the recording of intellectual property rights – such as patents, trademarks, copyrights, goodwill, internet domain names, customer lists, employment contracts, etc… -- on a blockchain.

Although this is one of the smallest categories of the NFT market at 1.4% or ~$329M, it has enormous potential given the value of IP in the United States alone is estimated at over $6 Trillion.

Why is tokenizing IP important?

For most of human history, our most valuable assets have been "tangible" – physical goods that we could use to create value. This includes everything from the earliest tools, to equipment in the first factories to the complicated manufacturing machines we use today.

With the advent of the internet and resulting transition to a service-based economy, however, "intangible" assets (e.g. patents, brand names, contracts, etc…) became more valuable. Indeed, intellectual property now represents over 90% of the market value of the S&P 500.

Intuitively this makes sense -- the brand name of Nike is much more valuable than any machine, and rights to Spiderman, Batman or Baby Yoda are much more valuable than almost any piece of real estate.

COMPONENTS *of* S&P 500 MARKET VALUE

Year	Tangible Assets	Intangible Assets
1975	83%	17%
1985	68%	32%
1995	32%	68%
2005	20%	80%
2015	16%	84%
2020*	10%	90%

SOURCE: OCEAN TOMO, LLC INTANGIBLE ASSET MARKET VALUE STUDY, 2020
*INTERIM STUDY UPDATE AS OF 7/1/2020

_____

_____

Source: [Messari](#)

Unfortunately, the legal frameworks surrounding the creation and enforcement of intellectual property rights have not caught up with the technology and rely on armies of lawyers and paper contracts to track ownership, determine rights and facilitate payments. This creates a system that is expensive, opaque, difficult to enforce and illiquid.

NFTs provide an opportunity to turn intangible intellectual property such as patents, trademarks copyrights and even employment contracts into programmable assets that are stored on a blockchain. This will likely create dozens of new uses cases for IP and greatly improve the efficiency of the market.

Indeed, tokenizing IP can lead to:

- **Lower Costs:** Creating the contracts to record intellectual property rights often requires a team of lawyers and enforcing them relies on an entire industry. Recording IP rights on a blockchain, however, is instant and greatly reduces the need for intellectual property contracts and lawyers, making transactions much cheaper

- **Irrefutable Provenance:** There's no standardized database that records all the owners of a piece of intellectual property to ensure everyone is paid. In addition, even if one can find the owners of a piece of IP, ownership percentages and rights are often recorded across dozens of contracts (or not recorded at all), making them difficult to track. Tokenizing IP can create an a unified, immutable log of all stakeholders, making it easier to ascertain exactly who owns what and how much they should get paid

- **Ease of Use:** Licensing approvals can be automated, allowing holders to instantly grant permissions to users who agree to preset terms and conditions. Payments can also be streamlined with subscription models or smart contracts that execute automatically when certain conditions are met

- **Contract Standardization:** Global intellectual laws for IP are relatively weak and inconsistent. For instance, it's quite difficult for a Western company to combat pirated software in China, India or Brazil, and the opposite is often true as well. With NFTs, there is no need to rely on third-party legal systems to enforce these laws, because all rules are encoded in the blockchain itself and executed via smart contracts (as they say in cryptoland, "code is law")

- **Liquidity**: There is no market for intellectual property, and it can only be valued by appraisals (which are costly and inaccurate) or corporate acquisitions (which are infrequent). NFTs allow for the create of "IP markets", where things such as patents, copyrights, trademarks, brand names, etc… can be traded in real-time

_____

_____

Chapter 34: Other NFT Applications

While tech and entertainment may provide some of the earliest use cases for NFTs, their utility does not end there. Indeed, there are almost infinite potential uses for the technology, including:

1. **Consumer Products:** NFTs can verify that products are legitimate and verify their origin

2. **Fashion:** Your avatars in the metaverse are going to need clothes! Adidas has already created a collection specifically for the Bored Ape Yacht Club

3. **Real estate:** NFTs could be used to provide proof of ownership, transfer deeds and even track changes in property values over time. Real estate could even be "tokenized" with NFTs, allowing commercial properties or apartment buildings to sell their assets to multiple parties

4. **Events and ticketing:** Tickets will likely be replaced by NFTs in the near future, reducing issues related to fraud and paper usage

5. **Healthcare:** NFTs can store immutable medical records without compromising confidentiality

6. **Digital Identity:** Birth certificates, passports, driver's licenses, etc… can all be made into NFTs

7. **Academic Credentials:** NFTs can provide a record of degrees earned, verify attendance and classes taken and a provide a record of performance

8. **Supply Chain:** Companies could track their products, from manufacturing to shipping to delivery with NFTs

9. **Advertising:** NFTs could be used to track the performance of a specific ad campaign, providing an immutable record of performance and reducing the threat of ad fraud (which is a ~$70M per year problem)

10. **Energy:** Companies could use NFTs to track energy usage and trade carbon credits

This is just the tip of the iceberg as almost any physical asset can leverage NFTs to verify ownership, establish provenance, prove authenticity, maintain immutability, and conduct decentralized transactions.

_____

_____

Chapter 35: NFT Infrastructure

In addition to the digital assets themselves, the NFT ecosystem is empowered by several key pieces of infrastructure including:

- **Smart Contract Platforms**: Decentralized computers, such as Ethereum, that create, store, and facilitate the exchange of NFTs

- **Rollups:** Protocols that are designed to increase the efficiency and affordability of smart contract platforms

- **Storage Providers**: Decentralized protocols such as Arweave and Filecoin that host the artwork, audio files, video files, etc… that constitute NFTs

- **Marketplaces**: Platforms such as OpenSea that allow users to buy and sell NFTs

- **Wallets**: Hot wallets such as Metamask that store NFTs and allow access to marketplaces and other dApps

We will cover many of these tools in more detail in Part 7: Web3 Infrastructure, but I'd like to highlight a few now due to their unique position in the NFT space.

Smart Contract Platforms

Smart contract platforms are the computers that run the entire NFT ecosystem, allowing users to create, store and trade digital assets.

We've already covered smart contract platforms in Part 3, so I won't go into much more detail here. That said, it's important to highlight that the prominent Layer 1s operating in the NFT ecosystem are a bit different from the general market.

For instance, while Cardano, Polkadot, Tron and NEAR are top 10 in market cap, they have little to no presence in the NFT space. In addition, many platforms that are popular in DeFi, such as BSC and Avalanche, have only recently started to grow their NFT sales.

As of May 2022, the largest smart contract platforms by Total NFT sales are Ethereum, Ronin, Solana, Flow, Polygon, Wax and Avalanche.

_____

_____

Ethereum Leads the Market with over 75% of NFT Sales
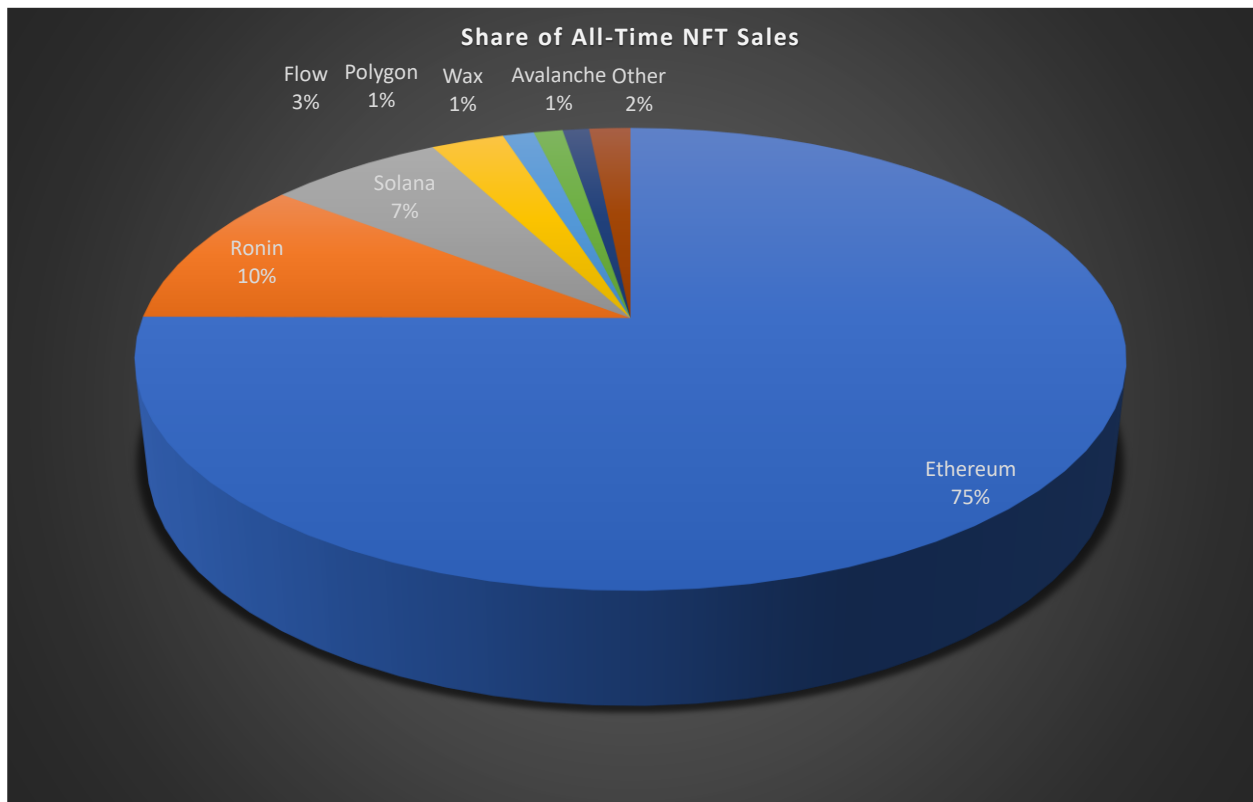
Source: Cryptoslam as of 10.2.22

Protocol	NFT Market Share	Description
ethereum	75%	Ethereum is the undisputed king of NFTs with a total market share of 73%
Ronin	10%	Ronin is the native blockchain for the game Axie Infinity

_____

SOLANA	7%	Solana is a single-chain protocol who boasts the fastest speeds (>50,000 TPS) and lowest fees (<$0.00025) of any major smart contract platform.
flow	3%	Flow is the native blockchain of NBA Top Shot
polygon	1%	Polygon is the most popular side chain on Ethereum
WAX	1%	WAX is a carbon neutral blockchain focused on specifically on NFTs
AVALANCHE	1%	One of the largest chains in DeFi, Avalanche has been making recent inroads into the NFT market

_____

Once again, smart contracts platforms are not only extremely important to NFTs, but also serve as the foundation for DeFi, DAOs and the decentralized economy as a whole. As such, I'd highly recommend rereading Part 3 if you're not fully up to speed on how they work.

Marketplaces

What are Marketplaces?

Marketplaces are online platforms that allow users to buy, sell, create, display and trade NFTs.

At the time of writing, most NFT marketplaces are decentralized, which means that users make transactions directly on a blockchain. As such, the user interface is different from a centralized service such as Coinbase and requires a:

- **Crypto wallet**: Wallets are needed to store cryptocurrencies, connect to a blockchain and make trades

- **Cryptocurrencies**: Most NFTs are priced in cryptocurrencies, such as ETH, instead of dollars. As such, users need to hold them

- **Account**: Like a traditional website, users must set up an account on the platform (although unlike a traditional website, they can be anonymous)

Because these marketplaces interact directly with an underlying blockchain, users must pay gas fees in addition to platform fees.

How do NFT Marketplaces work?

OpenSea is the dominant marketplace for NFTs. The company was founded by Devin Finzer and Alex Attalah in 2017 and is backed by several notable investors including A16Z, Michael Ovitz and Ashton Kutcher.

Currently, OpenSea has more than 2 million active users who generated an average of $2B in monthly volume over the last year (with a peak of $4.9 billion in January). The platform supports the Ethereum, Polygon, Klaytn and Solana blockchains and hosts over 50 million NFTS across a variety of genres including art, virtual land, music, gaming assets, collectibles, social tokens, domain names and many more.

OpenSea's Average Monthly Volume is Over $2 Billion

_____

OpenSea Monthly Volume
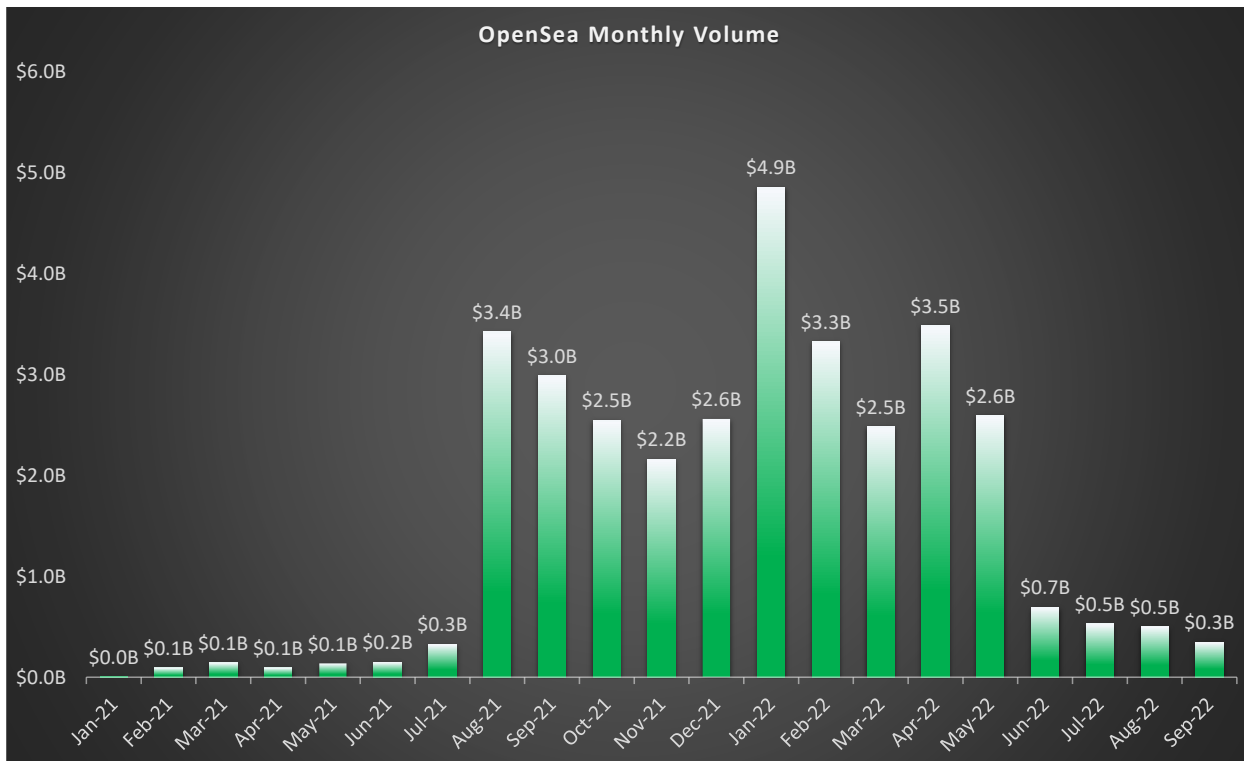
Source: Richard Chen (@RChen8) via Dune Analytics.

So how exactly does OpenSea work?

While it's easy to imagine that marketplaces such as OpenSea hold your assets, initiate transactions and transfer payments between users when they buy and sell – like a crypto equivalent of eBay – this is not what actually happens.

Instead, Open Sea is "non-custodial" which means that it **DOES NOT**:

1. Store Assets: NFTs are stored on a blockchain
2. Initiate Transactions: Permissions are given to the smart contract platform directly through a user's wallet
3. Transfer Payments: Transactions are done and assets are transferred via smart contracts on the blockchain

Instead, OpenSea serves two functions: 1) it provides a graphical display that allows you to *look* at what's already on the blockchain and 2) it acts in a manner similar to a broker, relaying your desires to a smart contract platform such as Ethereum. To accomplish the latter, they allow consumers to use one of their pre-made smart contracts (via their "Wyvern Protocol") to tell a blockchain to list an asset, buy an asset, sell an asset, create an asset, etc…

_____

For example, let's say Alice wants to list her BAYC for 100 ETH through OpenSea:

1. Alice has shared her public address with OpenSea, so they can read the Ethereum blockchain to see that she owns Bored Ape Yacht Club #0001
2. As such, OpenSea will display the image of that ape on their website, along with a big button that says "list for sale"
3. When Alice is ready to list, she pushes that button and chooses 100 ETH as the price
4. OpenSea then writes a smart contract to Ethereum that says "sell this NFT if anyone offers 100 ETH or more".
5. Alice must approve this contract through her wallet
6. Once live, anyone who wishes can see that listing on the Ethereum blockchain (whether they are viewing it through OpenSea or another marketplace) and write a smart contract to pay 100 ETH
7. Once purchased, the Ethereum network transfers the asset from Alice's address to the buyer's address (and transfers 100 ETH in the other direction)
8. Now, when Alice views OpenSea, she will no longer see the Bored Ape, because it is no longer connected to her address. The buyer, however, will (although he will now have 100 fewer ETH in his wallet).

So while OpenSea makes this all very simple to do, in practice they're actually not doing much more than letting you use one of their pre-written smart contracts (and charging you 2.5% in return).

If this sounds critical of OpenSea, that was not my intent. While the platform does have its detractors, it offers a strong user interface and its smart contracts are generally quite well-formed and "battle-tested".

Perhaps that's why it generates an estimated $1B+ of revenue per year and recently achieved a valuation of over $13B.

<u>Key Players</u>

While OpenSea is the dominant marketplace with 66% of all-time volume, there are a few other notable players including Axie Infinity, CryptoPunks, Magic Eden, LooksRare and NBA Top Shot.

_____

OpenSea Controls 66% of All-Time NFT Marketplace Trading Volume

Share of All-Time NFT Transaction Volume

- NBA TopShot 2%
- LooksRare 3%
- Magic Eden 3%
- CryptoPunks 6%
- Axie Marketplace 9%
- Other 11%
- OpenSea 66%
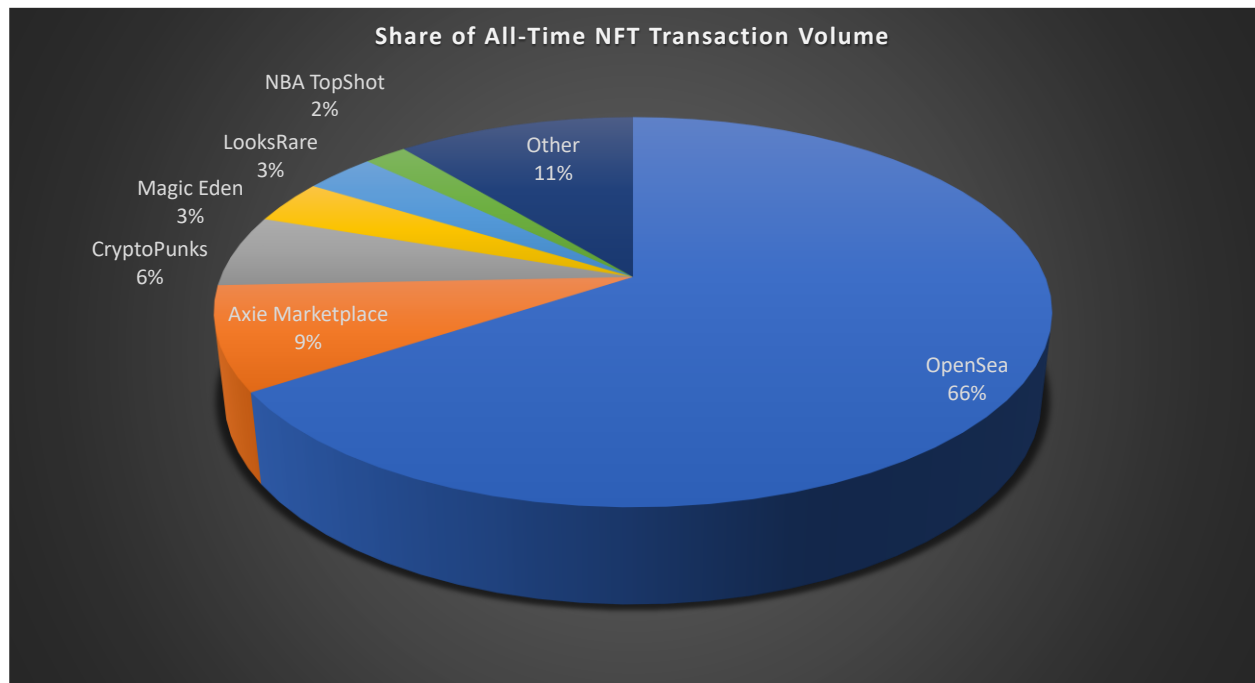
Source: DappRadar as of 10.2.22

Marketplace	Market Share	Description
OpenSea	66%	OpenSea is one of the oldest and most popular NFT marketplaces, commanding over 66% of all-time volume
Axie Infinity	9%	The native marketplace for assets of the game Axie Infinity
CryptoPunks	6%	CryptoPunk's native marketplace

_____

_____

	3%	Magic Eden is the leading marketplace on Solana
	3%	LooksRare is another generalized marketplace that launched in January 2022 through a "vampire attack" on OpenSea
	2%	Native marketplace for collecting and trading NBA Top Shot's NFTs

_____

Chapter 36: NFT Financialization

What is NFT financialization?

One major limitation to NFTs is that – like physical assets such as traditional art, baseball cards, sculptures, etc… – they aren't very liquid.

Fungible assets such as the US dollar, Ethereum or Bitcoin are extremely liquid because they have tens of thousands of potential buyers and, as such, can be quickly traded on almost any marketplace. Unfortunately, non-fungible assets do not have that luxury because – by definition – they are one-of-a-kind.

As such, whether you are selling a Picasso, Rodin, Honus Wagner baseball card, X-Men #1 or Mutant Ape Yacht Club #26044, you need to find a single buyer who wants to purchase your particular piece.

Fortunately, NFTs offer several paths to liquidity – some of the more common are:

- **Borrowing and Lending:** Platforms such as NFTFi allow NFT holders to use their asset as collateral to borrow money, while other platforms allow users to rent their NFTs to others. While renting NFTs may sound strange at first glance, it's quite common in Play-to-Earn gaming where purchasing the assets required to play some games can cost hundreds to thousands of dollars

- **Licensing**: Like art, music or intellectual property, NFTs can be licensed. For instance, a user could pay to stream a music NFT and the holder of an avatar such as a Cryptopunk could charge a royalty to Taco Bell for its use in a commercial

- **Fractionalization**: Platforms such as Fractional allow NFT holders to issue tokens that represent their asset and sell these tokens to multiple users

The added benefit of these strategies is that they allow users to continue to hold the underlying asset while reaping the financial rewards.

Let's take a deeper look into each of these categories…

How does NFT financialization work?

Borrowing and Lending

A popular way to obtain liquidity from NFTs is by using them as collateral for a loan.

NFTfi is a platform that facilitates this: offering borrowers the ability to get liquidity from their NFTs and lenders the ability to earn an attractive yield (and, in the case of default, acquire assets at steep discounts).

_____

_____

Process of Obtaining a Loan through NFTFi
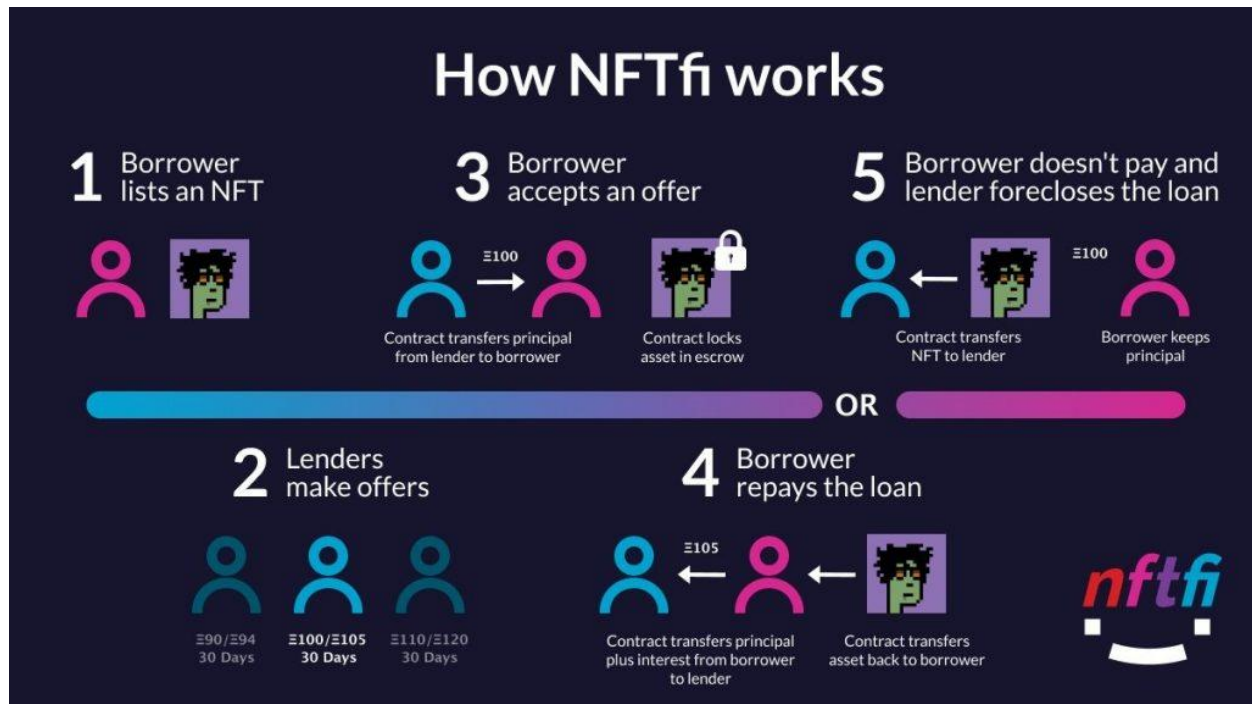
Source: NFTfi

NFTfi is completely decentralized and operates in a trustless, peer-to-peer manner. To obtain a loan:

1. Borrowers upload their NFTs as collateral on the NFTfi platform
2. Once listed, the asset appears in the marketplace, allowing anyone on the site to view it
3. Lenders can make offers with a specific loan amount, duration and interest rate
4. If a loan is accepted, funds are distributed to the borrower and the NFT is transferred to a smart contract to be held in escrow
5. Upon repayment of the loan, the borrower will receive his NFT back. If he defaults, the NFT is transferred to the lender (often at a steep discount).

NFTfi currently supports 100 assets and is constantly adding more.

Licensing

Another way to obtain liquidity from NFTs is by licensing the intellectual property to third parties.

While there are thousands of law firms and talent agencies that can assist with this process, Universal Music Group has shown early interest in the NFT space through its Web 3 label known as "10:22PM".

Founded by Celine Joshua in 2018, 10:22PM unit is responsible for "discovering, developing and empowering artists, digital creators and brands".

_____

_____

While the market for NFT licensing is just getting started, the unit has already inked a deal to create a virtual band known as Kingship.

Kingship is comprised of four Bored Ape Yacht Club apes (three "OG" apes and one mutant) owned by noted NFT collector Jimmy McNelis. Like Gorrilaz – the groundbreaking virtual band from the 90s who sold over 26 million records – the group hopes to combine UMGs connections and know-how in the music space with the popularity of the BAYC brand to become a top-selling ensemble.

<u>Could Kingship be the next Beatles?</u>

Source: Universal Music Group via Twitter

_____

_____

In a press release, 10:22PM's Joshua said "just as we would with any artist or creator, my team and I will work with KINGSHIP to sharpen their vision and develop their unique sound. Each member of the group has their own story and personality that influences and contributes to KINGSHIP's overall narrative. Through music and events across the metaverse, we will bring the Apes in KINGSHIP to life by building communities and utility, and entertaining audiences around the world."

In addition to the formation of Kingship, there have been several other notable licensing deals including a partnership with Timbaland as well as one between CAA and noted NFT personality 0xb1 to commercialize his collection.

Fractionalization

"Fractionalization" is another popular way of obtaining liquidity from NFTs.

It refers to the process of *economically* splitting up the ownership of an NFT into smaller pieces which can be bought, sold, traded and held by multiple users.

The term "economically" is key here as NFTs can't actually be divided (much like you couldn't cut a physical piece of art into smaller pieces without destroying its value). Instead, the process of fractionalization involves the issuance of tokens that represent a claim on the original asset (picture issuing shares on the Mona Lisa…).

One popular platform for fractionalization is Tessera (which was formerly named "Fractional").

Fractionalization of a CryptoPunk via Tessera
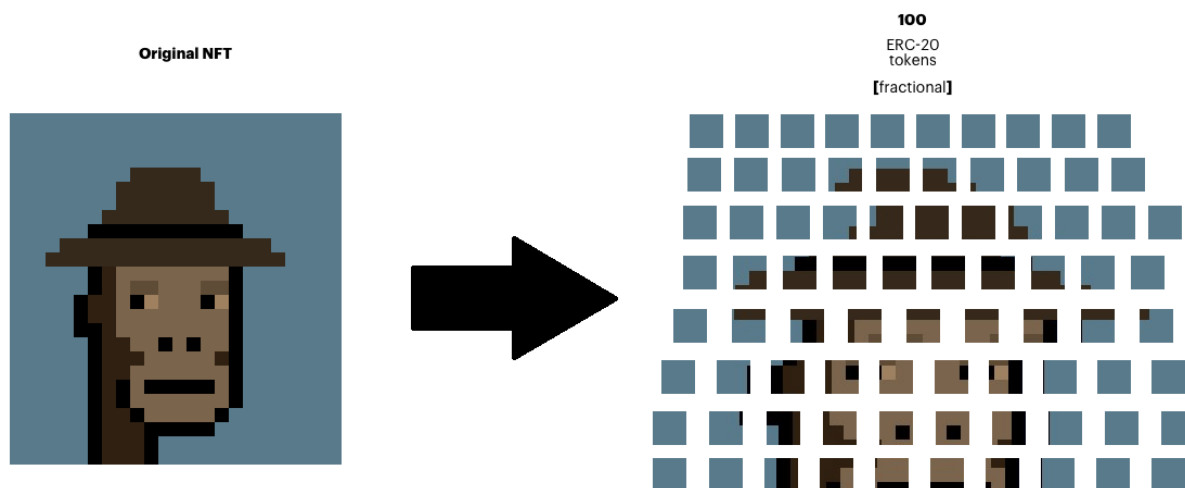
Source: Tessera

In order to fractionalize an NFT on Tessera, a user would:

- Create a Vault: NFT owners deposit their asset as collateral in a "vault" and specify the number of tokens they want to create
Mint Tokens: Once the collateral is deposited, Fractional issues the original owner 100% of the fractional ownership tokens

_____

_____

- Distribute Tokens: The owner can do anything she wants with these tokens – she can sell them, give them away or even add them to a liquidity pool
- Reedeem Tokens: When the vault is created, the original owner sets a "reserve price" – a price needed to trigger a buyout of the entire collection. If a buyer comes along and pays this reserve price, all of the token holders receive an immediate payout and the original NFT is transferred to the new owner

By way of example – let's say Alice wants to fractionalize her Cryptopunk. She could put it into a vault, issue 250 tokens priced at 1 ETH each, and sell them to 250 people (keeping 50 for herself). If she sets the reserve price at 2 ETH, a buyer could come along and buy the entire collection for 500 ETH, yielding a profit of 1 ETH for each token holder and 50 ETH for Alice.

Fractionalization yields several benefits in that it: 1) allows the average user access to extremely expensive works (such as CryptoPunks or Bored Ape Yacht Club) and 2) it allows owners to get some liquidity without selling the entire piece.

As such, the platform has done over $1.5 billion in volume.
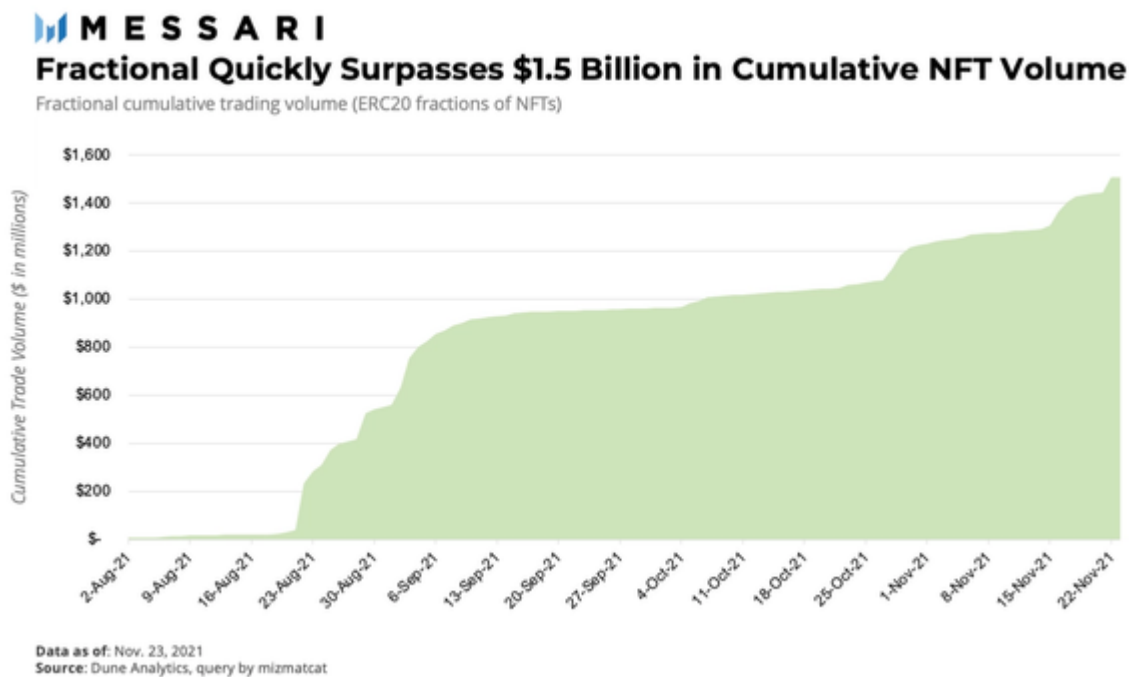
Source: Messari

_____

_____

Chapter 37: Criticisms of NFTs

Like any new market, the NFT space has its share of critics. While some of these gripes are legitimate, many are weak and come from people who don't understand economics, human psychology or the technology behind non-fungible tokens.

Videos such as "Line Goes Up – The Problem with NFTs" highlight several perceived problems in the space and claim that NFTs are:

- **Easily Copied:** Anyone can take a screenshot of an NFT and claim they own it
- **Centralized:** Most of the art for NFTs exists on centralized servers
- **Tacky:** NFTs are nothing more than a way to show wealth

While some of these are technically true, keep reading to see why they're not serious problems.

"Right Click Save"

One of the most sophomoric criticisms of NFTs is what's known as "right-click save". Critics argue that NFTs have no value because as digital files, it's easy for anyone to copy them and represent themselves as the owner.

Source: NFT Plazas

This argument is deeply flawed, of course, as there are thousands of reproductions of the Mona Lisa, but this doesn't diminish the value of the original. In fact, there's plenty of evidence to argue the opposite – the more a piece of art is counterfeited, the more valuable it becomes.

_____

_____

Moreover, as tools for verification mature – such as Twitter's new feature that displays a "hex" when NFTs are authentic – it will soon be even easier to spot fake NFTs (much easier, in fact, than for traditional art or luxury goods).

You Don't Really Own Your NFT

There's actually some merit to this – as mentioned previously, when you buy an NFT, you generally aren't purchasing a digital good or piece of art.

The art that represents most NFTs is simply too large to be hosted on a blockchain, and storing even a modest picture could cost thousands of dollars. As such, the assets themselves need to be stored on a separate server, and the NFT itself is little more than a link that points to the address of this database.
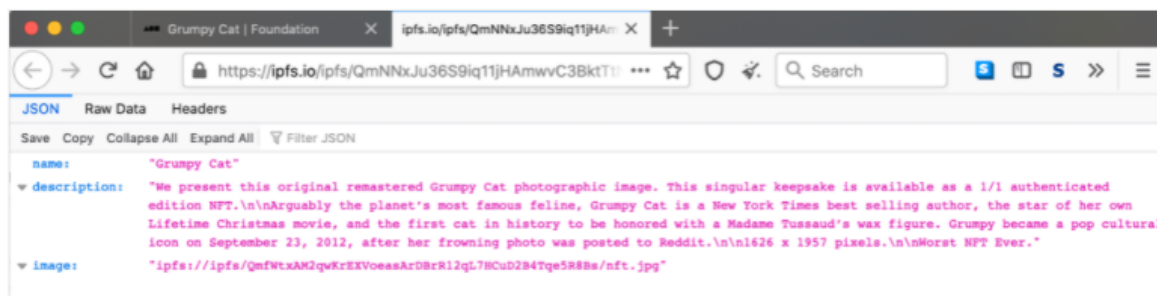
Metadata of an actual NFT that includes the name, description and a URL to where its stored

This scares some people – and rightfully so. If your image is stored on a third-party, centralized server, who is to say that they can't replace the image?

Fortunately, many projects are shifting to decentralized storage services such as Filecoin's IFPS and Arweave. These services use blockchain technology to encrypt and store data across several different devices, offering the same advantages as a standard database, with the added benefits that no one entity controls your asset.

In addition, many newer NFTs – such as Chainrunners – are opting for simpler formats that allow them to store all of their data "on-chain".

People only use NFTs to Show Off their Wealth

Even if that were the *only* reason – which, as stated above, I don't think is true – so what? That's a bit like saying "people only acquire money to spend it".

Human beings are evolutionarily wired to seek social status. It's highly correlated with a host of benefits including better health, more resources, increased happiness, higher social approval, greater influence and better access to mates.

_____

_____

Indeed, some researchers believe that over *90% of our behaviors are intended to show off our status*. It's why we buy Rolexes, Lamborghinis, Picassos, Louboutins and Birkin Bags; it's the reason that fewer than 5% of charitable donations are anonymous; it's probably even why we built the Pyramids!

The Global Market for Luxury Goods Exceeds $1 Trillion

Source: Bain & Co.

What separates NFTs from other status symbols is the fact that they are effectively **the first "digital" status symbol**. As such, they have a much broader reach than any necklace, dress, coat, watch, handbag, pair of shoes, car, house or physical piece of art could ever have.

And considering that watches are falling out of favor, ridesharing may reduce car ownership (especially with autonomous cars) and home ownership may decline with the rise of remote work and the digital nomad lifestyle, your Facebook, Twitter or Instagram profile pic may soon become your most valuable piece of real estate.

So yes, I'll concede that many people buy NFTs to show off their wealth. And guess what, the fact that millions of people can see your Cryptopunk or Bored Ape means that **it's probably the best damn way to show status that's ever been invented**!

Legitimate Criticisms of NFTs

While many of the concerns against NFTs are unfounded and / or poorly-reasoned, there are legitimate criticisms surrounding the technology and industry. Notably, the space suffers from:

- High Fees
- Rampant Fraud and Theft
- Poor User Experience

We will cover these concerns – as well as others – in Part 8: Challenges Facing Web3.

_____

_____

Chapter 38: Why NFTs Will Eat Hollywood (and maybe the World…)

Why Hollywood Won't Survive

I believe that NFTs represent a classic case of disruptive innovation and have the potential to change our lives in ways we can't even imagine.

Like most disruptors, they definitely have a ton of problems today – such as high fees, rampant fraud and theft and a relatively poor user experience.   But they also offer one advantage that the traditional entertainment industry simply cannot match – true ownership of content.   This will yield several benefits to artists and consumers, including:

- **Unparalleled economics**: The almost total elimination of intermediaries such as record labels, film and TV studios, game developers, distribution platforms, etc… allow NFTs to offer artists rates an order of magnitude over what they're getting now. They also, for the first time ever, provide a realistic and repeatable way for consumers to profit off their data and digital assets

- **Unprecedented Customer Experience**: NFTs offer the promise of a digital world that's fully interoperable, free of censorship and – most importantly – democratic. And while this compelling on its face, I believe that like smart phones, ATMs or the internet, we won't truly understand the utility NFTs can bring to our lives until we've experienced them at scale

- **New Sources of Innovation**: Not only are NFTs unburdened by regulation, knowledge is freely shared and there's an ability to crowdsource the ideas of millions of users to rapidly create and test better products. As such, it's not inconceivable that NFTs could catalyze a user-driven cultural "renaissance"

Perhaps most importantly, Hollywood can't replicate NFTs without cannibalizing itself, and regulators can't stop their progress due to their decentralized nature.

Could NFTs Replace the Physical Asset Market?

As discussed, NFTs aren't limited to digital assets, they can also serve as representations of physical assets as well.

While the thought of the digital asset market eclipsing the physical one may seem ridiculous at first glance, such a feat is not without precedent as:

- Digital entertainment makes up 72% of all entertainment revenue
- Online advertising makes up 2/3rds of total advertising
- Global eCommerce sales are approximately 20% of total retail sales and expected to grow to nearly 25% by 2025 (and in some countries, such as China, online sales make up almost half of all purchases)

_____

As the NFT market matures, it too will likely begin to take share. While how much is still up for debate, the fact that the digital asset market is less than 0.005% (1 / 20,000th) of the physical asset market means that there's a lot of room to grow!

<u>Quantifying the Potential Value of NFTs</u>

While it's difficult to put a number on disruption, when we compare cryptocurrencies to the market cap of cryptocurrencies, the entertainment industry, the top 10 tech companies and the stock market value of all tech companies we can see that there is still significant room for appreciation.

<u>NFTs are Less than 1% of the Entertainment Industry and Less than 0.1% of All Tech Stocks</u>
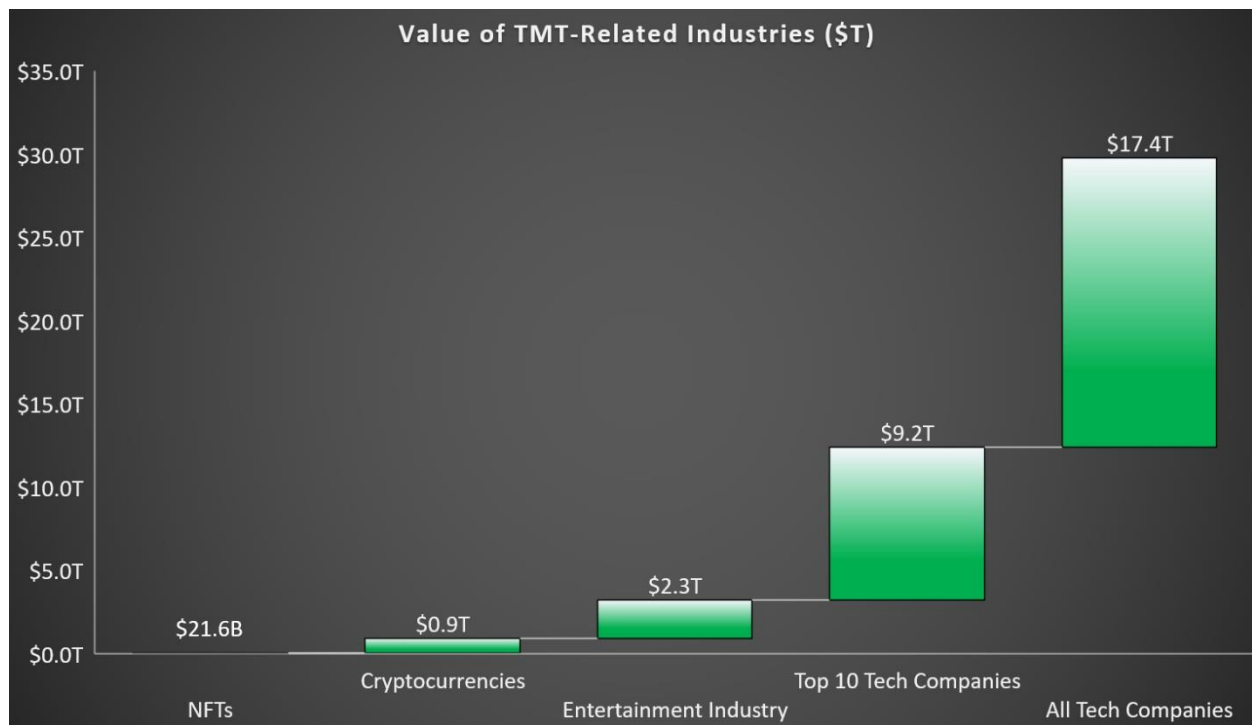
Indeed, the NFT market could grow 10x from here (to $216B) and still represent less than a quarter of the crypto space…

…it could grow 100x from here (to $2.2T) and be roughly equivalent to the global entertainment market…

…it could grow 1,000x from here (to $22T) and be roughly equivalent to the global technology market…

…it could even grow 10,000x from here ($220T) and be roughly 40% of the physical asset market today.

Wherever this thing ends up, it's important to watch as it has the potential to be both an existential threat to traditional entertainment and technology and a road to almost unlimited potential for investors.

_____

Part 5: Decentralized Finance ("DeFi")

_____

Chapter 39: What is DeFi?

DeFi, or Decentralized Finance, refers to a global, peer-to-peer network that is built to replace the traditional banking system.

Using blockchain technology, consumers can store their own assets and freely transact directly with other users without relying on traditional intermediaries such as banks, brokers, exchanges and insurance companies. This eliminates many of the costs, restrictions and regulations associated with our legacy financial system.

TRADITIONAL FINANCIAL SYSTEM

DECENTRALIZED FINANCIAL SYSTEM
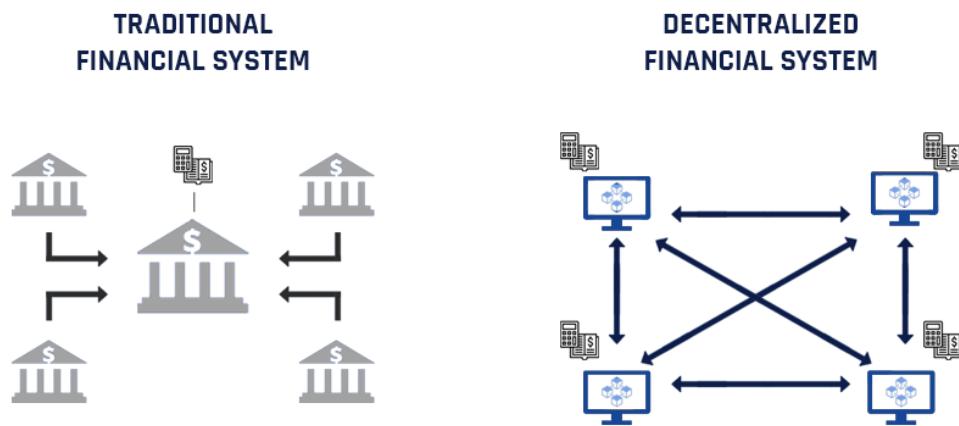
In the traditional (centralized) financial system, consumers must operate through banks, brokers and exchanges

In a decentralized financial system, consumers are free to transact directly with one another

Source: Medium

Proponents assert that DeFi is superior to traditional finance because it retains all the benefits of conventional banking while being cheaper, faster and much more accessible and transparent. Critics argue that it represents an existential threat to the global financial system, a serious danger to the community and must be regulated at all costs.

Whatever side of the argument one falls on, DeFi's popularity is undeniable. The market has grown 100x since January 1st, 2020, to a current value of over ~$50B in deposits (and it nearly reached $200B during the bull market).

_____

_____
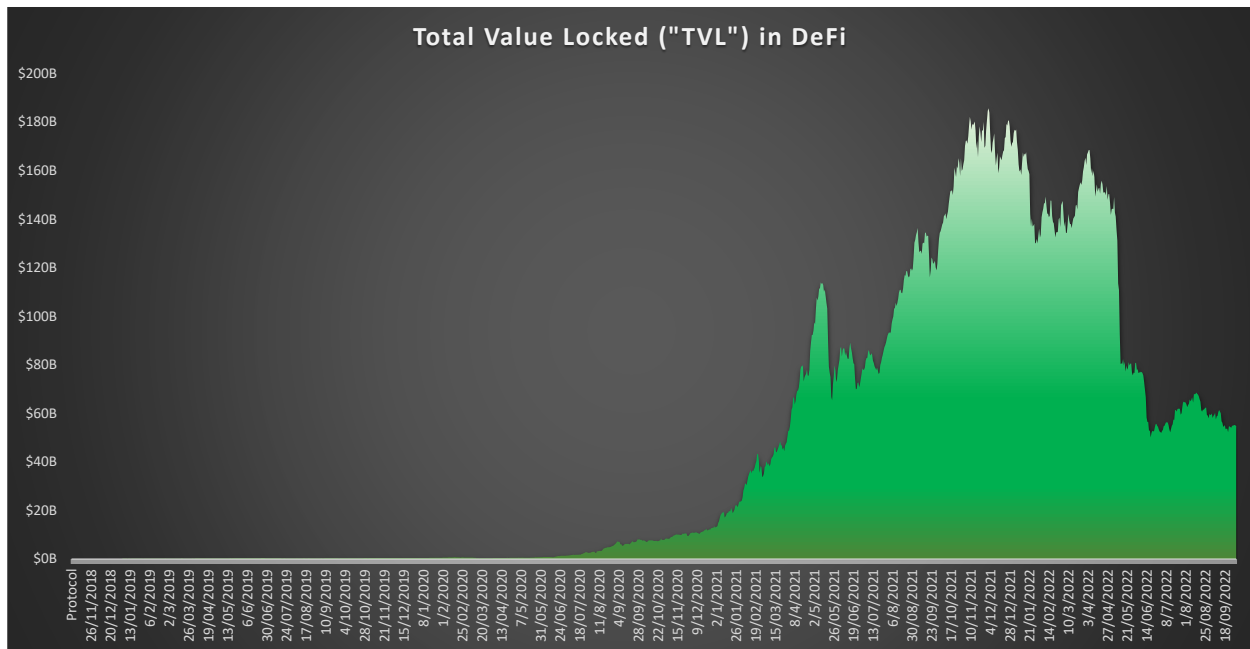
Source: Defillama.com as of 10.2.22

What is driving this popularity? Let's dig a little deeper…

Chapter 40: The Problem with Centralized Finance

Our current financial system is highly centralized and quite complex – central banks such as the Federal Reserve issue and control the money supply, borrowing and lending is conducted through the banking system, trading is done through exchanges and the system is supported by a host of national and international regulatory bodies.

Overview of the financial system in the United States

Note: No need to analyze this – the entire point is that it's very complex…

Source: Researchgate.net
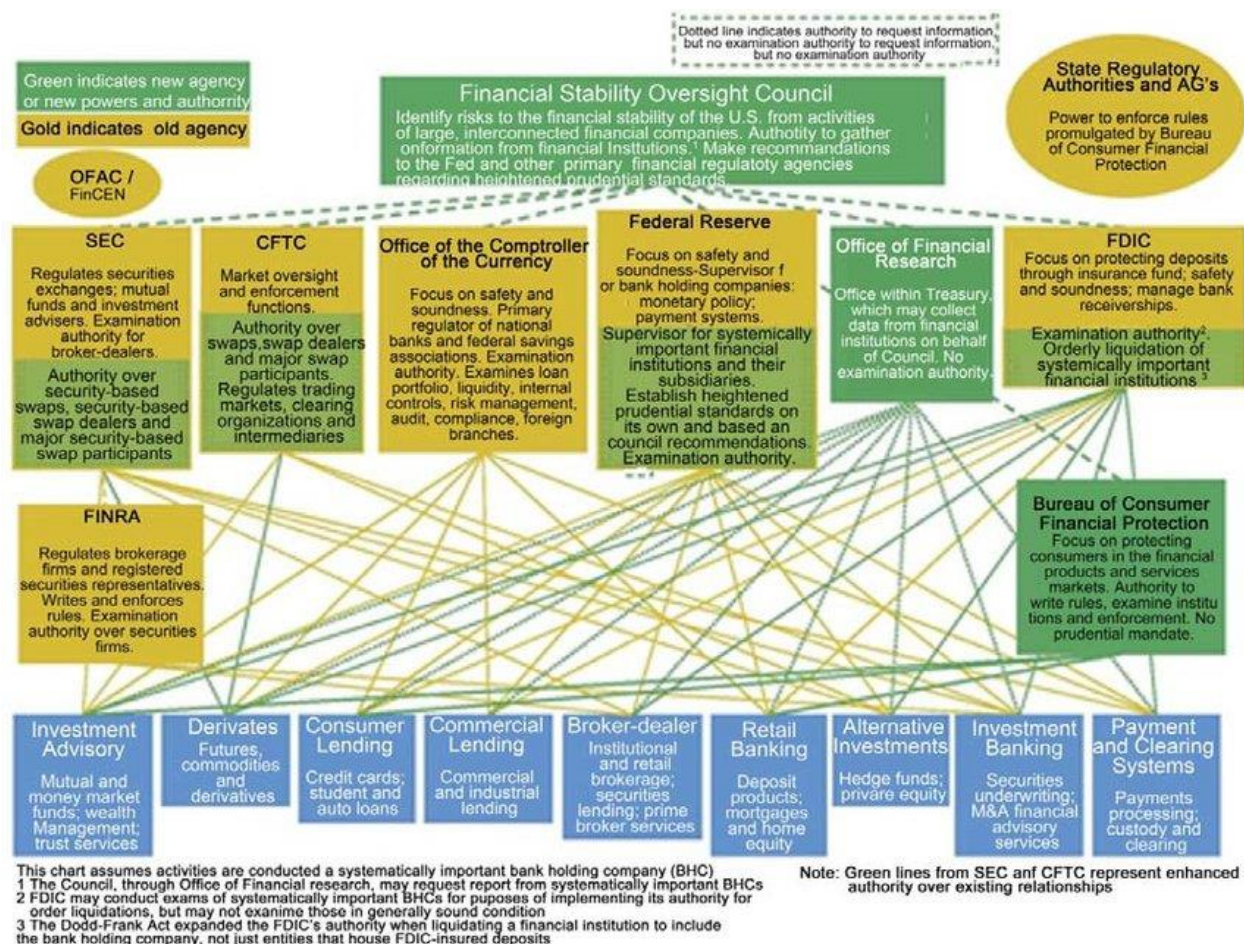
Unlike some in the crypto space I don't hate banks or international financial systems. In fact, I think that our current system has served us remarkably well and has undoubtedly been a key driver of the prosperity we've seen over the last century. It facilitates growth via trade and the international flow of investment capital, provides security and helps establish trust through regulation, legal frameworks and the certification of formal and informal economic actors.

_____

But, like any centralized system, our current infrastructure has become bloated, byzantine and draconian. This leads to numerous problems for the consumer including:

- **Third-Party Custody**: In the current financial system, you don't really hold your funds – the banks do. This means that they can freeze and even seize your assets at will (while this may seem far-fetched, consider that in 2013, the Government of Cyprus seized 47.5% of all bank accounts over €100,000 to bail-out its failing banking system)

- **Limited Access:** Banks can decide whether they want you as a customer. While generally not a problem in the developed world, this is a huge issue in growing economies. Today, nearly 1.7 billion people remain unbanked simply because they aren't profitable enough to be considered by global financial institutions

- **No Privacy**: Banks must collect detailed personal information to adhere to KYC, AML and CFT regulations and require credit scores for borrowing

- **Expensive and Inefficient:** The current financial system is rife with inefficiencies and unnecessary expenses. Payment networks charge up to 3% on credit card fees, cross-border remittance payments can take up to a week and cost 10%, and even in developed nations, users are faced with long transfer times and bloated fees

- **Lack of Interoperability:** Most banks currently operate as "walled gardens", making it difficult to even transfer funds between entities let alone share and collaborate on new technologies and products.

- **Opacity:** The financial crisis of 2008 made it abundantly clear that our current financial system lacks transparency, as even the droves of regulatory bodies had little idea what was sitting on the balance sheets of our largest institutions

Together, these concerns represent a major problem. Not only do they limit growth, but they also continue to drive inequality.

So why do we tolerate these inefficiencies? Once again, it's due to the Byzantine General's Problem. Up until recently, there was no way for large groups of humans to trust one another or coordinate across vast distances without using third parties (such as banks) to establish trust.

In short, while some may call the banking system "evil", up until now it has been a "necessary evil".

_____

_____

Chapter 41: The Benefits of Decentralized Finance

As discussed, this all changed with the invention of Bitcoin, which solved the Byzantine General's Problem and made it possible to perform **direct, peer-to-peer transactions without relying on third parties to establish trust**.

The effect of this cannot be overstated. Imagine for a bit, how you would design a financial system if you no longer needed intermediaries. After all, what's the point of banks if you can safely hold your own assets? What's the point of financial intermediaries if you can make loans directly? What's the point of lawyers if everything is executed in code? What's the point of exchanges if you can trade directly? What's the point of regulators in an industry that can't be regulated?

If you're like me, you're probably envisioning something much simpler and more elegant than what we have today…

That system is DeFi, and it may allow us to reap all the benefits of centralized banking – namely trust, security and growth – while removing most of the downsides. Indeed, DeFi offers:

- **Self-Custody:** Instead of relying on a bank or brokerage to hold your assets, you control all of your funds with your own wallet. As such, there's no one to seize your assets, limit withdrawals or tell you where you can and can't spend your money. Want to send all your life savings to a sketchy gambling website? Go for it!

- **Permission-Less**:   Users don't need permission from third parties. Anyone with money and an internet connection can access any DeFi service and trade coins, create derivatives, lend and borrow, buy insurance, etc… in markets that are open 24 hours a day, 7 days a week and 365 days a year

- **Private:** Users can choose to (and often do) remain anonymous. As Coindesk so eloquently stated: "On the normal web, you can't buy a blender without giving the site owner enough data to learn your whole life history. In DeFi, you can borrow money without anyone even asking for your name."

- **Efficiency:** DeFi operates almost entirely via computer programs which automate the execution of financial transactions. As such, there's no need for intermediaries such as bankers, regulators, lawyers, accountants, escrow agents, etc… making the system much faster *and* much cheaper

- **Interoperability:** DeFi protocols are built to be composable, that is, they can be programmed to work with one another allowing users to build increasingly complex and novel financial products

- **Transparency:** Every transaction in DeFi is broadcast to the public allowing for real-time monitoring and maximum transparency. In addition, protocols are built with open-source code allowing any user to audit them

_____

_____

DeFi offers many of the same products as Traditional Finance, including loans, savings accounts, exchanges, insurance, etc…

What's shocking though is that many of these familiar products work in very unfamiliar ways. To see what I mean, let's look at a few examples including decentralized cash, exchanges, lending and borrowing, insurance and derivatives.

_____

Chapter 42: Decentralized Cash (aka "Stablecoins")

What are Stablecoins?

While DeFi has enormous potential to disrupt traditional finance, one thing limiting its development is price volatility. After all, how can we use cryptocurrencies as a medium of exchange if the value is so unpredictable? What good are double-digit interest rates if the value of the underlying assets can decrease by 50% overnight?

Stablecoins help mitigate this volatility. In a sense, a stablecoin is nothing more than a cryptocurrency pegged to a (relatively) secure asset such as the US Dollar. They can be used to buy things, lend and borrow, collect interest and even hold as a store of value. In effect, anything you can do with cash you can do with a stablecoin.

<u>The Total Stablecoin Supply is Nearly $150B</u>
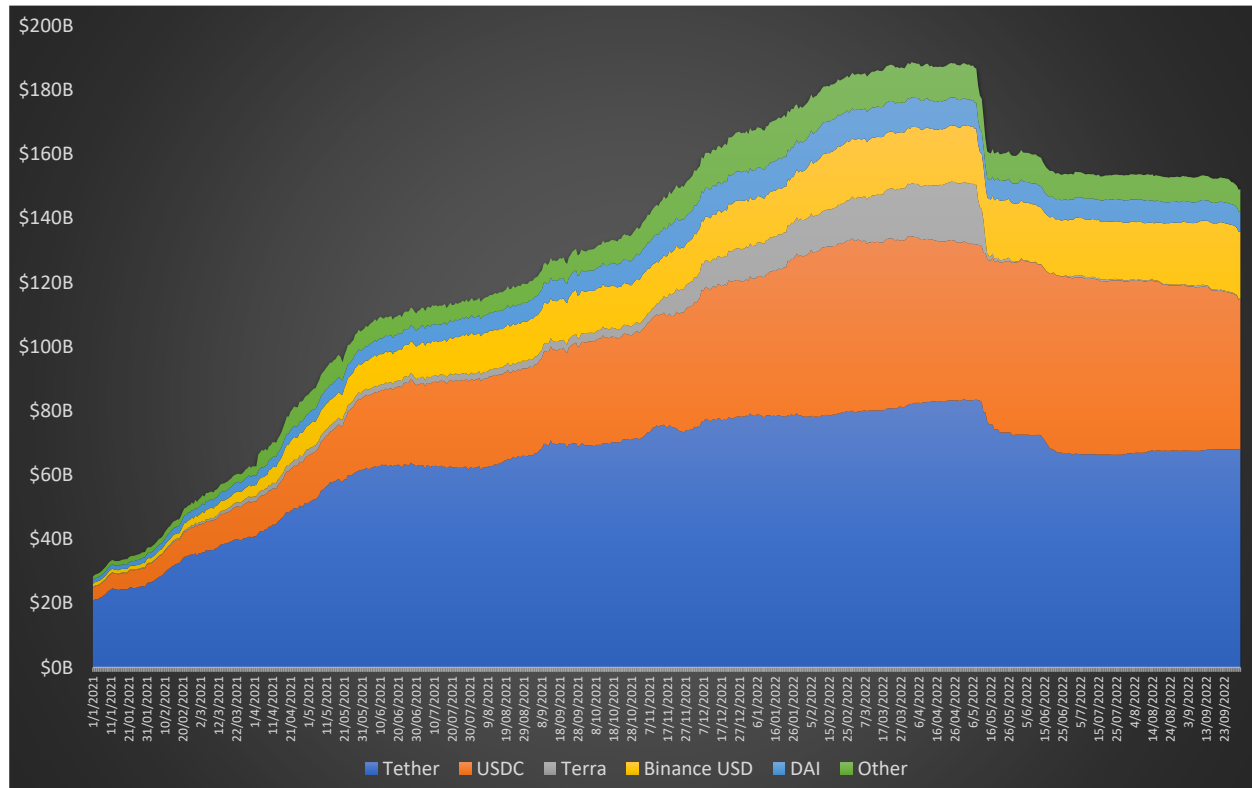
Source: <u>DeFi Llama</u> as of 10.2.22

The stablecoin market has grown almost 500% since January 1st 2021, and currently stands at nearly $150B.

How Are They Different?

While on the surface stablecoins might seem very similar to the digital money we use today, under the hood they are very different animals. Perhaps the most glaring distinction is in the ownership

_____

and control of the assets. The dollar is owned by the United States government – the Fed sets the rules and controls the supply, commercial banks distribute the funds through fractional reserve banking and depositors receive interest.

Stablecoins on the other hand, are a form of private money. They either are governed by a corporation or a DAO (to keep things simple you can think of this as a collective), users create and distribute the funds by depositing collateral and token owners claim the interest.

Today, there are three main types of stablecoins:

1. **Fiat-Collateralized**: Fiat-collateralized stablecoins such as Tether and USDC are (or at least claim to be) fully backed by cash. That is, for each $1 of Tether, there should be $1 sitting in a bank account somewhere.

   The problem with these coins is that, by definition, they are still centralized, relying on banks and other third parties to keep custody of the collateral. This goes against the decentralized ethos of DeFi, as any centralized point in the chain makes the entire system vulnerable and serves as a magnet for regulators.

2. **Crypto-Collateralized**: Crypto-collateralized stablecoins such as Dai are, as the name suggests, backed by a basked of cryptocurrencies and use autonomous protocols to maintain the peg.

   While promising, crypto-collateralized stablecoins are currently very inefficient, requiring huge amounts of overcollateralization. That's why the holy grail of DeFi has long been the creation of an Algorithmic Stablecoin.

3. **Algorithmic**: Algorithmic stablecoins are decentralized and do not require collateral. The peg is maintained through a complicated incentive program. In essence, when the price goes above $1, more coins are issued, diluting the supply and lowering the price. When it goes below $1, coins are bought back to raise the price.

While algorithmic stablecoins are great in theory, they may not be possible in practice. Economists are quick to point out that they violate the "impossible trinity", which states that you can't have a free capital flow, sovereign monetary policy and a fixed exchange rate at the same time.

Indeed, virtually every experiment in this space has failed because incentives stop working if people don't believe there's inherent value in the currency. Once trust is loss, everyone sells contributing to a "death spiral" that quickly reduces the value of the coin to zero.

Whether or not this problem is solved by the current batch of market participants, stablecoins will likely continue to play a major role in DeFi as they offer several core benefits:

- **Permissionless:** Anyone can access stablecoins and use them to freely move assets across international borders

- **Cheaper:** Although Ethereum is currently experiencing a significant fee problem, many competing networks offer near-zero fees for using stablecoins (much less than the 2-3%

_____

_____

charged by Visa and Mastercard)

- **Faster:** Stablecoin transactions and transfers are near instant and can be performed at any time

- **Programmable:** It's helpful to remember that stablecoins are software and, as such, can be easily programmed into smart contracts, creating a variety of potential use cases

- **Transparent:** Anyone can view the underlying code and all transactions are easily discoverable on blockchain explorers

Who are the Key Players?

Stablecoins by Market Capitalization

Dai 4%
Other 5%
Binance USD 14%
Tether 46%
USD Coin 31%

Source: Defillama as of 10.2.22

_____

The market for stablecoins is currently dominated by the fiat-collateralized model, with Tether, USDC and BUSD holding a combined 91% market share.

Project	Market Share	Description
	46%	Tether is a fiat-collateralized stablecoin that is (or at least claims to be) fully backed by cash. For each $1 of Tether, there should be $1 sitting in a bank account somewhere.
	31%	Like Tether, USDC is a fiat-collateralized stablecoin backed by US dollars held in reserve. The token is very popular on Coinbase.
	14%	BinanceUSD is another fiat-collateralized stablecoin backed by US dollars or treasury bills. It was created as a partnership between Binance and Paxos.
	4%	MakerDAO is a decentralized organization responsible for the creation and management of DAI, a decentralized, crypto-collateralized stablecoin.
	<1%	Terra is an algorithmic stablecoin that once held 10% market share in the stablecoin market. The project rapidly collapsed in May 2022, destroying tens of billions of value.

_____

Chapter 43: Decentralized Exchanges

What are Decentralized Exchanges?

Decentralized exchanges (or DEXs) are peer-to-peer marketplaces where users can directly trade with one another without the need for banks, brokers or any other financial intermediaries.

DeXes Hosted Over $1.5 Trillion in Volume Over the Last Year
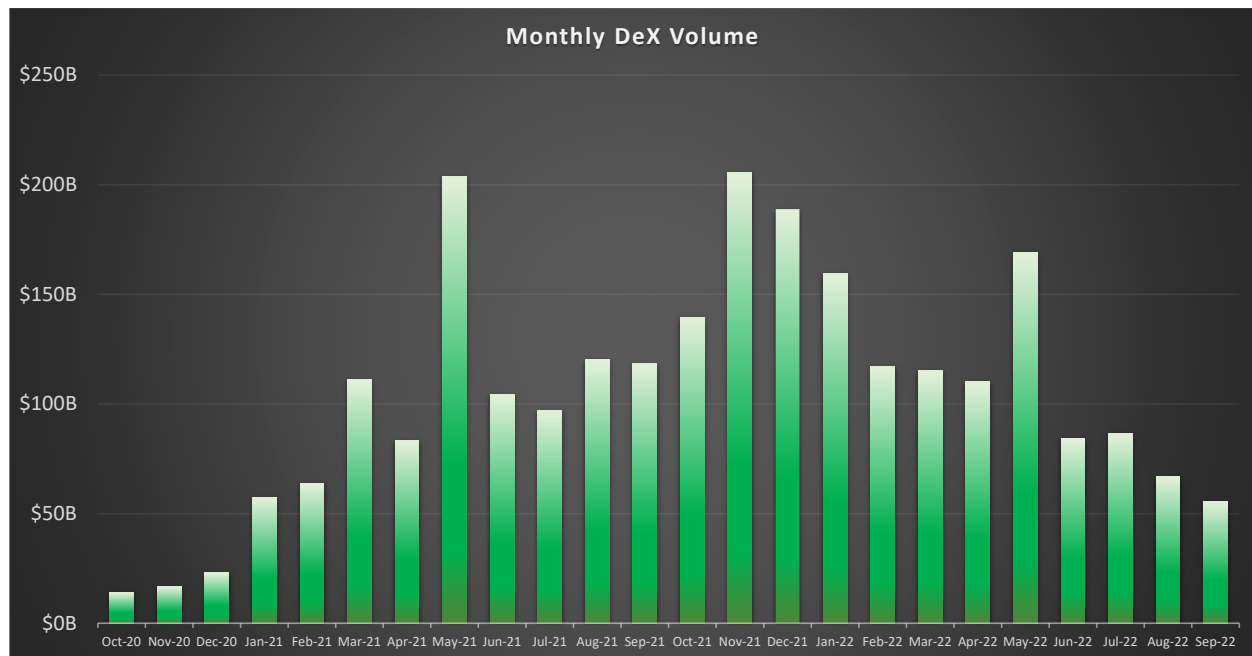
Source: Dune Analytics as of 10.2.22

They have hosted nearly $1.5T of trades over the last 12 months and are even catching up to centralized exchanges.

How Are They Different?

Traditional exchanges, such as the NYSE, Nasdaq or Coinbase, provide a platform to match buyers and sellers of securities. This begs the question, what happens if there's a temporary imbalance between the two?

Enter market makers. Market makers, who are often brokerage houses, hold onto a "reserve" of assets that they are always ready to buy or sell. Instead of trying to profit from the movement of a security, they profit from the difference in the buying price and the selling price, known as the bid-ask spread.

These professionals are essential because they ensure that traders can always immediately buy or sell during trading hours, providing much needed liquidity to the markets.

_____

A new breed of decentralized exchanges, however, is removing the need for these middlemen and allowing direct peer-to-peer trading through what is known as an Automated Market Maker ("AMM").

Instead of needing to match buyers and sellers in real-time, the participants of an AMM contribute their tokens to a centralized reserve known as a liquidity pool. This eliminates the need for a market maker as prospective traders can now directly through that pool, depositing what they want to sell and taking what they want to buy.

For example, let's say you wanted to trade ETH for UST on Uniswap. You would simply go to the site, access the ETH-UST pool, send in your ETH and receive UST in return. The price is controlled by a simple algorithm that raises the price of a token when demand increases and lowers it when demand falls.
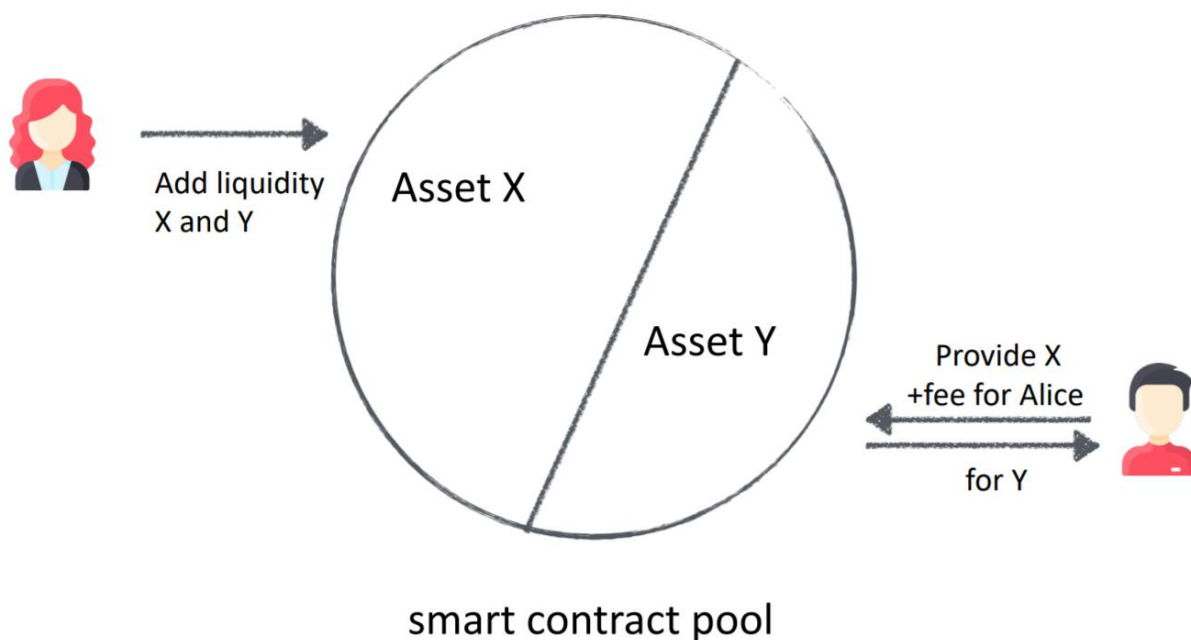
Source: Berkeley DeFi MooC

The decentralized nature of these AMMs has several unique benefits:

- **Anonymity:** DEXs don't require sign-ups, KYC information or any customer information at all

- **24/7/365:** The unique liquidity pool structure of AMMs means that trading never shuts down

- **Deep liquidity:** Although DEXs have not yet caught up to their centralized competitors, the fact that anyone can provide liquidity creates huge potential for the market

Personally, I believe that one of the most beneficial aspect of DEXs today is that they're not subjected to the limitations of Coinbase and Binance. Unfortunately, the two largest centralized exchanges often have arbitrary and stringent rules for listing coins, so it's not uncommon to be

blocked from purchasing a popular token. With over 50,000 trading pairs listed on Uniswap, however, you can almost always find what you are looking for!

While extremely elegant and seemingly much more efficient than traditional exchanges AMMs are not without their risks, which include:

- **Smart Contract Risk**: It's vital to remember that these AMMs are nothing more than lines of code, and code can be very vulnerable. For instance, if there's a bug or if a hacker finds an exploit, participants could easily lose all of their funds. That's why some of the largest exchanges hold reimbursement funds

- **Impermanent Loss:** Impermanent loss is a complicated concept whose mechanics are outside the scope of this article. But in essence, it's a form of opportunity cost, where a liquidity provider loses out on potential gains because his or her funds are locked in a liquidity pool

<u>Who are the Key Players?</u>

Source: The Block as of 10.2.22

_____

At the time of writing, the largest decentralized exchanges by volume are Uniswap, PancakeSwap, Dodo, Curve, Balancer, Sushiswap and Orca.

Project	Market Share	Description
UNISWAP	67%	Uniswap is an Ethereum-based decentralized exchange using an AMM model. It currently holds 77% market share and recently released a popular new version (v3) designed to protect liquidity providers.
PancakeSwap	12%	PancakeSwap is a DeX native to the BNB ecosystem
DODO	9%	A decentralized exchange that uses a variation of an AMM known as a PMM ("proactive market maker")
Curve	7%	Curve is an AMM that focuses on trading stablecoins
Balancer	3%	Balancer hosts multi-asset liquidity pools, allowing up to 16 tokens per pool
SushiSwap	1%	Sushiswap is a fork (literally a copy) of Uniswap that initially pulled many users from its parent. Recently, however, the company has been plagued by infighting and has seen its token drop
ORCA	1%	Orca is a DeX native to the Solana ecosystem

_____

_____

Chapter 44: Decentralized Lending and Borrowing

What are Decentralized Loans?

Decentralized lending operates on peer-to-peer lending platforms that allow **anyone** to give and receive loans without using a bank or other third-party intermediary.

The Decentralized Lending Market Has Grown 700% Since 2020
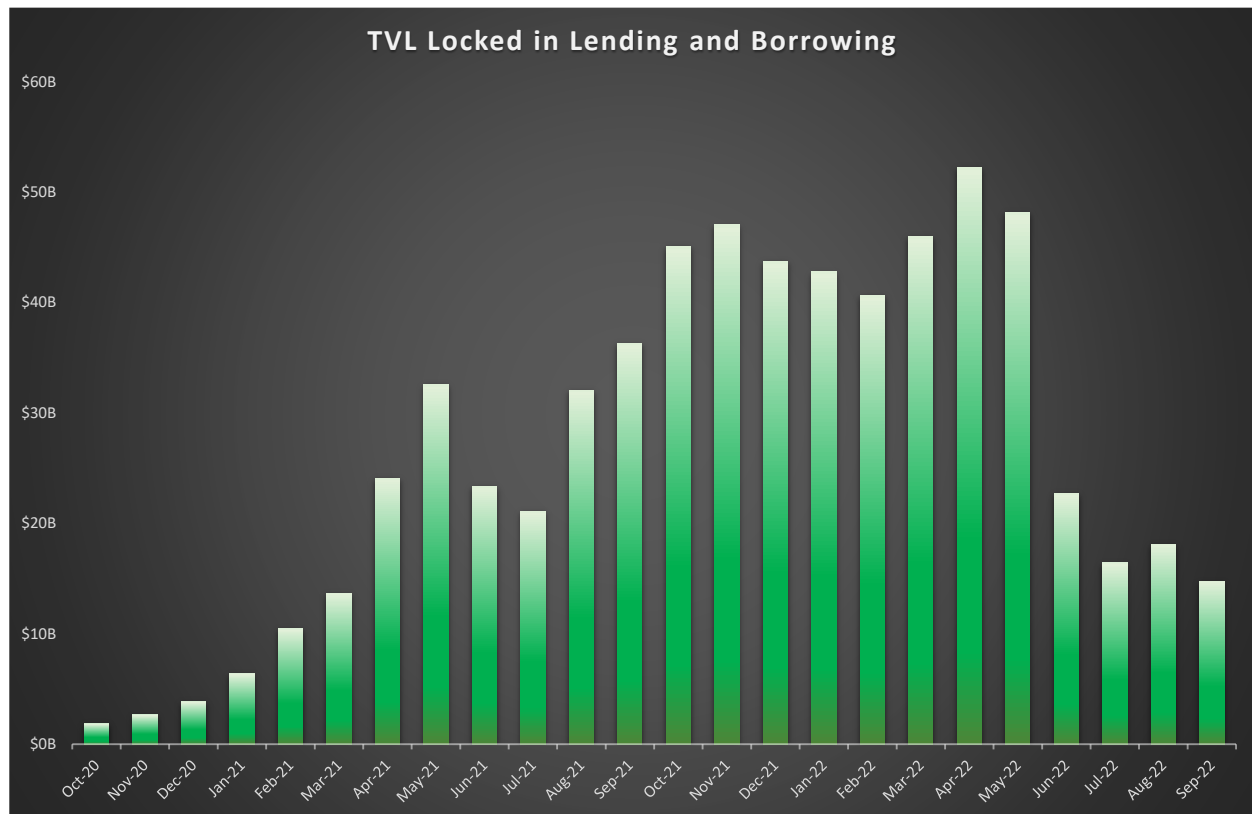
Source: Defillama as of 10.2.22

According to Defi Llama, there were $14.6B outstanding DeFi loans as of October 2022 – up nearly 700% from January 2020 (and the market exceeded $50B in April 2022).

How Are They Different?

In traditional finance, borrowing and lending is facilitated by banks or other financial institutions. While some Fintechs have introduced peer-to-peer lending, the mechanics are largely similar, as both methods rely on centralized parties and require detailed onboarding, credit checks, KYC and underwriting.

Once again, DeFi does things in a totally different way.

_____

_____

Instead of relying on a bank or third-party platform to serve as a matching agent, DeFi lenders contribute their assets to a pool and encode the rules of the loan into a smart contract. These pools use a mathematical formula to calculate interest rates.

When a borrower wants to take a loan, all they have to do is deposit some cryptocurrency for collateral (generally overcollateralizing by 133% to 150%) and they are free to take the loan. This process requires no KYC, no credit checks and no legal documentation. In fact, you don't even have to give anyone your name!

Once they're done with the loan, borrowers can simply pay back the principal plus interest and get their collateral back.

The fact that these loans are collateralized with such a liquid instrument has a few unique consequences:

- Lenders have zero default risk – if the borrower fails to repay or if the collateral goes below a certain threshold, it's immediately liquidated and paid to the lender
- There are no repayment schedules or any obligation to repay at all. Borrowers can keep the loan as long as they want providing that the collateral remains in good standing

Indeed, decentralized loans offer several advantages over their traditional counterparts:

- **Permissionless**: Anyone with collateral can get a loan, and they can do it anonymously

- **Faster**: Decentralized loans are settled instantly

- **Cheaper**: As there is no need for loan documentation, underwriting, KYC, etc… decentralized loans often cost a fraction of their traditional counterparts

All this said, decentralized loans are not without risk, as they are still susceptible to the smart contract risk and rug pulls that we've discussed above.

_____

_____

Who are the Key Players?
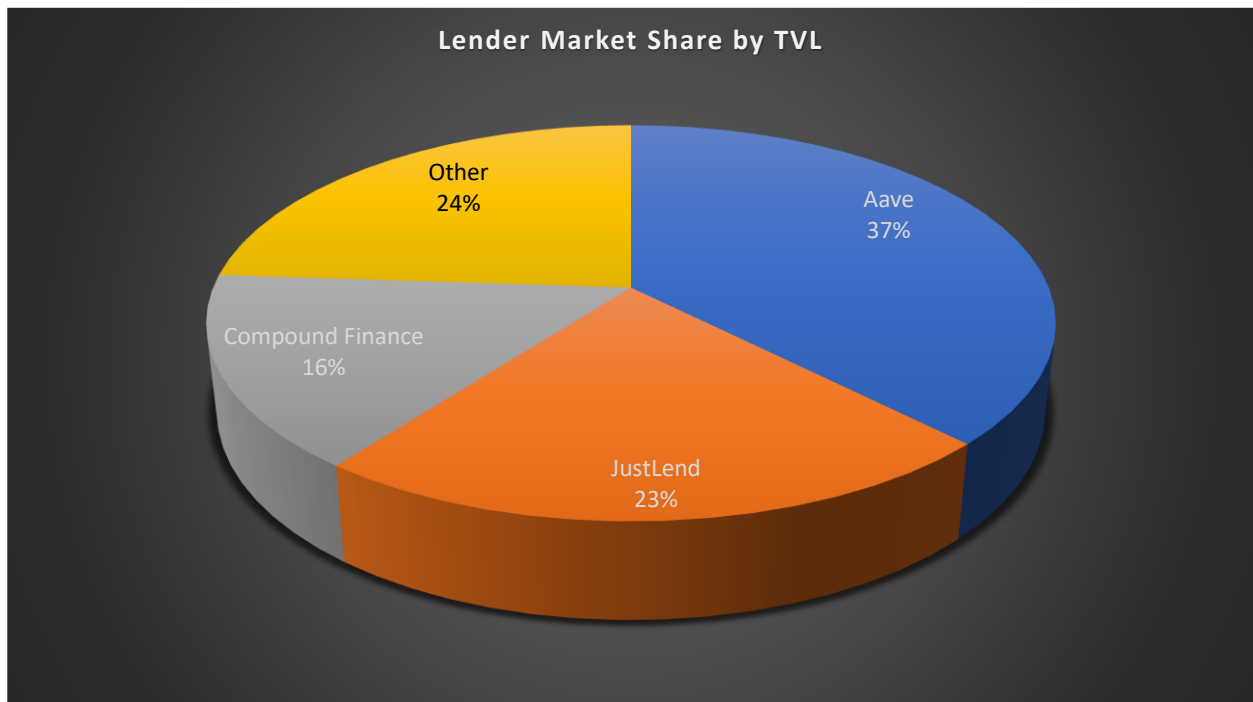
Source: Defi Llama as of 10.2.22

The three largest players – Aave, JustLend and Compound – control over 76% of the lending market's Total Value Locked (the value of assets deposited into smart contracts pools by lenders and borrowers).

Project	Market Share	Description
AAVE	38%	Aave is the largest "pure" lender on Ethereum. It is known for its wide range of products, financial innovation and asset diversity.
JustLend	23%	JustLend is a decentralized lending platform operating on the TRON blockchain
Compound	16%	Once a very close competitor to Aave, Compound has lost share over 2021 and is generally regarded as less flexible.

_____

_____

Chapter 45: Decentralized Insurance

What is Decentralized Insurance?

Decentralized insurance utilizes the power of blockchain technology and smart contracts to offer users cover against black swan events, wallet hacks, smart contract exploits and much more.

The space is still in its infancy – while there have been billions of losses due to crime across the crypto space (up to $14B in 2021 according to some experts), the TVL of decentralized insurance remains under $500M. This pales in comparison to the $6.3T traditional insurance industry.

How Is It Different?

At a fundamental level, insurance is a way to pool risk:

- Customers pay premiums, which go into a community pool owned by the insurance company
- If something bad happens, the insurance company will hire claim adjustors to validate and pay out the claim.
- The insurance company will keep amount of the pool as a "reserve" to pay out claims, but often invest the rest

There are two main problems with this model: 1) administrative expenses can be very high and 2) the principal-agent problem (i.e. the insurance company is responsible for validating the claims, which means that they are incentivized not to pay them out)

Decentralized insurance protocols are designed differently, with the aim of solving both of these issues.

To understand how decentralized insurance differs, let's look at an example from Nexus Mutual, one of the leading insurers that specializes in smart contract risk.

There are three main actors in the Nexus Mutual ecosystem:

- Customers: Customers purchase insurance from Nexus Mutual and pay premiums
- Risk Assessors: Members who are confident in their ability to assess the vulnerabilities of smart contract code may volunteer to be a Risk Assessor
- Claims Assessor: Members may also volunteer to be Claims Assessors and vote on claims (i.e. "has a breach occurred?")

Now that we know the players, let's see how this works in practice:

- Let's say that Alice is lending money on Compound. She wants to insure against a smart contract breach (i.e. someone hacking Compound and stealing all of the funds), so she buys Smart Contract insurance on Nexus Mutual
- Like in traditional insurance, Alice will purchase the insurance and deposit the premiums into a pool

_____

_____

- Risk assessors who believe that Compound is safe will underwrite her insurance by putting tokens up as collateral
- If no breach occurs, then the Risk Assessors get their collateral back plus part of the premium pool
- If Alice believes a breach does occur, then the issue is sent to Claims Assessors who will research and vote on the issue. Claims Assessors also provide collateral
- If a majority of the Claims Assessors agree that a breach has occurred, then Alice will get paid and the any Claims Assessor who voted with the majority will receive their collateral back plus some portion of the premium (Claims Assessosr who vote the opposite way will lose their collateral)
- In the case of a breach, the Risk Assessor will lose their collateral

By effectively pitting the Risk Assessor and Claim Assessors against one another, Nexus Mutual is able to remove the principal-agent problem and massively reduce expenses.

The genius of this method is that it removes the principal agent problem, greatly reduces expenses and offers near-immediate claim payouts.

Decentralized insurance protocols are not without risks, however, and Claims and Risk adjustors that don't have a deep knowledge of their craft can lose a lot of capital.

<u>Who are the Key Players?</u>

Source: DeFiLlama as of 10.2.22

_____

_____
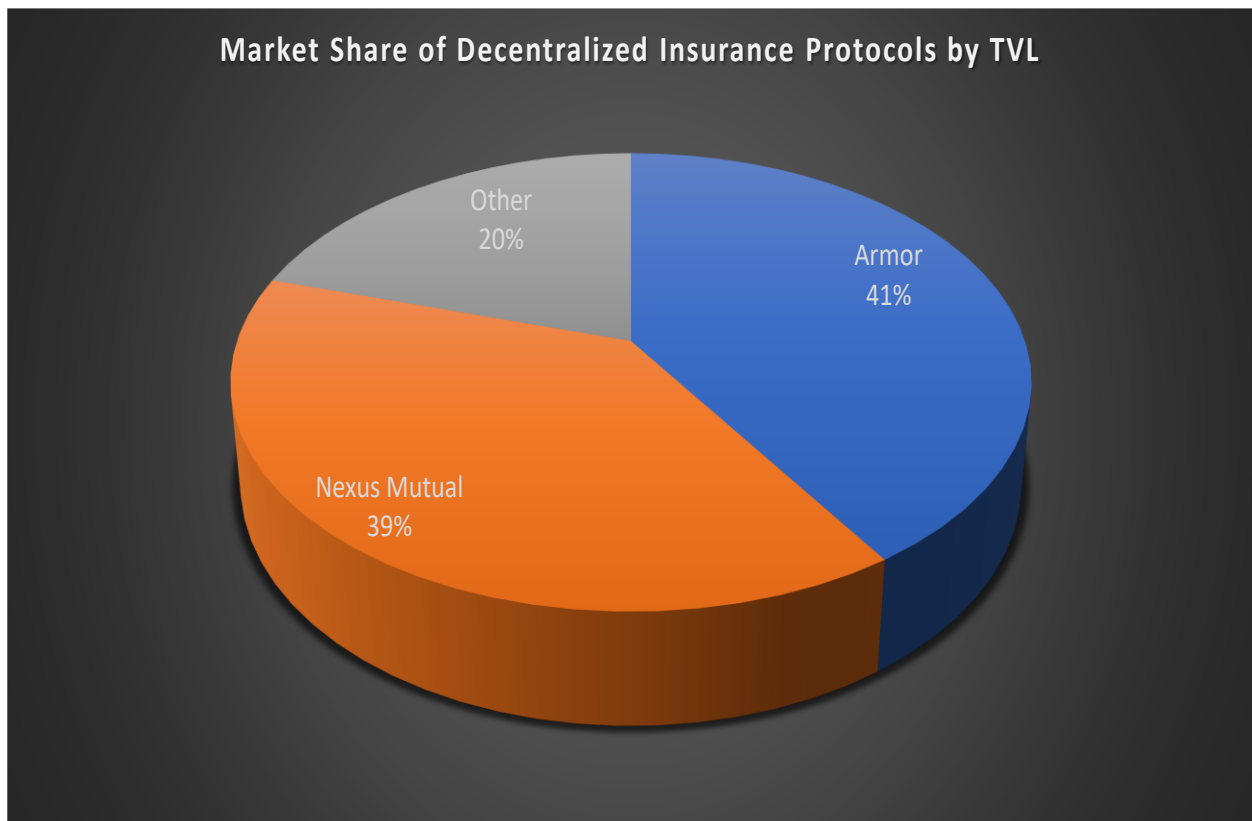
At the time of writing, Armor and Nexus Mutual control over 80% of the TVL in insurance. The two are currently partnered in a broker (Armor) – underwriter (Nexus) relationship.

Project	Market Share	Description
	41%	Armor is a decentralized insurance broker and aggregator that removes the need for KYC. It is currently underwritten by Nexus Mutual.
	39%	Nexus Mutual is an Ethereum-based decentralized insurance platform

_____

_____

Chapter 46: Decentralized Derivatives

What are Decentralized Derivatives?

Derivatives are financial instruments that derive their value from an underlying asset such as a stock, bond, commodity, market index or currency. Most traditional derivatives are traded on conventional exchanges such as the Nasdaq or CME, and crypto derivatives are traded on centralized exchanges such as Binance and FTX.

As the name would suggest, decentralized derivatives refer to the exchanges and protocols that facilitate the creation and trading of derivatives *without* using a centralized party.
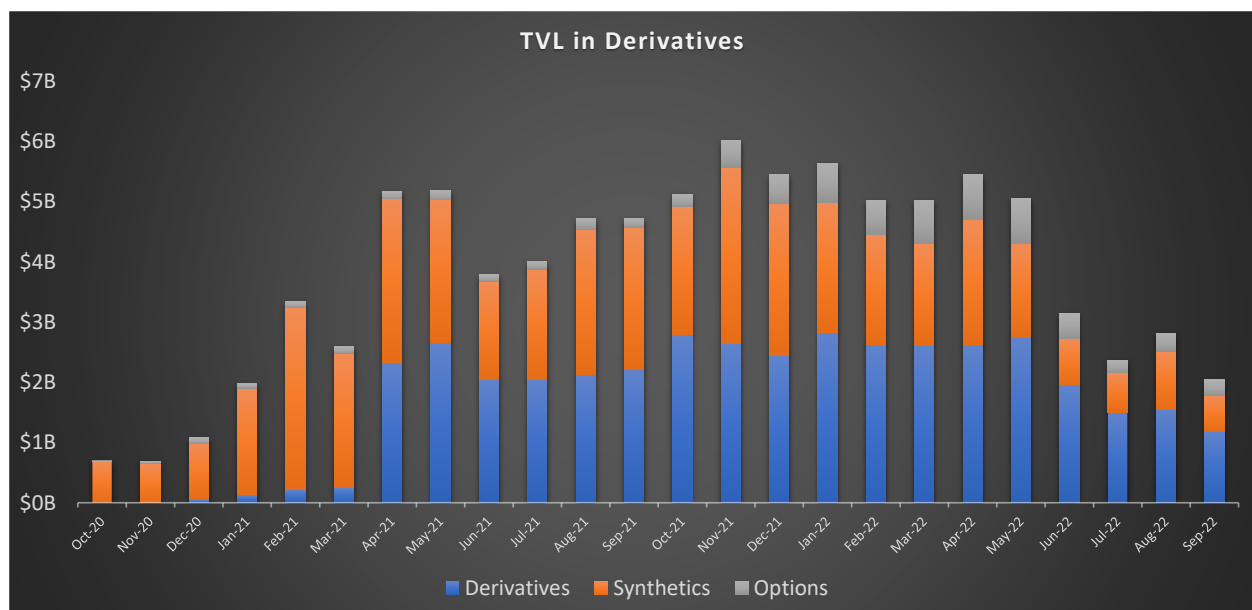
Source: Defillama as of 10.2.22

Although it has grown over 200% since 2020, the space is still relatively small. According to Defi Llama, as of October 2022 there is approximately ~$2B locked in derivatives – barely a speck of dust when compared to the $1 quadrillion traditional derivatives market.

While the potential of decentralized derivatives is immense, the technology has not yet caught up to the promise. In particular, current offerings suffer from high fees, capital inefficiencies, poor pricing and a general lack of the level of sophistication needed for professional users.

How Are They Different?

There are currently three major classes of crypto derivatives:

- **Perpetuals:** Futures with no expiration date
- **Options:** Calls, puts, etc…
- **Synthetics**: Instruments designed to mimic the value of other assets

_____

_____

Of these, the most novel may be synthetics.

Although synthetics do exist in the traditional financial world, they are often extremely expensive, complicated, opaque and limited to select clients. An infamous example of this is synthetic CDOs, a particularly convoluted instrument that many blame for financial crash of 2008.

On the contrary, crypto synthetics are relatively cheap, simple to design, easily auditable and – best of all – anyone can create and use them! For example, let's say that you wanted to design a token that tracks the price of oil, you would:

1. Deposit your collateral into a platform
2. Design a synthetic that tracks the price of oil through an off-chain data feed known as an oracle
3. Create and issue the synthetic to a liquidity pool
4. Allow traders to trade your newly created asset
5. Collect trading fees

There are already many tokenized synthetics that track assets such as gold, coins such as BTC and ETH and stocks such as Tesla or GameStop.

While there's a huge opportunity for synthetics in finance, "non-financial" use cases may be even more exciting.

Indeed, as Bankless points out in its writeup on [The Wild Future of Synthetic Assets](#), the fact that you can create a synthetic asset out of nearly anything that is measurable opens up a world of options beyond traditional finance. For instance:

- Politicians could incentivize public action by designing a token that rewards a desired behavior – for instance, one that increases in value with the vaccination rate

- Bookies could create "celebrity betting markets" that track the popularity of public figures by measuring their Twitter followers (and this would be difficult to regulate because of the decentralized and anonymous nature of synths)

The potential use cases are virtually endless, and the introduction of synthetic assets could spur a revolution in "user-generated finance", potentially transforming Wall Street in the same way that "user-generated content" disrupted Hollywood.

While synthetic assets offer an enormous amount of long-term potential, there are several kinks that need to be ironed out. One of the biggest issues today is capital efficiency, as the average synthetic requires over 600% collateralization.

_____

<u>Who are the Key Players?</u>
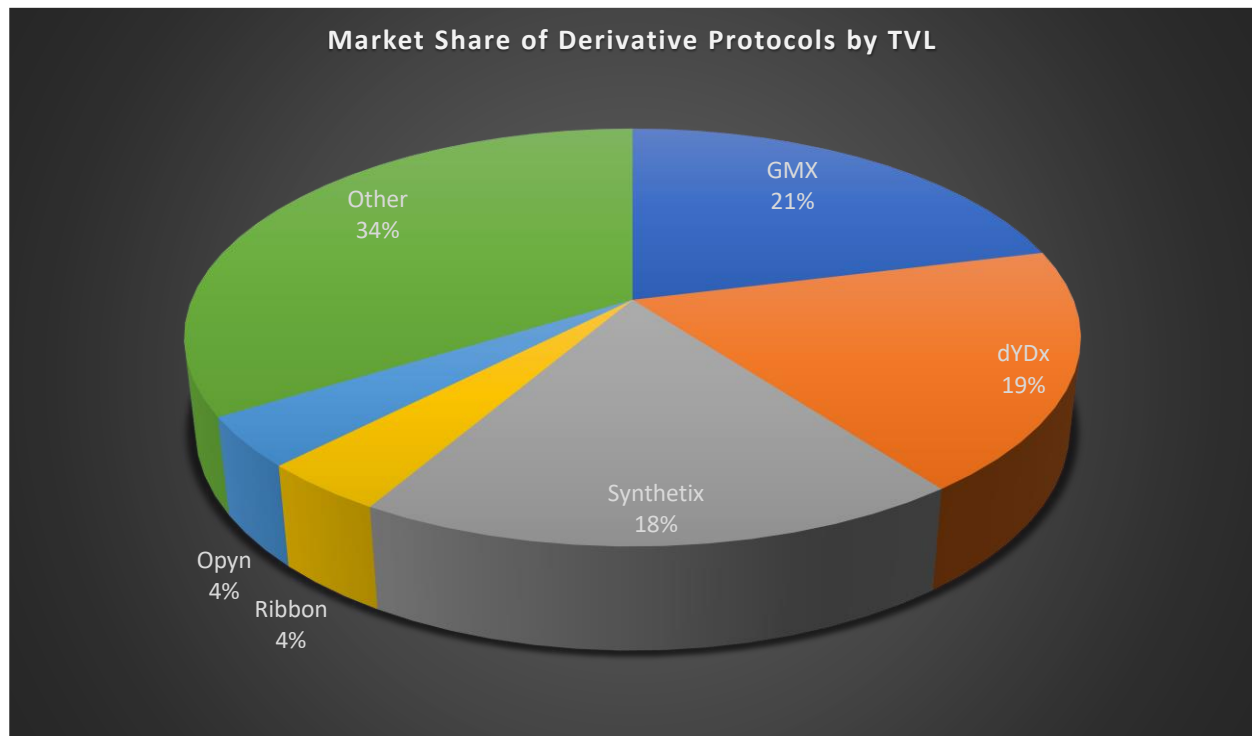
Source: DeFiLlama as of 10.2.22

Project	Market Share	Description
GMX	21%	GMX is a decentralized spot and perpetual exchange built on the Arbitrum and Avalanche blockchains
δY/δX	19%	dYdX is a decentralized derivatives exchange founded by an ex-Coinbase engineer. The project is backed by A16Z, Polychain and Bain Capital
SYNTHETIX	18%	Synthetix is an Ethereum-based decentralized platform that allows users to mint and trade synthetic assets
RIBBON	4%	Ribbon Finance provides structured crypto products such as covered calls or put selling
opyn	4%	Opyn is one of the first decentralized options trading platforms and is famous for launching "Squeeth", a product that squares a user's gains (or losses) on ETH

_____

Chapter 47: Yield Farming

Tokens don't offer dividends and few banks will let you put them in your savings account. So what's an investor seeking passive returns to do?

As usual, the DeFi community has created their own unique ways of earning interest, and they call these strategies "yield farming".

Four of the most popular strategies include:

- Staking
- Lending
- Liquidity Mining
- Incentive Programs
- Airdrop Farming

Staking

Many modern blockchains use a system known as "Proof of Stake" to maintain security. In this system, "validators" (who are effectively auditors) verify transactions, review data and confirm what needs to be added to the ledger. Validators receive rewards for doing this, but they must also put up collateral that may be seized if they are malicious or negligent. The act of putting up collateral is known as "staking", and if a Validator is competent and honest, it's a relatively risk-free way to earn interest on crypto

While running a validator node is generally way too complicated for the average user, there are many services such as Coinbase, Binance and Lido that allow users to lend their crypto to Validators for a piece of the fees.

Staking is generally considered the safest method of Yield Farming and rates generally range from 5% to 20% for established projects (and can exceed 50% for riskier projects).

_____

_____

Users Can Often Earn 5% to 20% from Staking

Staking Rewards of the Largest Smart Contract Platforms
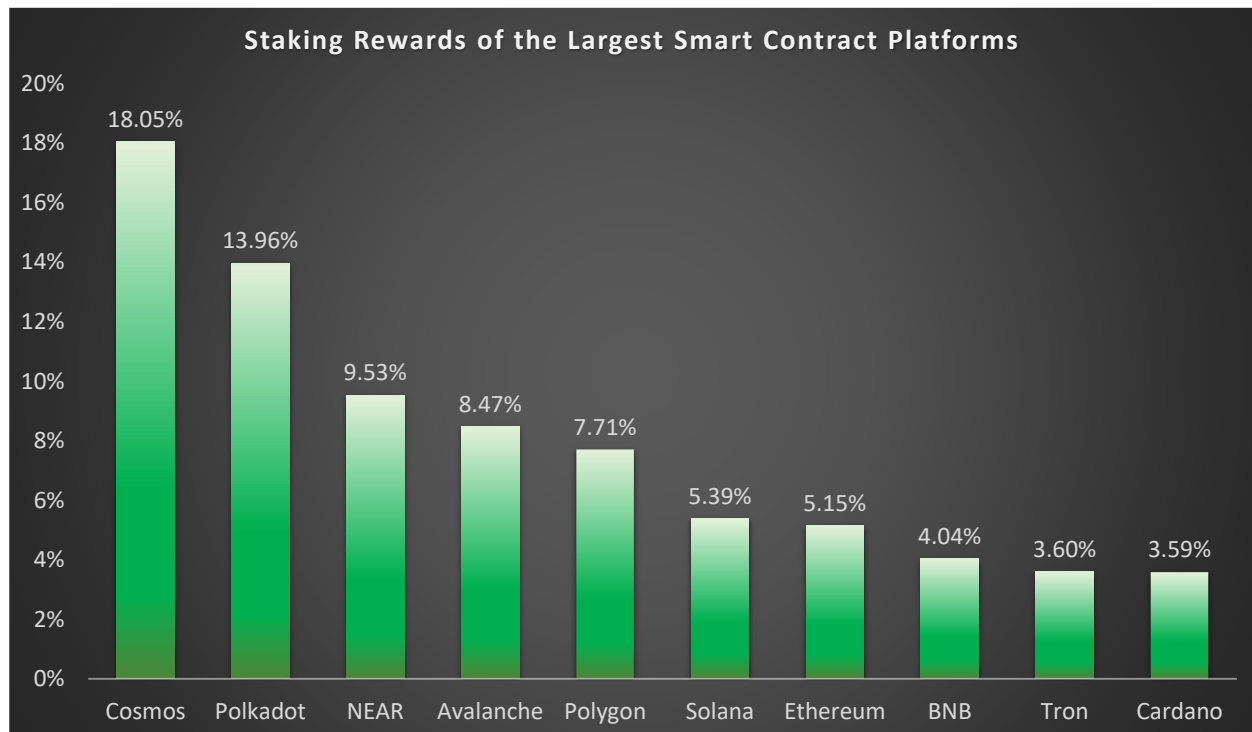
Source: Stakingrewards.com as of 10.2.22.

Lending

Despite having different mechanics, the results of lending crypto are similar in both the CeFi and DeFi worlds - you lend someone money and they pay you back with interest.

What is dramatically different is the rates. In early 2021, lending rates were outrageous – lenders could often earn over 40% APY!

While the market has become a lot more competitive and rates have dropped dramatically since then, lenders can still expect to earn between 3% to 5%. This is a decent return given that – as discussed – crypto loans have almost no default risk.

_____

_____

Crypto Lending Rates Range Between 3% and 5%
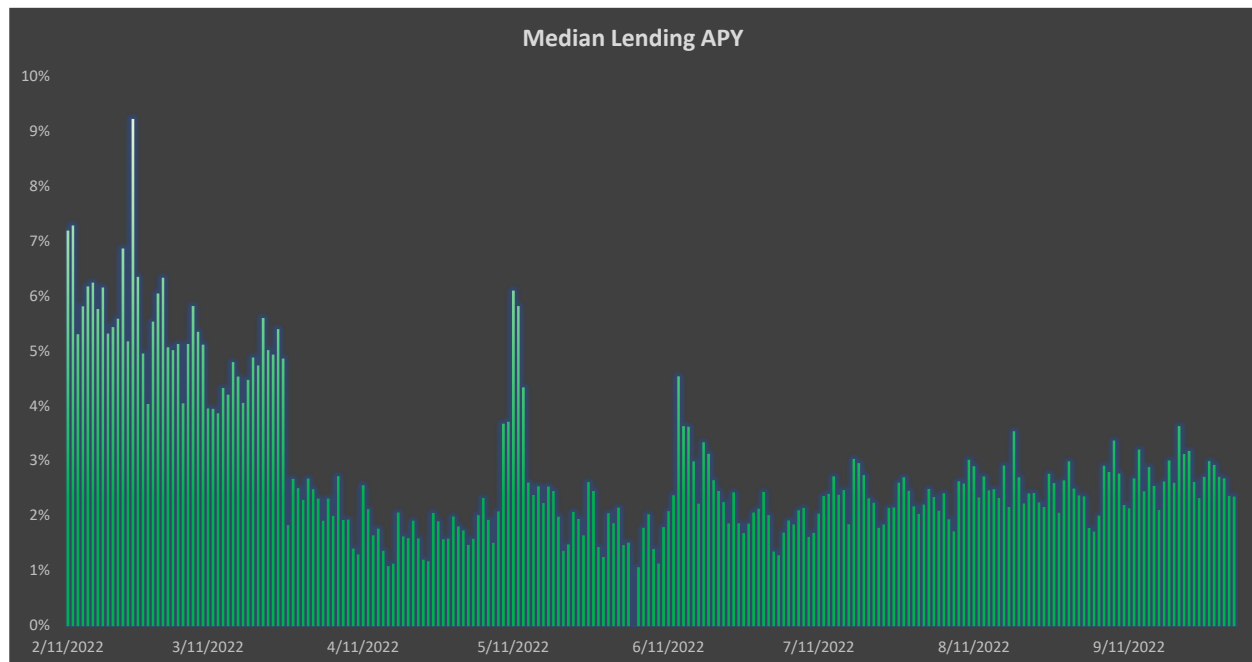
Source: Defillama as of 10.2.22

Liquidity Mining

Liquidity mining is yield farming's "high risk - high return" strategy.

Remember those liquidity pools we discussed earlier? In an AMM-based decentralized exchange, "liquidity providers" (also known as LPs or liquidity miners) deposit coins into a liquidity pool so that traders can trade them. As compensation for their deposit, LPs split the trading fees equally.

For example, let's say that 100 LPs deposit $1M of USDT and ETH into a liquidity pool on Uniswap. If there are $30M in trades over the next month, then the pool will generate $90K in profit at a 0.30% take rate. If an LP wants to exit at that time, she'll receive a 9% return in a month (>100% APR).

Return rates on liquidity mining vary wildly – stable pools on stable exchanges can have APRs ranging from 0% to 50%, while risky pools on risky exchanges can have short-term APRs exceeding 1,000%. Rates can also change dramatically from day to day. Finally, impermanent loss can eat into these returns, sometimes even resulting in a loss.

In the best cases though, the returns are robust. In this analysis from APY Vision, we see that the top 5 pools produced an average net return of 107%.

_____

_____

The Top 5 Liquidity Pools Have an Average APY of Over 100%
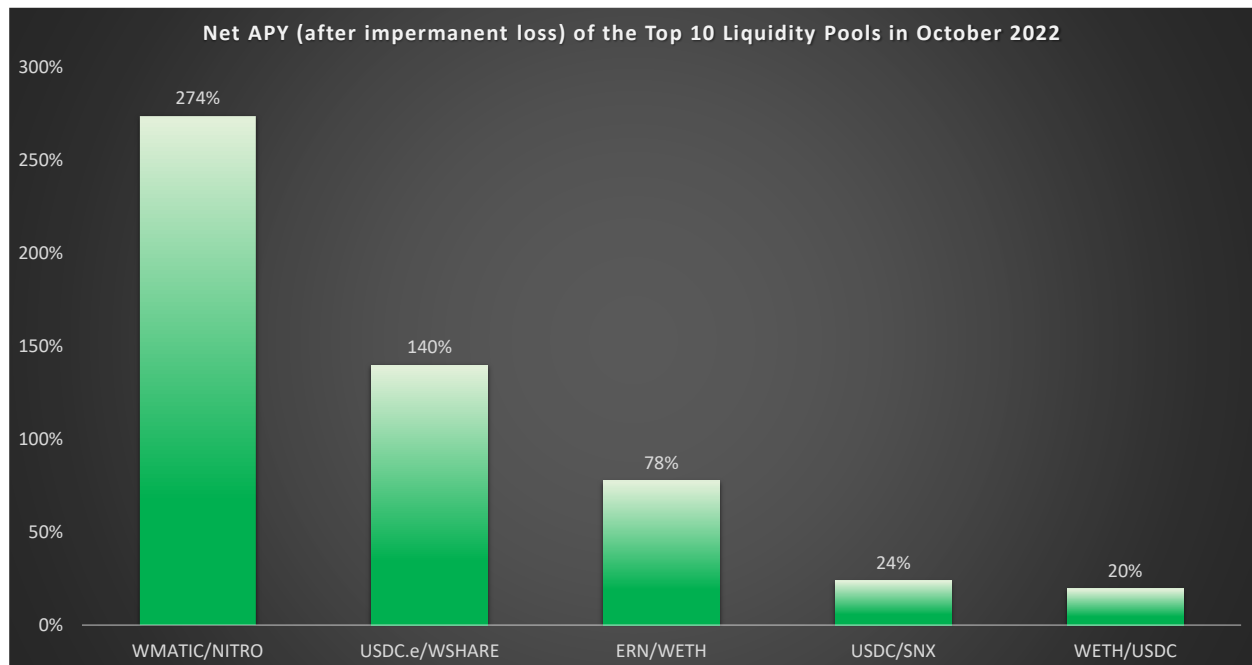
Source: APY Vision as of 10.2.22

Incentive Programs

Incentive programs can be seen as a form of marketing. New exchanges, or those that want to increase growth, often offer their native tokens as a bonus to liquidity providers. Most major DEXs, such as Uniswap, Sushiswap and Curve have all paid incentives at one time or another.

Incentives aren't limited to exchanges though. Let's say you're a new project that just listed your token on Uniswap. How do you get people to provide liquidity and trade your token? Simple, you bribe them!

When you compound these two sources, you can start to see extremely high yields.

For instance, let's say Synthetix is offering a reward program by giving free SNX tokens to anyone providing liquidity on their pool in Sushiswap, and Sushiswap is offering SUSHI tokens for anyone that provides liquidity to any of its pools. If you became a liquidity provider to the SNX-USD pool on Sushiswap then you'd earn:

- Interest from being an LP
- Free SNX tokens from Synthetix for supporting the project
- Free SUSHI tokens from Sushiswap for supporting the exchange

In effect, you're triple dipping!

When you hear about projects offering >100% to >1,000% APYs in DeFi, you can bet you're dealing with an incentive program like this.

_____

Unfortunately, these funds are almost always limited, so these deals rarely last, and token prices often crash when the music stops.

<u>Airdrop Farming</u>

It's debatable whether this last category actually qualifies as yield farming, but it's an interesting topic nonetheless.

Airdrops are a hybrid IPO / marketing strategy where coins are dropped into the wallets of existing users. One of the most recent and famous examples of an airdrop was conducted by Ethereum Name Services.

Basically, anyone who had bought an ENS domain prior to the airdrop got free tokens. While most domains cost <$200 to purchase, these value of tokens shot up to almost $20,000, a 100x return. Some people that bought multiple domains made hundreds of thousands of dollars.

This strategy is unheard of in the traditional world. Imagine if Nike were a private company, but instead of IPOing they decided that they were just going to give shares to everyone that bought a pair of shoes!

As a result of ENS and other high-profile airdrops, many crypto fans are using services with the hope of benefitting from the next one. Some contenders that are frequently cited are Metamask, OpenSea, Rabbithole and Arbitrum.

<u>Conclusion</u>

Interest is serious business when it comes to DeFi. At the peak of the bull market, yield farmers were easily earning double to triple-digit interest rates. Even the safest options today can offer yields that substantially exceed traditional finance.

For example, being a liquidity provider to a stablecoin pair is one of the safest plays in crypto. Because you're holding two stablecoins, there's no risk of loss of principal (they're both tied to the dollar), and there's no risk of impermanent loss (because the assets move in tandem). Outside of the threat of an exchange being hacked – which, to be fair, is a real consideration – this should have the same risk as holding dollars in a savings account.

While the difference isn't as stark as it once was, we can see that the best performing stable asset pools still offer significantly higher rates than the top online savings accounts.

_____

<u>Traditional Savings Account vs. DeFi Savings Accounts</u>

Top Online Savings Accounts

SoFi ⠿   ally   Marcus:
                              by Goldman Sachs®

2.50%   **2.25%**   **2.15%**

Top Stable Asset Pools

Ⓒ$ FRAX/USDC   €$ USDC/DAI   T€$ DAI/USDT/USDC

8.73%   **8.35%**   **3.34%**

Source: [APY Vision](#) as of 10.2.22

How is this all possible though? How can DeFi afford to pay out so much?

Well, there are several possible reasons, including: 1) unstated risks such as smart contract risk, impermanent loss, etc… 2) temporary arbitrage opportunities due to the immaturity of the market and 3) unsustainable, short-term incentive payments for marketing purposes.

As Vitalik pointed out:

_____

_____

> **vitalik.eth** ✓
> @VitalikButerin
>
> Honestly I think we emphasize flashy defi things that give you fancy high interest rates way too much. Interest rates significantly higher than what you can get in traditional finance are inherently either temporary arbitrage opportunities or come with unstated risks attached.
>
> 1:44 PM · Jun 20, 2020 · Twitter Web App

Many of these concerns have proved prescient, and DeFi yields have dropped significantly in the past year (indeed, as recently as six months ago, stablecoin pools were offering returns that were 20x to 30x greater than online savings accounts).

Still, it's difficult to believe that at least some of this alpha isn't permanent. After all, the average bank is very bloated — "non-interest" costs such as corporate overhead, legal services, occupancy costs, regulatory fees and intermediary compensation average around 60% of revenue today. By eliminating the middleman and automating transactions, it's likely that DeFi can purge many, if not most, of these costs. This should free up more profits for the consumer which, in turn, should translate to higher rates.

_____

_____

Chapter 48: Flash Loans

Flash loans are an entirely new financial product that lets users borrow substantial amounts of capital with no collateral for extremely short time periods (i.e. measured in seconds).

This new product is only possible due to the unique properties of smart contracts, which allow borrowers to execute multiple steps within the same transaction.

For example, let's see you notice that the price of USDC is $1.00 on Uniswap and $1.01 on Sushiswap. You could code a contract to:

1. Borrow $100 million on Aave
2. Buy 100 million tokens of USDC on Uniswap for $100 million
3. Sell 100 tokens of USDC on Sushiswap for $101,000,000
4. Repay your $100 million loan on Aave
5. Profit a cool $1 million

This works because these steps occur almost instantaneously and within the same smart contract transaction, so there's no execution or repayment risk. If the code determines this isn't possible, it simply won't execute or will return the funds to the lender as if the transaction never happened.

Although the market has slowed down a bit, Aave has still issued more than $5B of flash loans in the last 18 months.
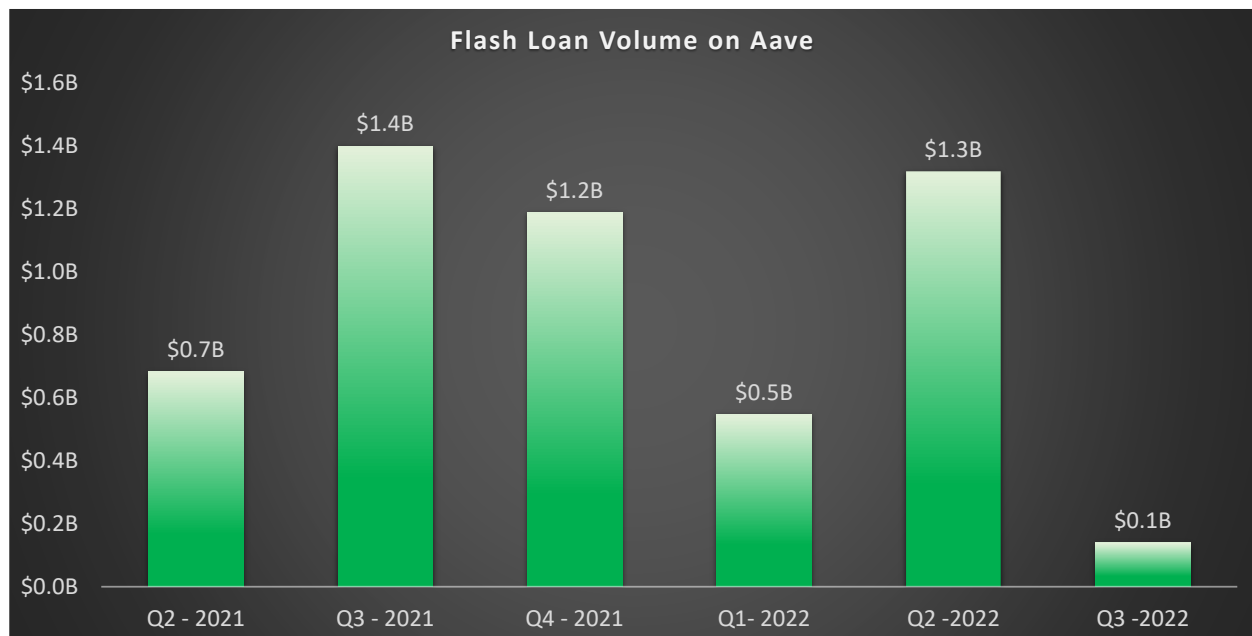
Source: Footprint Analytics as of 10.2.22

Nothing close to this exists in traditional finance. Imagine walking into a bank and saying "hey, I'd like to borrow $100M for 10 minutes – I'm not going to give you any collateral and not even going to tell you my name" and getting the loan!

_____

_____

Chapter 49: Money Legos

One of the most exciting applications of DeFi is a phenomenon known as composability, or in Web3 parlance, "money legos".

DeFi protocols run using open-sourced software, which means that any of the apps listed above can be easily programmed to interact with others. As such, you can think of each individual app as a "lego brick" that can be combined with others in an infinite number of ways to create more complex and innovative financial products.

One example of the benefits of composability can be seen in the creation of Yearn Finance.

Yearn began as a passion project. The original program was designed by Andre Cronje to automate the process of identifying the lenders (e.g. Aave, Compound) with the highest returns and moving his tokens to them.

Other users noticed his success and began to contribute funds and join him, and the project soon expanded to liquidity mining on AMMs such as Curve and Balancer.

Eventually, this developed into more complicated, actively managed strategies known as vaults. One of the more popular vaults – known as Yearn ETH – used Ethereum to create Dai, then used the Dai to invest in Curve's Y pool, which provided interest and rewards in the form of the CRV token, which were then staked to Curve Gauge to earn even more interest and rewards.

While the strategy eventually petered out and shut down, at one point it was earning users a 60% annual yield on ETH!

_____

_____
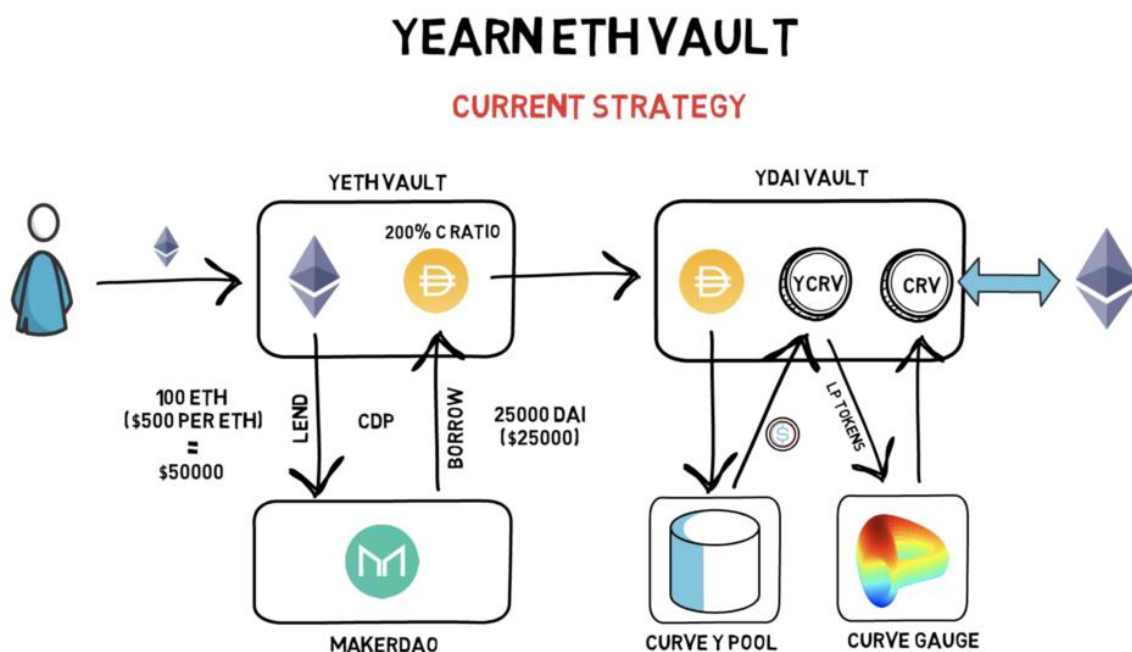
Source: Finematics

Oh, along the way Yearn also issued a token which increased to over $3B in market cap within its first year…

So Andre created a multi-billion dollar crypto-hedge fund without needing to register with any authorities because he could freely access and move tokens between protocols.

And that's the great thing about DeFi and composability in particular – innovation is practically unlimited as it's no longer constrained by the imagination of a few select individuals locked deep within the bowels of the banking system.

_____

Chapter 50: DeFi Infrastructure

In order to achieve its potential, DeFi needs several key pieces of infrastructure including:

- **Smart Contract Platforms**: Smart contract platforms are the decentralized computers that run all of the applications listed above. They are used to create, store and facilitate the exchange of DeFi tokens

- **Oracles**: Oracles connect blockchains to real-world data sources. They can retrieve a variety of information including, price reports, weather, sporting scores, results of elections, geodata, random numbers, etc…

- **Data Aggregators**: Like a blockchain-based version of Google, data aggregators use a process called indexing to make it easy for developers and users to quickly search a blockchain for important data

- **Interoperability Protocols**: Interoperability protocols, also known as "bridges", are systems designed to allow the transfer of information and assets between two or more blockchains

We will cover all of these tools in depth in Part 7: Web3 Infrastructure.

_____

_____

Chapter 51: Why DeFi will Eat Wall Street

<u>Why Wall Street Won't Survive</u>

I believe that DeFi represents a classic case of disruptive innovation that has the potential to change our lives in ways we can't even imagine.

Like most disruptors, it definitely has a ton of problems today – such as smart contract risk, rug pulls, irreversibility and the potential for abuse.   But it also has several advantages that traditional finance simply cannot replicate, such as:

- **Unmatchable Rates**: The almost total elimination of intermediaries such as bankers, brokers, lawyers, regulators, accountants, etc… will allow DeFi to offer customers rates that are significantly greater than traditional banks

- **Unprecedented Customer Experience**: Instant, permissionless, 24/7 access to financial products and markets and the ability to remain completely anonymous create a banking experience that no one alive has ever seen. And while this compelling on its face, I believe that like smart phones, ATMs or the internet, we won't truly understand the utility DeFi can bring to our lives until we've experienced it at scale

- **New Sources of Innovation**: Not only is DeFi unburdened by regulation, knowledge is freely shared and there's an ability to crowdsource the ideas of millions of users to rapidly create and test better financial products. As such, it's not inconceivable that DeFi could catalyze a user-driven financial "renaissance". If you don't think this is possible, consider how a bunch of kids recently used Reddit to beat world's biggest hedge funds at their own game…

Perhaps most importantly, Wall Street can't replicate DeFi without cannibalizing itself, and regulators can't stop its progress due to its decentralized nature.

As such, I simply don't see how traditional banking can survive.

<u>Almost Unmeasurable Potential</u>

It's difficult to describe the potential impact of disruptive technologies without sounding hyperbolic at best and insane at worst.

But there are some people that are very bullish on DeFi. For example, the <u>World Economic Forum estimates</u> that $867 Trillion could eventually be transferred to decentralized financial markets. Given that the space is a mere $54.8 Billion at the time of writing – 0.06% or approximately 1/15,000th of the WEF's estimates – there's definitely a lot of room to grow.

_____

_____

Decentralized Finance Represents a Fraction of the Global Financial Markets

Value of Global Financial Markets

DeFi	$54.8B
Global Equities	$106T
Global Debt	$253T
Derivatives	$1,000T
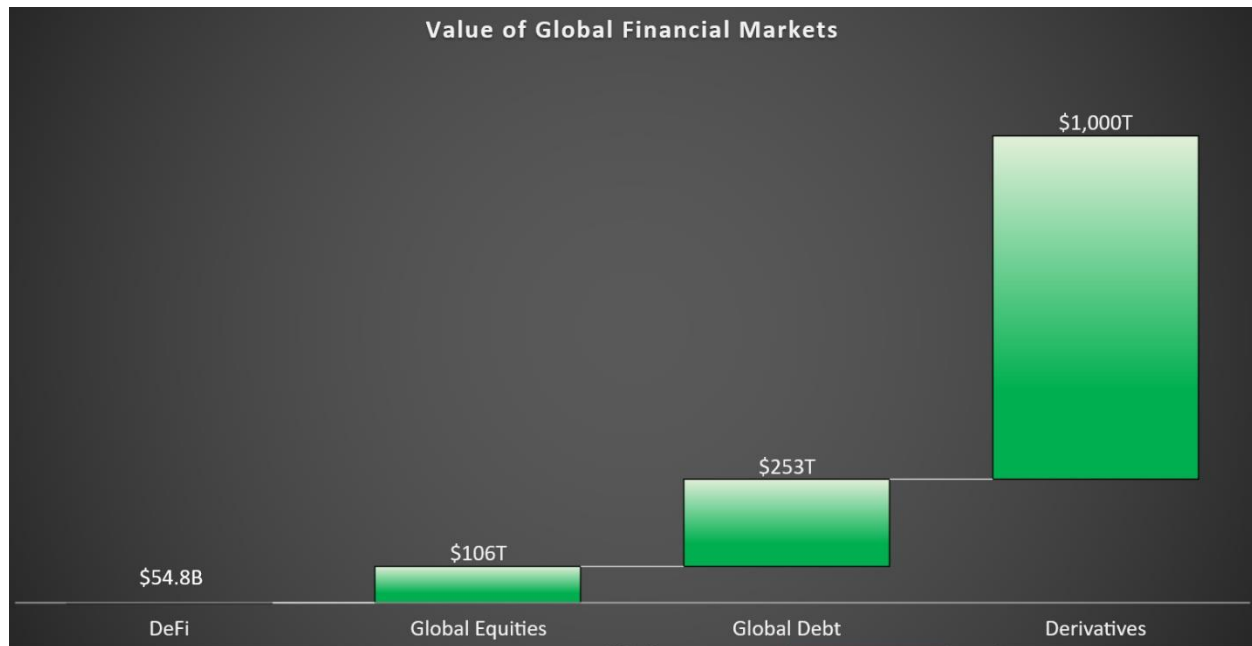
Indeed, DeFi could grow 100x from here (to $5.5T) and be worth roughly 5% of the total stock market …

…it could grow 1,000x from here (to $55T) and be only 20% of the global debt market …

…it could even grow over 10,000x from here (to $550T) and represent a little over half of the value of the derivative markets today.

Wherever this thing ends up, it's important to watch as it has the potential to be both an existential threat to Wall Street and a road to almost unlimited potential for investors.

_____

Part 6: Decentralized Autonomous Organizations

_____

Chapter 52: What is a DAO?

A DAO is a blockchain-based organization that may replace the modern corporation.

Unlike a traditional corporation, **no single person or group owns or controls a DAO**. They do not have CEOs, Boards or managers. Instead, they are owned and operated by members who make decisions democratically (much like a modern-day cooperative).

This allows for many exciting innovations such as user-owned social networks, vendor-owned eCommerce sites, player-owned games and driver-owned ride sharing companies.

<u>DAOs Eschew the Hierarchy of Traditional Corporations</u>
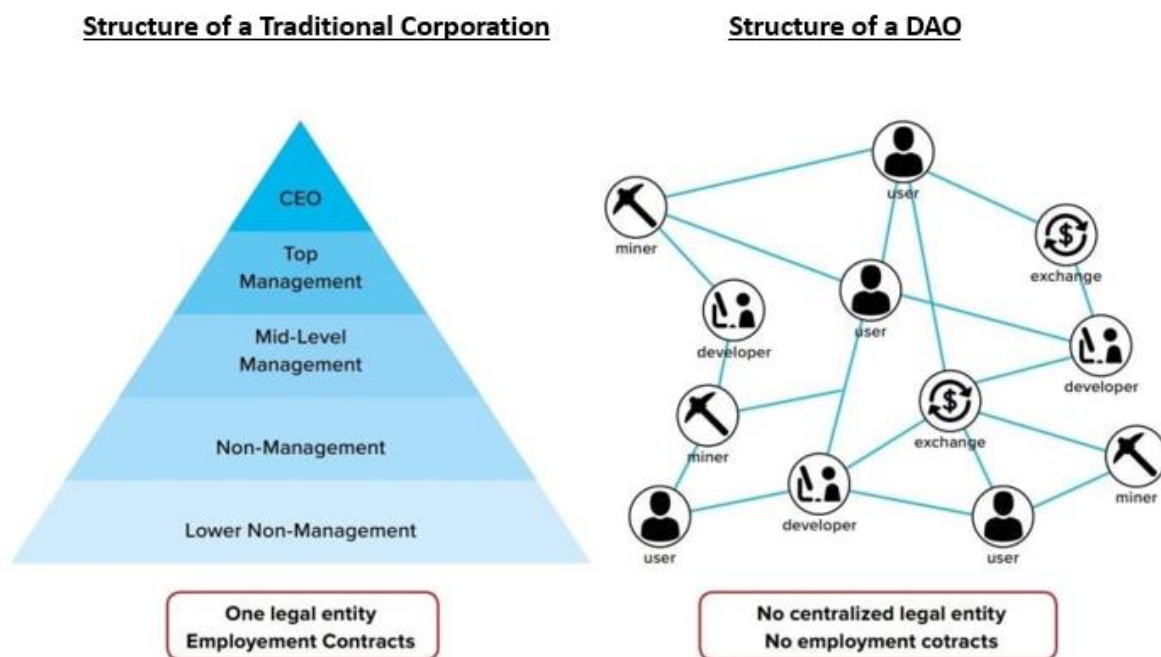
Source: Hritwik Tripathi

Furthermore, DAOs use blockchain technology to store their own funds and smart contracts to enforce their own laws – meaning that they don't have to rely on traditional intermediaries such as banks or courts. As such, **DAOs largely operate outside of the purview of the existing financial and legal ecosystem**, allowing them to eliminate many of the costs, restrictions and regulations imposed on conventional organizations.

The term stands for "decentralized autonomous organization", as **DAOs are sovereign entities** with:

- **No Headquarters**: DAOs have no physical location – they are composed of members from all over the world who coordinate through internet chatrooms

_____

_____

- **No Hierarchy (or Limited Hierarchy)**: Decisions are made democratically, and each member can propose, discuss and vote on initiatives

- **No Employment Contracts**: Anyone can contribute and get paid and workers are free to come and go as they please

- **No Governing Law**: DAOs aren't incorporated in any particular location and, as such, operate outside of the purview of the existing legal system

- **No Banks**: DAOs raise their own capital through cryptocurrency or NFT sales and self-custody these funds in a treasury

Proponents assert that DAOs are superior to traditional corporations because they retain all of their benefits while being much more flexible, transparent and democratic (in fact, Mark Cuban called them the "ultimate combination of capitalism and progressivism"). Critics argue that DAOs will be inefficient, prone to crime and represent a legal and regulatory nightmare.

Whatever side of the argument one falls on, the popularity of DAOs is undeniable. There are nearly 5,000 DAOs today representing 3.9 million members (up nearly 300x from January 2021). DAOs have been formed to manage a variety of initiatives including investment funds, charity organizations, entertainment studios, worker collectives, social clubs and operating businesses.

Total assets under management exploded in 2021, growing from $400 million in January 2021 to a peak of $13 billion in November 2021 (30x growth). Even today, during what many are calling a bear market, DAO treasures hold nearly $10 billion in funds (~ 25x growth from January 2021).

DAO Treasuries Hold Nearly $10 Billion in Funds (up 25x from 2021)
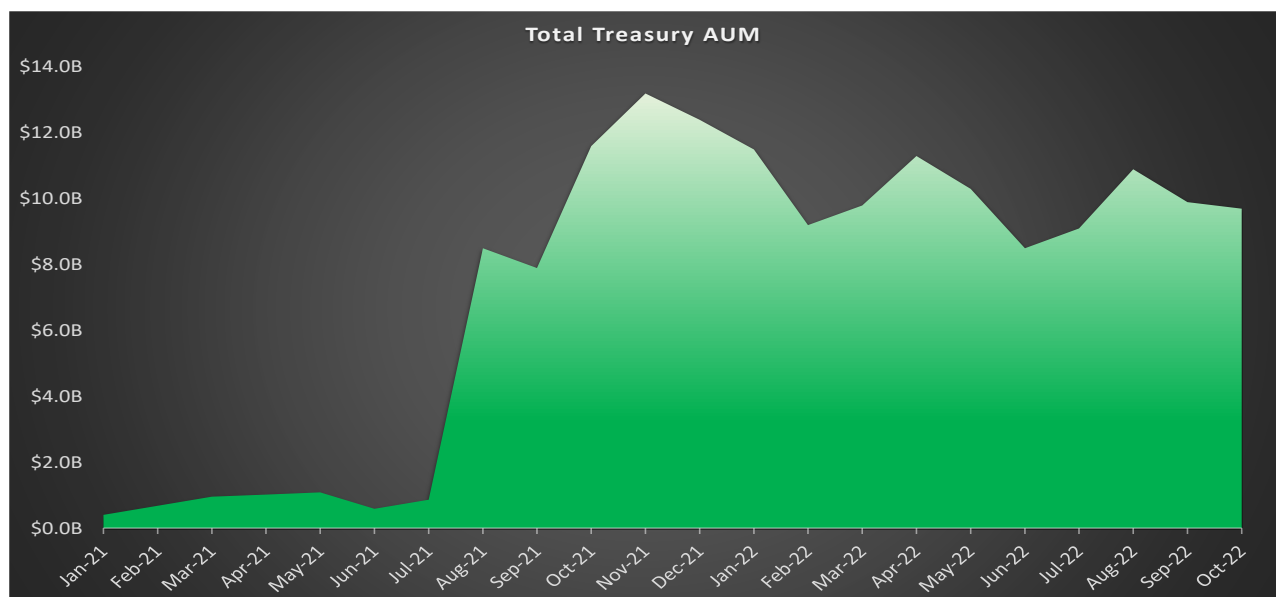
Source: DeepDao as of 10.2.22

_____

_____

Chapter 53: The Problems with Traditional Corporations

Unlike many in the crypto space I don't hate corporations. In fact, I think that they are one of the most important economic innovations in history as **they enable large groups of people to work together to accomplish a common goal**.

One of the ways they do this is by serving as a "nexus of contracts". Corporations help coordinate the vast array of contracts that exist between the disparate (and often adversarial) group of stakeholders required to run a sizable business. This includes owners, management teams, employees, customers, suppliers, investors, creditors, etc…

Because these contracts are backed by a well-developed system of laws and enforced through the courts, they essentially allow a diverse group of strangers to trust one another and do business in a complicated, and often global, business environment.

Corporations Form the "Nexus of Contracts" That Allows Diverse Stakeholders to Trust One Another
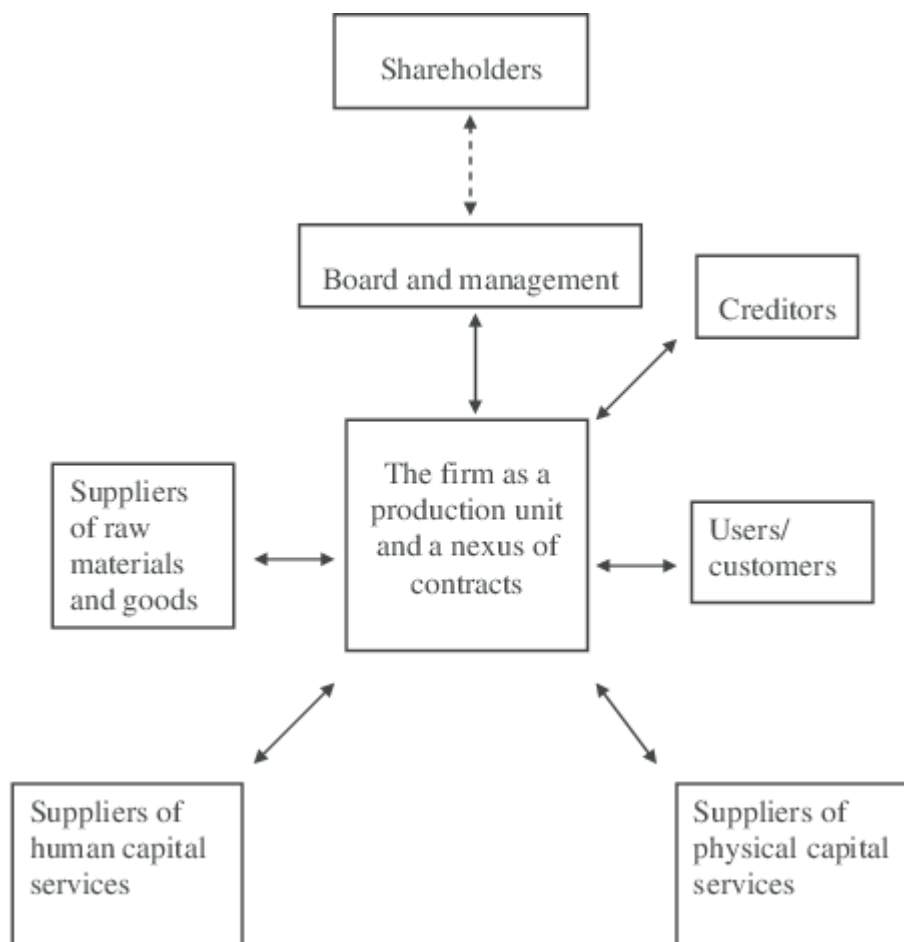
Source: ResearchGate

_____

Indeed, corporations work closely with the banking and legal system to provide covenants that protect:

- **Owners**: Partnership agreements guarantee that each of the owners of a business will receive his or her fair share of the profits. In modern corporations, they also provide limited liability protection, meaning that an owner's personal assets can't be seized in a judgement against the entity

- **Investors:** Investor agreements protect both corporations and sponsors by clarifying the amount of investment, key terms and conditions, the percentage of ownership received and the requirements of both parties to consummate the transaction

- **Employees**: Employment contracts ensure that workers will get paid for labor performed and that management will have recourse in the case of negligence or bad faith

- **Customers and Suppliers**: Customer and supplier agreements guarantee that the product will be delivered as promised and at the agreed upon price

- **Funds:** Corporations serve as the legal entity that interacts with the banking system and the only "person" that can access an organization's funds and transfer capital. In addition, corporations also serve as a fundraising vehicle – instead of each individual raising money separately, they provide a single point of contact for financial markets

- **Technology**: Intellectual property agreements protect the intangible assets of a corporation such as trademarks, copyrights, patents and trade secrets

With all these stakeholders, it's no surprise that the average Fortune 2000 company has 20,000 to 40,000 active contracts at any given time!

Unfortunately, managing the administrative, legal and regulatory requirements of all of these contractual relationships requires a lot of bureaucracy and overhead, and this makes corporations quite inefficient. In particular, they are often:

- **Slow**: Hierarchical layers slow communication and new ideas must often pass-through multiple rounds of approval before being implemented

- **Expensive**: Upper and mid-level managers can be very expensive, often comprising the bulk of payroll cost while representing a relatively small portion of the total employees

- **Unimaginative**: Top-down decision-making reduces innovation, often spurring a vicious cycle where employees lose motivation as their interests depart from the firm

- **Restrictive**: Corporations are often subjected to strict regulatory requirements for hiring and retaining talent (especially international talent), contributing to a "sticky" labor market

_____

- **Opaque**: Most businesses tightly guard internal information and financial results, and public corporations are only forced to report on a quarterly basis

- **Disjointed**: The larger a corporation gets; the less employees align with the vision

- **Highly Regulated**: Larger firms are much more vulnerable to regulation by governments, banks and other third parties

Together, these concerns represent a major problem – not only do they curb economic growth, but they also limit access for workers and contribute to inequality.

Unfortunately, we are all but forced to accept these consequences as corporations – in close partnership with banks and governments – have historically represented the best (if not only) way to provide the level of trust needed to organize a globally diverse group of economic actors.

So while some may call corporations "evil", up until now they have been a "necessary evil".

_____

_____

Chapter 54: The Benefits of a DAO

This all changed in 2015 with the launch of Ethereum and its "smart contracts".

Smart contracts are digital agreements that execute automatically when pre-determined conditions are met. For instance, you could program a smart contract to automatically pay an employee each time she launched a new product or feature, or automatically pay a supplier each time a product is delivered.

Unlike traditional contracts, smart contracts don't rely on corporations, banks, lawyers, courts or local laws to guarantee their enforcement. Instead, users **trust the technology** and its pre-programmed code to automatically execute when they've upheld their end of the deal.

Smart Contracts Don't Need Lawyers, Brokers, Banks, Courts or Governments
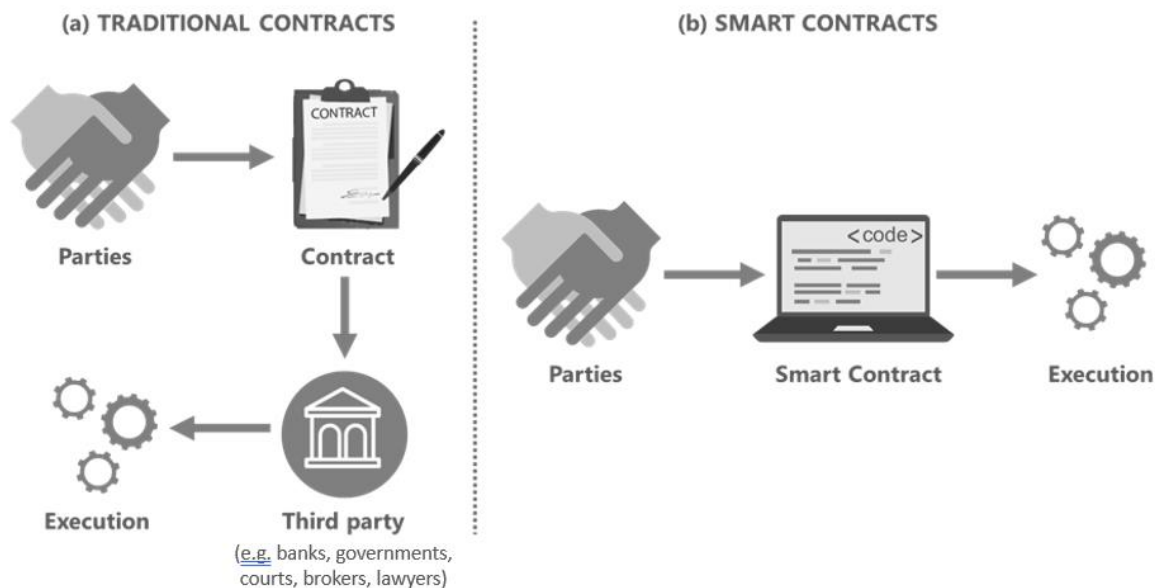
Source: Techskill Brew via Medium

The terms of a smart contract are fully transparent and accessible to all parties, and they will always execute exactly as programmed. Because they are created using blockchains, no one can alter these terms without consent from everyone involved.

Smart contracts make it possible – for the first time in history – to **organize a global and diverse group of economic actors without relying on third parties such as corporations, banks, governments and courts to establish trust**.

The effect of this cannot be overstated and requires thinking from first principles. Imagine for a bit, how you would design a corporation if you no longer needed traditional contracts or intermediaries:

_____

- After all, what's the point of registering as a legal entity if you can enforce your own laws through smart contracts?

- What's the point of partnership agreements if you know that ownership is fairly distributed?

- What's the point of employment contracts if workers are guaranteed to get paid when they complete their work?

- What's the point of entering into a banking relationship if you can hold your own funds and pay your workers directly?

- What's the point having investment banks draft complicated Private Placement Memoranda if you can raise your own capital?

- What's the point of a CEO and management team if there's no legal and regulatory bureaucracy to manage?

If you're like me, you're probably envisioning something much simpler and more elegant than what we have today…

In short, a "corporation" without managers, employment contracts, banks or legal and regulatory restrictions.

That entity is known as a DAO, and it may allow us to reap all the benefits of a traditional corporation – namely trust, security and growth – while removing most of the downsides. Indeed, DAOs are:

1. **Global:** DAOs are composed of individuals with different backgrounds, skills and viewpoints from all over the world

2. **Democratic:** Decisions are made democratically, and each member can propose, discuss and vote on initiatives

3. **Aligned:** In an ideal DAO, every member is an owner. Unlike traditional hourly or salaried workers, DAO contributors are all incentivized to contribute to a common goal – the overall growth of the enterprise

4. **Open:** Many DAOs don't have a hiring process, anyone can join, work and get paid

5. **Flexible:** DAO "employees" are free to come and go as they please, work for multiple DAOs and work as little or as much as they want

6. **Transparent:** All of a DAOs rules and transactions are recorded on a blockchain and its smart contracts, making them easy for anyone to audit and review. In addition, unlike traditional corporations, this information is accessible in real-time

_____

7. **Sovereign:** DAOs exist outside of the purview of the traditional financial and legal systems. While this may not seem very important in certain parts of the world, it can be a huge benefit to citizens of developing nations who face a very real threat of arbitrary regulation (e.g. because they hold political views that oppose the current administration)

8. **Self-Custodied:** In the current financial system, corporations don't really hold their funds – the banks do. This means that they can shut down, freeze and even seize an organization's asset at will. While this may seem far-fetched, consider that in 2013, the Government of Cyprus seized 47.5% of all bank accounts over €100,000 to bail-out its failing banking system

9. **Faster:** Because smart contracts execute instantly, they can save hours of various business processes

10. **Cheaper:** Smart contracts remove the needs for lawyers, bankers and brokers, making them much cheaper

To help you understand more about how DAOs can transform the world, let's go a bit deeper down the rabbit hole…

_____

_____

Chapter 55: How Does a DAO Work?

In many ways, DAOs operate the same as a traditional organization.

"For-profit" DAOs must define their mission, raise capital, create a strategy, build a product or service and then sell it for a profit. Investment DAOs need to find LPs, identify promising projects and invest in them.

As such, many DAOs are beginning to organize similarly to conventional corporations, and divide themselves into working groups corresponding to the primary functions of the business (e.g. strategy, sales & marketing, operations and finance).

<u>Larger DAOs are Often Organized into Functional Divisions</u>
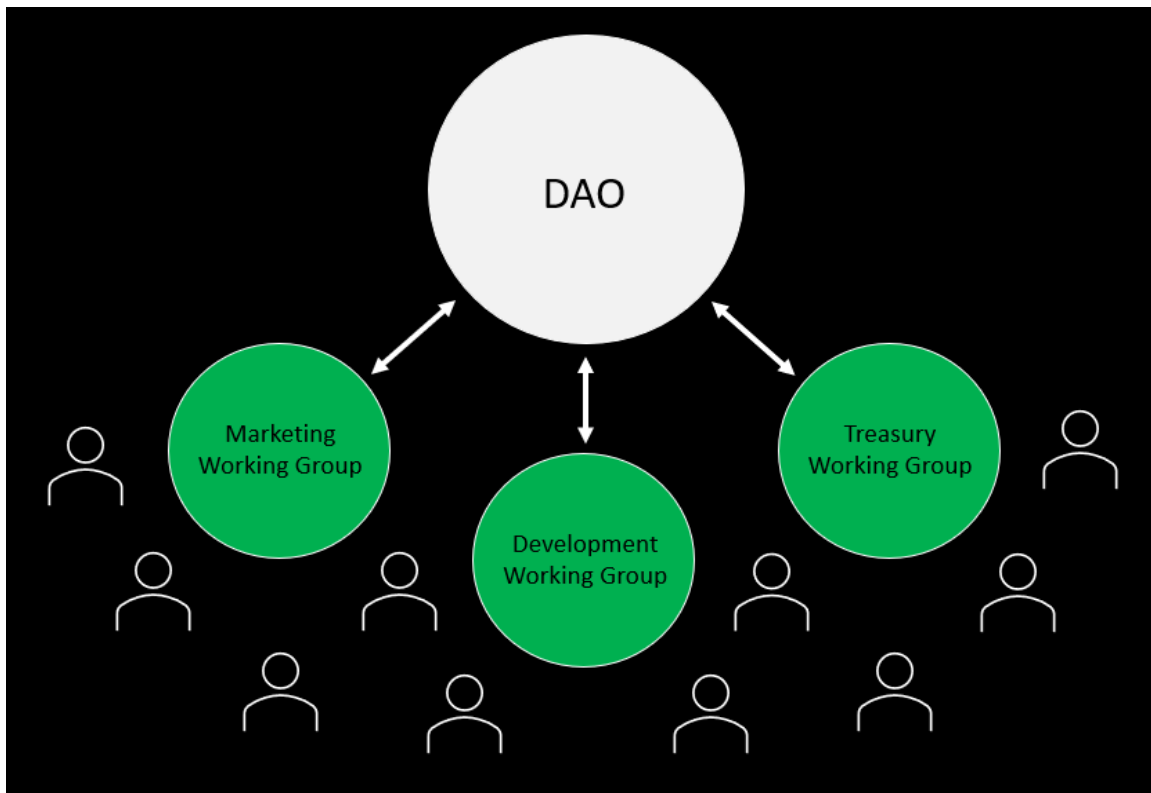
The most apparent difference between a DAO and a traditional organization is its decentralized nature. Unlike traditional organizations, DAOs are fully-remote entities – they have no headquarters, office or physical location and members often live all over the world.

In addition, they rarely have CEOs, Boards or managers. Instead, they are owned and operated by members who make decisions democratically.

While this may seem progressive, it's not exactly novel, as this system has existed for quite some time in the form of a cooperative. In fact, many prominent organizations today – including Nationwide, Land-o-Lakes and the Green Bay Packers – are organized as coops.

_____

_____

What truly makes a DAO disruptive then, is its *autonomous* nature. While many people disagree on the meaning of this term – some believe it describes an entity almost fully administered by machines or AI – a more modest take is that it simply means that **the organization has automated away unnecessary internal and external bureaucracy** by replacing traditional contracts with smart ones.

Indeed, from a technical standpoint, a DAO is essentially little more than a collection of smart contracts built on the blockchain of a decentralized platform such as Ethereum.

These contracts can be programmed to replace several processes in an organization and are used to:

1. **Define Rules**: DAOs don't need to register as a corporation, domicile in a particular jurisdiction or create an operating agreement. Instead, ownership percentages, member rights and responsibilities, voting rules and allocation protocols are coded directly into a smart contract

2. **Raise Funds:** Unlike traditional corporations, who generally raise capital through private placements or IPOs, DAOs don't use investment banks or the financial markets to raise funds and distribute ownership. Instead, they typically raise funds by creating and selling their own cryptocurrency token or NFT

3. **Store Funds**: DAOs don't use banks to hold their funds. Instead, they custody and manage their own assets on a blockchain, and the community democratically makes decisions on how to employ this "treasury"

4. **Govern**: As mentioned, most DAOs don't use a Board, CEO or Executive team to define strategy or make decisions. Instead, they power their non-hierarchical, democratic governance structure with a smart contract designed to tally voting results, record them onto the blockchain and sometimes even execute the decision

5. **Attract Workers**: Unlike traditional corporations, many DAOs don't have employment agreements and instead rely on smart contracts to compensate workers in cryptocurrency tokens or stablecoins. In theory, this allows anyone to join a DAO, come and go as they please, work as little or as much as they want and even choose to remain anonymous

6. **Pay Workers**: Many DAOs are using smart contracts to develop innovate new compensation structures such as bounties (payment per task), peer-based compensation (where team members collectively vote on the allocation of the DAO's budget) and "streamed" salaries (automated payments made in real-time)

7. **Distribute Funds**: DAOs can use smart contracts to transfer cryptocurrencies and stablecoins for virtually any purpose they deem necessary. This includes making distributions to owners, providing grants to developers, incentivizing customers, paying suppliers and partners, etc…. Because these payments bypass the traditional banking system, they theoretically aren't subject to local regulations or restrictions on international currency transfers

_____

_____

8. **Execute Operations**: Some DAOs – notably "protocol DAOs" such as the decentralized exchange Uniswap – run a significant portion of their business using smart contracts. In these cases, the DAOs could program one smart contract to interact with the others (for instance, a successful vote to increase the take rate made through the voting protocol would automatically update the smart contract responsible for administering fees)

In practice, not every DAO satisfies all of the above conditions – many today are not fully decentralized nor autonomous.

But proponents are quick to remind us that we are still very early, and thousands of entrepreneurs are experimenting to find the perfect form that blends: 1) the strengths of a traditional organization, 2) the democracy of decentralized ownership and 3) the efficiency of autonomous execution through smart contracts.

In fact, the marriage of these three features is where DAOs get their name – *Decentralized Autonomous Organizations*.

For more detail on how DAOs are used in practice, let's head to the next section…

_____

_____

Chapter 56: DAO Ecosystem

The DAO landscape is flourishing – there are currently almost 5K DAOs representing nearly $10B in capital and 3.7 million members. DAOs have been created for a variety of purposes including the management of companies, investment funds, collector groups, charities, media studios, talent agencies and social clubs.

One DAO even tried to buy the US constitution and almost did it!

<u>A Small Sample of the DAO Landscape</u>
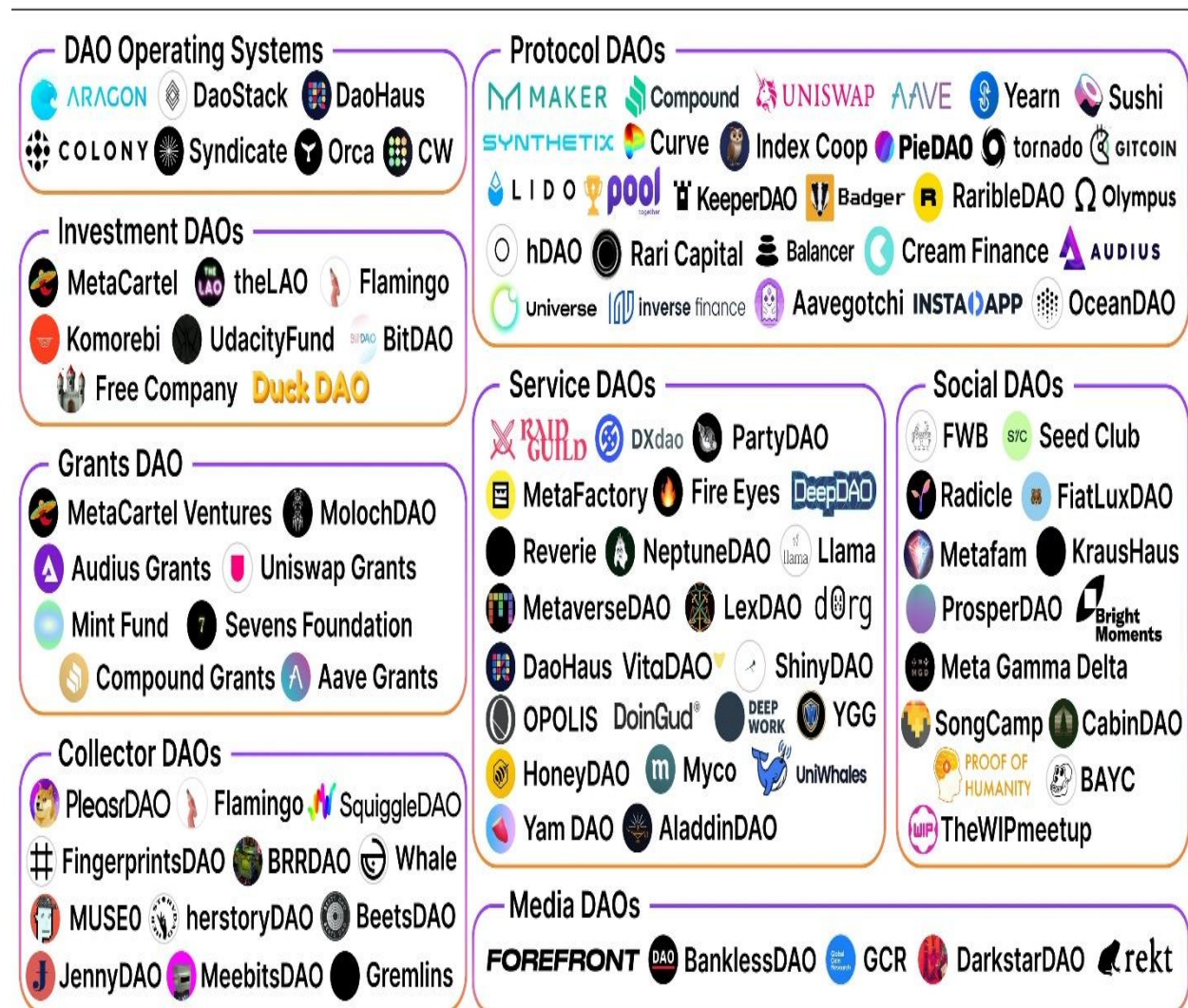
Source: Coopahtroopa

_____

_____

The core argument for DAOs is that they present a better way for human beings to organize. As such, they may soon begin to replace some of our longest standing institutions. Notable types of DAO include:

- **Protocol DAOs**: "For-profit" DAOs that operate a business (could replace traditional corporations)

- **Investment DAO**: DAOs that focus on pooling and investing capital (might disrupt VCs, PE shops and Hedge Funds)

- **Charity DAOs**: Provide grants to charitable organizations and projects (may become an online version of the United Way or Salvation Army)

- **Collector DAOs**: Focus on pooling capital and investing in digital assets such as NFTs (might undermine the current gallery and museum set)

- **Media DAOs**: Creator-owned DAOs that produce entertainment products (could subvert film studios, publishers, news organizations, record labels and game developers)

- **Service DAOs**: Member-owned freelancer networks (have the potential to supersede unions, consulting firms and talent agencies)

- **Social DAOs**: Virtual social clubs (may replace country clubs and member's clubs like Soho House)

Let's take a deeper dive into each of these categories below…

_____

_____

Chapter 57: Protocol DAOs

What is a Protocol DAO?

"Protocol" DAO is a bit of a nebulous term, but it's generally used to refer to a for-profit, operating businesses organized under a DAO structure. In short, it's a decentralized version of a traditional corporation.

While protocol DAOs can theoretically govern any type of business, in practice they are generally used for crypto-focused projects such as decentralized exchanges and borrowing / lending protocols.

They are currently the largest category in the space and represent 6 out of the top 10 DAOs.

How does a Protocol DAO Work?

To understand how a protocol DAO functions, let's take a look at Uniswap DAO – the organization responsible for managing Uniswap, the largest decentralized cryptocurrency exchange.

Decentralized exchanges (or DEXs) are peer-to-peer marketplaces where users can directly trade with one another without the need for banks, brokers or any other financial intermediaries. Unlike centralized exchanges such as Coinbase, they can't restrict users or decide what tokens are traded. In fact, they don't even require KYC, meaning that anyone can use a DEX from anywhere in the world and trade anonymously (provided they have a VPN).

Launched in 2018, Uniswap has become the largest DeX, and is currently generating over $1 billion in volume per day.

Uniswap is the Largest DEX with Over $1 Billion in Volume Per Day

Top 5 DeXes by Daily Volume

$1.2B	$0.2B	$0.2B	$0.1B	$0.1B
Uniswap	Pancake Swap	Dodo	Curve	Balancer

_____

_____
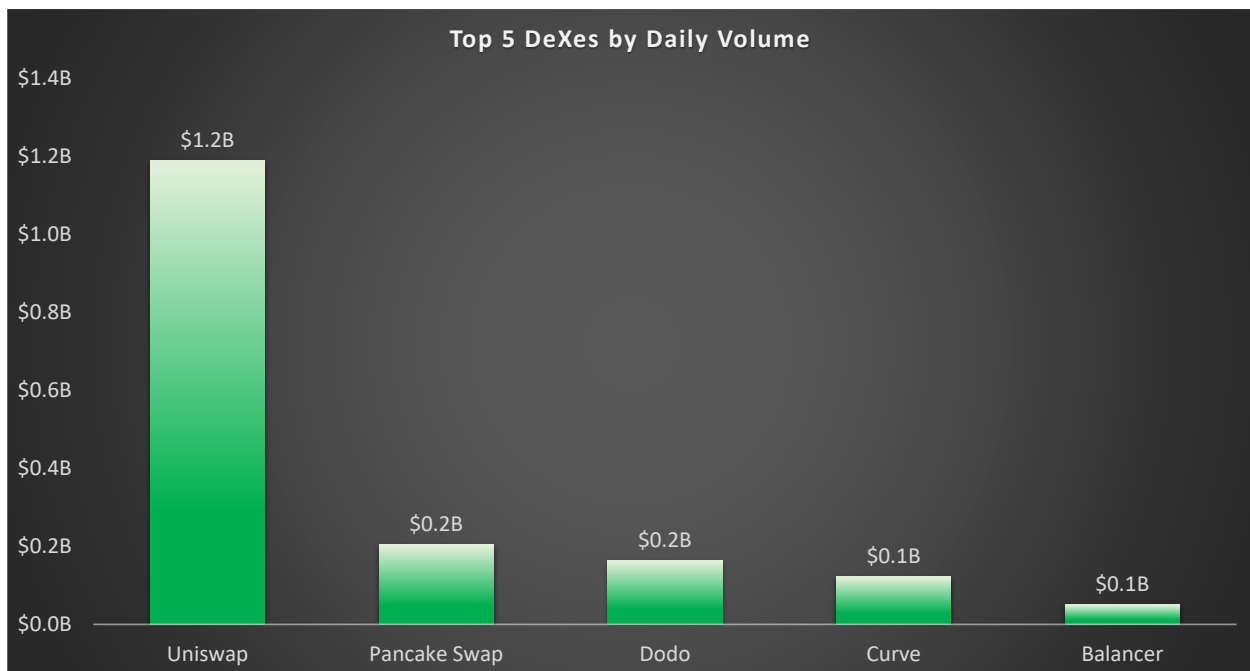
Source: [The Block](#) as of 10.2.22. Results based on September 2022 volume.

The protocol became a DAO in September 2020 when it issued 1 billion UNI tokens to its users, effectively transitioning management from the founders to the community. With the Uni governance token, users have full control over the project and are responsible for all decisions including how much it will charge and how it will spend its treasury.

To wit, any UNI holder can submit a proposal to change the protocol or introduce new features and have it approved by other DAO members. For instance, let's say that a member wanted to increase Uniswap's fee from 0.3% to 1.0%. She would follow a three-step proposal process that includes:

- Temperature Check: In the first phase, known as a "temperature check", members ask a simple question to the community on gov.uniswap.org and submit it to a vote in Snapshot. For example, a member may ask "should we increase our fee from 0.3% to 1.0%". If the proposal gets a majority vote with a 25K threshold, it proceeds to the next stage.

- Consensus Check: The second phase – the "consensus check" – requires members to create a more formalized proposal, incorporating any feedback from the first stage and submit it for a vote. This new proposal requires a minimum of 50K yes votes to proceed.

- Governance Proposal: In the last phase, known as the "governance proposal", members must submit a finalized pitch which includes the actual code. The code must be reviewed by a professional auditor, and members must have a minimum of 2.5 million UNI to submit.

After a proposal reaches the final stage, it is put to a vote. Any proposal that passes is ratified and the code is automatically updated.

Uniswap has been very successful under the DAO structure – it holds nearly $3 billion in assets and is the largest DAO today.

<u>Notable Protocol DAOs</u>

In addition to Uniswap, other notable Protocol DAOs include Gnosis, UXD, Polkadot and MangoDAO.

_____

_____

DAO	Treasury	Token Holders	Description
UNISWAP	$2.7B	323.5K	**Uniswap:** The largest DAO, UniswapDAO represents Uniswap, a decentralized exchange
ENS	$1.1B	58.7K	**Ethereum Name Services:** The DAO of ENS, a protocol that functions as a decentralized DNS, translating Ethereum addresses into a human readable form
Gnosis	$889M	15.5K	**Gnosis DAO:** Entity responsible for governing Gnosis products
LIDO	$274M	18.4K	**Lido:** Lido is a liquid staking solution that allows users to pool and stake Proof-of-Stake cryptocurrencies such as Ethereum
Mango	$218M	31.8K	**MangoDAO:** Mango DAO is the governing body of the Solana-based DEX
Compound	$177M	197.7K	**Compound:** Compound is a decentralized lending and borrowing application

Source: DeepDao as of 10.2.22

Note: The above list is not exhaustive. Although generally ranked by size, some smaller projects may be included for illustrative purposes. In addition, while DAOs often span multiple categories, they were only included once in the vertical that is believed to represent the best fit

_____

_____

Chapter 58: Investment DAOs

What are Investment DAOs?

Investment DAOs are collectives of investors who pool their capital to invest in early-stage crypto projects. Proponents argue they represent the ideal form of capital allocation and, as such, will replace VCs, PE shops and hedge funds.

Typically, membership in an investment-focused DAO involves an upfront buy-in in the form of the DAO's governance token in exchange for access to private spaces – e.g. invite-only Discord chats, Telegram groups or in-person events – where deals can be sourced and checks written.

They offer several benefits over traditional funds including:

- **Better Due Diligence**: Unlike traditional investment funds, who are generally limited to a small team of professionals, Investment DAOs can leverage a wide variety of expertise to gain insight into potential investment decisions. Membership is generally global, and these organizations are often composed of specialists from different disciplines including macroeconomics, business strategy and operations, sales & marketing, development and finance

- **Superior Decision Making**: Given their diverse nature, Investment DAOs can leverage the "wisdom of the crowds", gaining unique perspectives and avoiding potential blind spots. This stands in stark contrast to traditional investment funds, who often are forced to rely on a small group of advisors

- **Increased Deal Flow**: Members are incentivized to find and research deals, recruit talent and find partnerships and opportunities for portfolio companies. This effectively gives an Investment DAO a global sourcing network

- **Less Risk**: Unlike traditional funds which often require long lockups, Investment DAOs are often extremely liquid, allowing any investor to leave at any time with their pro rata share of assets

How do Investment DAOs work?

To understand how investment DAOs work, let's take a look at BitDAO, the largest investment DAO. The project was launched by ByBit, a decentralized exchange operating out of Singapore.

The project looks to further the development of decentralized technologies such as smart contract platforms, Layer 2 solutions, NFTs, DeFi, etc… They can do this by making direct investments, performing token swaps, building products and / or providing grants to research teams.

With $1.3 billion in AUM, BitDAO boasts the second largest treasury of any DAO.

_____

_____

BitDAO holds over $1 Billion in its Treasury

Largest DAOs by AUM
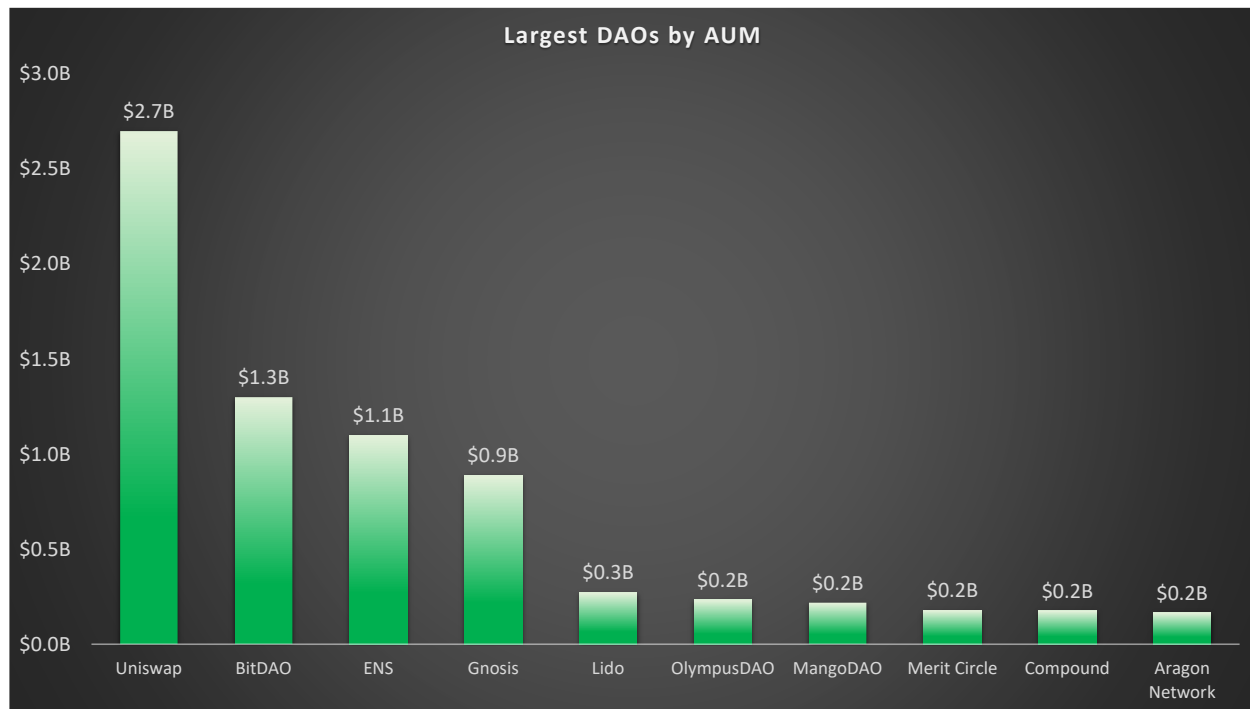
Source: DeepDao as of 10.2.22

BitDAO raised nearly $600M in a series of token sales in the summer of 2021 (one private, one public). The tokens – trading under the symbol BIT – come with both ownership and governance rights, allowing holders to vote on a variety of initiatives including:

- **Investments**: Direct investment in projects
- **Partnerships**: Partner with projects through token swaps and co-development efforts
- **Development**: Build core products that allow decentralized organizations to function more effectively, such as governance and treasury management tools
- **Grants**: Grants to research teams, R&D organizations, educational programs, blockchain technology projects and other public goods
- **Protocol Upgrades**: Changes to the BItDAO core code

This is not an exhaustive list by any means. Like any DAO, members have the ultimate flexibility to evolve with market conditions and find new ways to support the projects vision of an open and decentralized economy.

BitDAO is backed by several notable investors including Peter Thiel, Founders Fund, Pantera Capital, Polygon and ByBit.

_____

Key Players

DAO	Treasury	Token Holders	Description
BitDAO	$1.3B	18.1K	BitDAO: Focuses on investments that further the development of decentralized technologies (i.e. smart contract platforms, Layer 2 solutions, NFTs, DeFi)
Olympus	$234M	8.1K	OlympusDAO: Although Olympus DAO's stated goal is to build an algorithmic stablecoin, the fact that it by backing it with a basket of cryptocurrenices cause many to argue that it is a de facto hedge fund
THE LAO	$8M	144	The LAO: Investment DAO that is registered as an LLC, providing legal protection for its members. Unlike many DAOs, the LAO requires KYC to join
MetaCartel DAO	$6M	183	Metacartel Ventures: Decentralized venture capital fund investing in projects building applications on Ethereum

Source: DeepDao as of 10.2.22

Note: The above list is not exhaustive. Although generally ranked by size, some smaller projects may be included for illustrative purposes. In addition, while DAOs often span multiple categories, they were only included once in the vertical that is believed to represent the best fit

_____

Chapter 59: Charity DAOs

What are Charity DAOs?

One of the earliest use cases of the decentralized autonomous organizational structure, charity DAOs could replace traditional charities such as the United Way or Salvation Army, or traditional grants institutions such as the NIH.

In a charity DAO – also known as a grants DAO – the community pools their capital into a blockchain-based treasury and then collectively votes on how to distribute these funds.

Charity DAOs have almost an unlimited number of potential use cases. They can be used to fund children's and family services, homeless services, education, food banks, social services, youth development, environmental efforts, animal welfare, education, international NGOs, etc…

They offer several benefits over traditional charities such as:

- **Lower cost**: On average, charities spend 25% on administrative and fundraising costs – the automated nature of DAOs can largely eliminate this

- **Governance**: Unlike traditional grant / charity organizations, members have a direct say in the governance of the DAO, meaning that they can direct it to issue funds to projects they are passionate about

- **Transparency**: It is estimated that over $40B of charitable donations are stolen each year. Because every transaction in a grants DAO is recorded on a blockchain, it will be easy to identify theft and fraud

How do they Work?

To understand how grants DAOs work, let's take a look at Gitcoin – a crowd-sourcing platform that provides grants to developers working on open-source software projects. The project was founded in 2017 by Kevin Owocki, has 29K members and nearly $50 million AUM. It is advised by Balaji Srinivasan, Naval Ravikant and Joe Lubin (founder of ConsenSys).

Gitcoin focuses on funding developers working on "public goods" projects. From an economic standpoint, the two features that distinguish a public good is that it's: 1) "non-rivalrous" (i.e. it doesn't decrease in supply if more people use it) and 2) "non-excludible" (i.e. it's available to everyone). Common examples of public goods include clean air, better infrastructure and privacy.

_____

_____

Gitcoin Funds "Non-Excludable" and "Non-Rivalrous" Public Goods
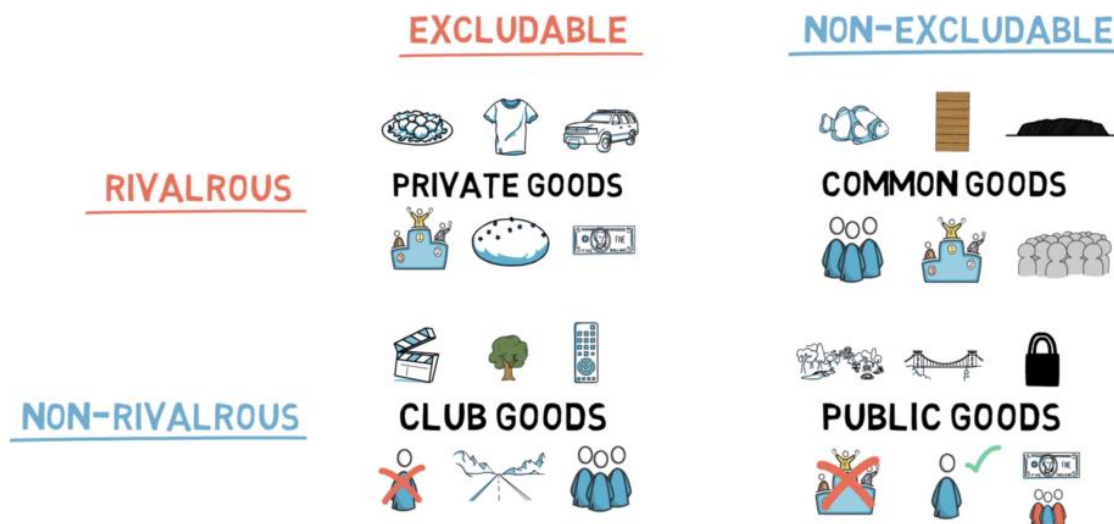
Source: Finematics

Like many charitable organizations, Gitcoin uses "matching" – a process where individual donations are matched from a larger pool of funding supplied by bigger donors.

Unlike traditional charities, which match funding dollar-per-dollar or by a percentage of the total amount given, the platform uses a process called "quadratic funding". Quadratic funding is a mathematically-based scheme that rewards the *number* of contributions over the dollar amount of these contributions (incentivizing people to make many small donations vs. a few large ones). In theory, this creates a more democratic process and gets people more involved in the ecosystem.

Feel free to skip this section if you're not interested in the math behind this, but if you are – quadratic funding works by taking the square root of each contribution to a project, summing and squaring that total and then comparing the result to similar projects.

This probably seems a bit confusing, so let's explain with an example. Imagine that there is a $10,000 matching pool and three projects that each raise $5,000, but from a different number of donors (let's say 5, 2 and 10 donors). In a traditional matching scheme, because each project raised the same amount, they would split the matching pool equally, getting $3.3K (33%) each. Under quadratic funding, however, we would get a different result:

- Project A: If the first project raised $1,000 each from 5 donors, we would take the square root of all the donations ($\sqrt{\$1,000} = \$31.62$), sum them up to get $158.12 and then square this to get $25,000

- Project B: If the second project raised $2,500 each from 2 donors, we would take the square root of all the donations ($\sqrt{\$2,500} = \$50.00$), sum them up to get $100.00 and then square this to get $10,000

_____

_____

- Project C: If the third project raised $500 each from 10 donors, we would take the square root of all the donations ($\sqrt{\$1,000}$ = $22.36), sum them up to get $223.61 and then square this to get $50,000

We would then sum all three totals to get $120,000. While this figure doesn't represent an actual funding amount, it will be used to calculate the percentages of the matching pool given to each project. Based on these numbers, we can see that project A garnered 21% of the new total ($25,000 / $120,000), project B garnered 8% ($10,000 / $120,000) and project C garnered 71% ($85,000 / $120,000).

As such, out of the original matching pool of $10,000, project A would receive $2,083.33, project B $833.33 and project C $7,083.33.

Again, it's not really necessary to understand the math, only that even though each project raised the same amount, the one with the most donations received *a lot* more total funding.

<u>Who are the Key Players?</u>

In addition to Gitcoin, other notable Grants DAOs include Moloch, VitaDAO, Big Green, UkraineDAO and KlimaDAO

DAO	Treasury	Token Holders	Description
	$48M	28.7K	Gitcoin: Provides funding for public goods projects using quadratic funding
	$4M	1.4K	VitaDAO: DAO funding early-stage longevity research and drug development
	$195K	3.7K	UkraineDAO: Supports the defense of the Ukraine in its war against Russia

_____

_____

	NA	118	MolochDAO: Moloch DAO funds public goods projects that help with the growth of the Ethereum ecosystem. The project is particularly notable given that its set of governance smart contracts, known as Moloch, has been used as the framework for many other DAOs
	NA	NA	Big GreenDAO: Provides grants to organizations that are advancing the development of food, gardening and agriculture. Big Green was founded by Elon Musk's brother Kimbal
	NA	NA	KlimaDAO: Focused on purchasing carbon credits in an attempt to drive the price up and force companies to reduce emissions

Source: DeepDao as of 10.2.22

Note: The above list is not exhaustive. Although generally ranked by size, some smaller projects may be included for illustrative purposes. In addition, while DAOs often span multiple categories, they were only included once in the vertical that is believed to represent the best fit

_____

_____

Chapter 60: Collector DAOs

What are Collector DAOs?

Collector DAOs are the close cousin to investor DAOs in that they pool money together to purchase and co-own digital assets such as NFTs.

These DAOs became popular in response to the NFT boom of 2021, which saw average prices increase from $128 to $6,900 (including several high-profile sales such as *Beeple's Everydays* for $69.3 million). As asset prices became out of reach for the average person, collector DAOs offered a logical way to preserve access to the most desirable NFTs.

The NFT Market has grown almost 400x since 2021
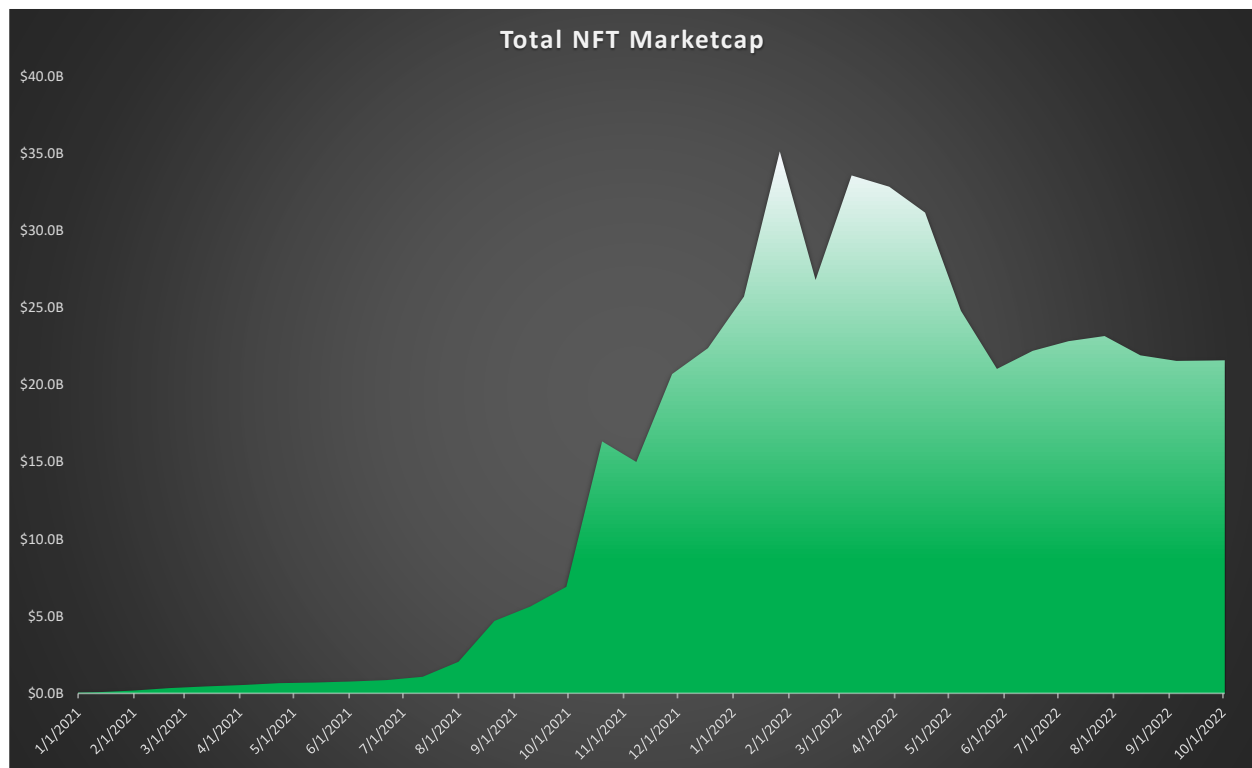
Source: NFTGo as of 10.2.22

Collector DAOs provide members with several unique benefits including:

- **Shared costs**: Sharing the cost of expensive NFTs dramatically lowers the barrier to entry for the average user (as well as the risks)

- **Collective Intelligence**: Like investment DAOs, collector DAOs can leverage a diverse set of viewpoints and experiences to help them make decisions into what projects to invest in

_____

- **Flexibility**: In addition to pooling funds to purchase art, collector DAOs can choose to make angel investments with the goal of growing the entire digital art community

How do Collector DAOs work?

To understand how collector DAOs work, let's take a look at PleasrDAO, an organization that focuses on the collective purchase of expensive NFTs. The project was founded in 2021 and is backed by Andreessen Horowitz.

The DAO pools capital from potential investors, uses this money to purchase an NFT and then returns each investor a token representing their pro-rata share of the NFT.

For example, if Alice contributed $1,000 to the purchase of a $100,000 NFT, she would get 1% of the tokens issued by Pleasr. These tokens can generally be traded on the open market, giving investors liquidity and allowing them to speculate on asset prices.

Shares are created through a process known as "fractionalization" – a method of *economically* splitting up the ownership of an NFT into smaller pieces which can be bought, sold, traded and held by multiple users.

The term "economically" is key here as NFTs can't actually be divided (much like you couldn't cut a physical piece of art into little pieces without destroying its value). Instead, the process of fractionalization involves the issuance of tokens that represent a *claim* on the original asset.

<u>Fractionalization of a CryptoPunk</u>
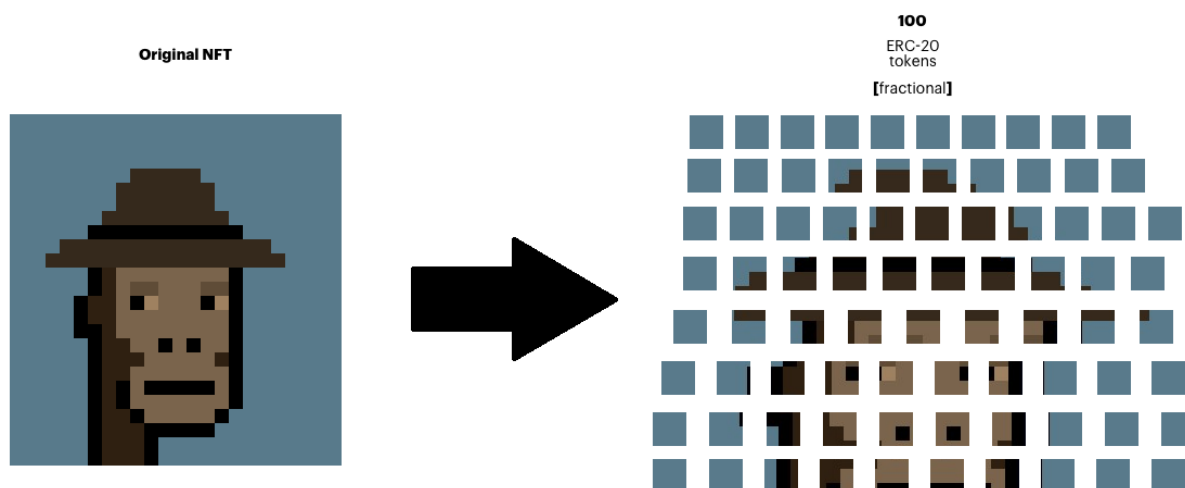
Source: Tessera

PleasrDAO often uses a platform known as Tessera (formerly Fractional) to distribute tokens to the community. To issue a token via Tessera, PleasrDAO would need to:

- Create a Vault: PleasrDAO would deposit their asset as collateral in a "vault" on Tessera and specify the number of tokens they want to create

_____

- Mint Tokens: Once the collateral is deposited, Fractional issues the PleasrDAO 100% of the fractional ownership tokens
- Distribute Tokens: PleasrDAO would distribute each investor their pro-rate share of tokens.

Fractionalization yields several benefits in that it: 1) allows the average user access to extremely expensive works (such as CryptoPunks or Bored Ape Yacht Club), 2) facilitates price discovery and 2) provides liquidity allowing members to sell a portion of their assets (which can't be done with traditional NFTs)

To date, PleasrDAO has purchased several notable works such as the "DOGE" meme NFT for $4million, an NFT from Edward Snowden for $5.5 million and the only copy of an album from the Wu-Tang Clan for $4 million.

Key Players

In addition to PleasrDAO, other notable collector DAOs include FingerprintsDAO, Bright Moments DAO, Flamingo DAO, Squiggle DAO, Constitution DAO and Yield Guild Games.

DAO	Treasury	Token Holders	Description
Merit Circle	$180M	8.3K	Merit Circle: Guild focusing on investing in Play-to-Earn gaming assets and using them within their ecosystem of players
PleasrDAO	$30M	171	PleasrDAO: DAO focused on crowdfunded NFT purchases
Fingerprints DAO	$22M	480	FingerPrintsDAO: Collects notable NFTs such as Autoglyphs, Meebits and CryptoVoxels land
SquiggleDAO	$4M	835	SquiggleDAO: Focuses on acquiring "Squiggles", a generative art NFT found on ArtBlocks

Bright Moments DAO	$483K	1.9K	Bright Moments DAO: Purchases NFTs and intends to display them in a network of real-world art galleries
Flamingo DAO	$23K	NA	Flamingo: Allows for fractionalized NFT purchases, similar to PleasrDAO
ConstitutionDAO	NA	19.9	Constitution DAO: Raised almost $50 million to buy a copy of the US constitution in a public auction and narrowly lost to Ken Griffin, the CEO of Citadel
Yield Guild	NA	NA	Yield Guild Games: Invests in NFTs used in Play-to-Earn games (mostly Axie Infinity), rents them out to members and collectively assists with game play and strategy

Source: DeepDao as of 10.2.22

Note: The above list is not exhaustive. Although generally ranked by size, some smaller projects may be included for illustrative purposes. In addition, while DAOs often span multiple categories, they were only included once in the vertical that is believed to represent the best fit

_____

Chapter 61: Media DAOs

What are Media DAOs?

Media DAOs are decentralized information and entertainment companies that are directly owned by creators and consumers.

Musicians, artists, game developers, independent journalists, podcasters, bloggers, YouTubers and social media influencers could all transition their communities to a DAO structure. By "cutting out the middleman", Media DAOs have the potential to subvert film studios, publishers, news organizations, record labels and game development studios.

Media DAOs offer both creators and consumers substantial benefits, including:

- **Increase Profits:** Intermediaries take a large cut out of an artist's revenue. After accounting for record labels, producers and streaming platforms, artists earn fewer than 12% on platforms such as Spotify. Removing these intermediaries could significantly increase profit (some decentralized music services are offer a 90% share!)

- **Less Censorship:** Companies such as Twitter frequently ban users, and Apple banned Epic Games, the creator of the multi-billion dollar game Fortnite, from its App Store after a revenue dispute. Media DAOs could free creators from this restriction, allowing them to upload any content, no matter how controversial, to any platform they choose

- **Enhanced Fan Involvement**: Finally, Music DAOs will likely increase the incentives for collaboration between creators and their fanbase. For instance, members could gain economic benefit from creating derivative works and remixes, or even building decentralized applications that incorporate a piece of work

The combination of NFTs – which allow personal ownership of intellectual property – and Media DAOs is particularly exciting. One could imagine a world where a group of individual rights holders collectively organize to build the next Marvel.

How do Media DAOs work?

To understand how Media DAOs work, let's take a look at Bankless – a digital media company that focuses on crypto education and infotainment through its flagship podcast and newsletter.

The Bankless organization was originally founded in 2020 by David Hoffman and Ryan Sean Adams. In 2021, they decided to shift the structure to a DAO by creating and distributing over 1 billion BANK tokens (30% to community members retroactively, 30% to the DAO's treasury and 40% for future grants).

The DAO was formed to expand on Bankless's original mission by evolving into a diversified entertainment studio. As such, BanklessDAO and Bankless LLC are technically separate entities, with the original company being just one player in a larger ecosystem (although it does own 25%).

_____

_____

Bankless LLC is Just One Part of a Broader Ecosystem
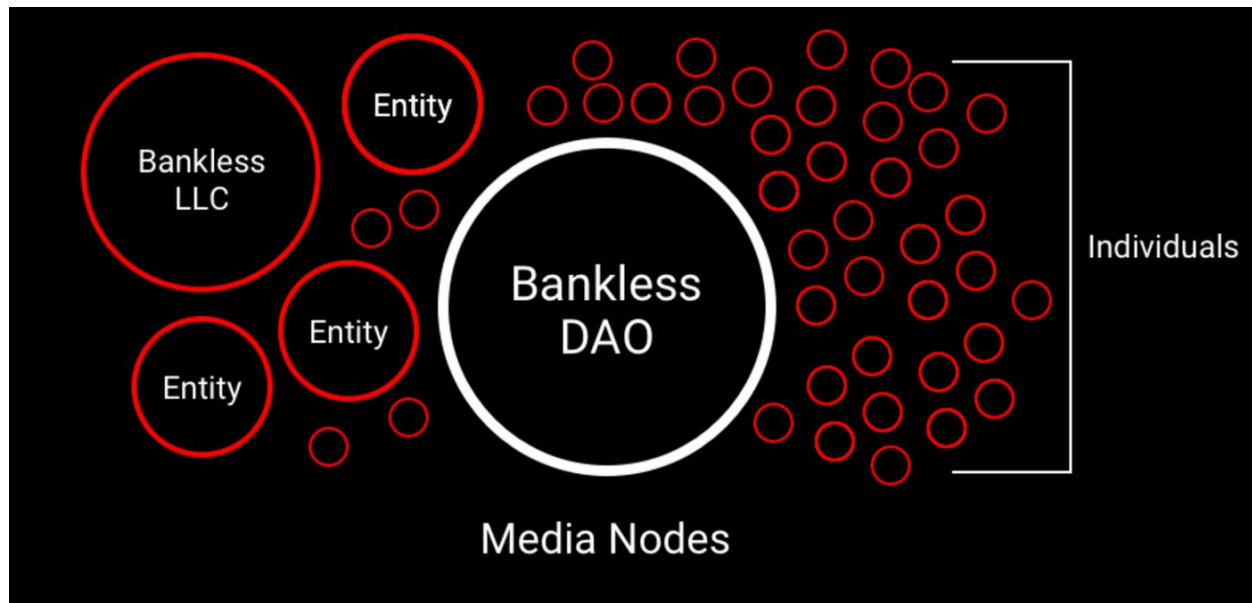
Source: Bankless via Medium

In many ways, the BanklessDAO runs similarly to a traditional media studio. It is organized into departments, called Guilds, that perform the basic functions that you would find in any media organization. Some of the more prominent Guilds include:

- **Content Creation:** Writer's Guild, AudioVisual Guild and Translator's Guild
- **R&D:** Research Guild and Education Guild
- **Sales:** Marketing Guild and "DAOlationships" Guild
- **Operations:** Operations Guild and Analytics Guild
- **Tech:** Developer's Guild and Design Guild
- **Finance:** Treasury Guild
- **Legal:** Legal Guild

Contributors to the DAO are paid in BANK tokens using a blend of bounties and reputation-based compensation methods.

Unlike traditional publishers, BanklessDAO is owned by the community. Anyone can become a member for 35K BANK tokens (~$300 at the time of writing) and make proposals, participate in discussion and vote on key issue.

Currently, there are 7.3K members of the Bankless DAO managing $2 million.

Key Players

In addition to Bankless, other notable media DAOs include Global Coin Research, Mirror and Rekt.

_____

DAO	Treasury	Token Holders	Description
Global Coin Research	$8M	825	GlobalCoin Research: Hybrid media and investment organization that performs deep research on the crypto space and uses the results to create content and make investments
BANKLESS DAO	$2M	7.3K	BanklessDAO: DAO spun out of Bankless LLC, an entertainment company that provides podcasts, videos and newsletters on developments in the crypto space
Mirror	NA	NA	Mirror DAO: DAO for the decentralized blogging platform Mirror
rekt	NA	NA	Rekt: Web3-focused publisher organized into a DAO

Source: DeepDao as of 10.2.22

Note: The above list is not exhaustive. Although generally ranked by size, some smaller projects may be included for illustrative purposes. In addition, while DAOs often span multiple categories, they were only included once in the vertical that is believed to represent the best fit

_____

Chapter 62: Service DAOs

What is a Service DAO?

Service DAOs are modern-day labor aggregators – similar to decentralized unions, consulting firms or talent agencies.

They are generally composed of freelancers from Web3-related fields, such as design, development, marketing, sales, operations and treasury management. Members collectively own the DAO and work is often compensated in stablecoins or the DAO's native token.

Virtual talent platforms are not a new phenomenon. As the number of registered freelancers has ballooned to over 150 million, several companies such as Upwork and Guru have launched.

These companies help freelancers find clients and then take a percentage of the profits. Using a virtual talent platform has several benefits: freelancers don't have to spend time finding clients and employers get faster recruiting times, access to a global network of talent and cheaper labor.

Service DAOs retain all these benefits and add a few more, including:

- **Lower Fees**: Commissions for many freelance matchmaking services can range between 20% to 40% of the work performed. ServiceDAOs can "cut out the middleman", lowering costs for customers and increasing payouts to freelancers

- **Interoperability**: A freelancer's work history, namely his or her reputation or reviews on a specific platform, generally can't be imported to another freelance service. ServiceDAOs have the potential to change this, allowing freelancers to share their reputation broadly

- **Ownership:** Historically freelancers haven't had any ownership stake in virtual talent platforms or the ability to change the parameters of the platform (e.g. fees, review moderation). Service DAOs change that, aligning incentives and increasing engagement

How do Service DAOs work?

To understand how Service DAOs work, let's take a look at RaidGuild – a design, development and marketing agency focused on Web3 projects.

Clients who wish to hire RaidGuild must deposit 500 DAI and will have an initial call with an account manager (known internally as a "Cleric") to discuss the project. If the initial call is successful, the client will submit funds in escrow, the account manager will assemble the appropriate team of subject matter experts and the "raid" will begin.

The team is primarily composed of developers, designers and marketers and has completed several projects to date. The DAO has completed several projects including a metrics dashboard for Aragon, front and backend for Stake On Me, community tracking for 1Up World and strategic consulting to help Senary Blockchain Ventures design a DAO.

_____

_____

<u>RaidGuild Team Members on the Aragon Metrics Dashboard Project</u>
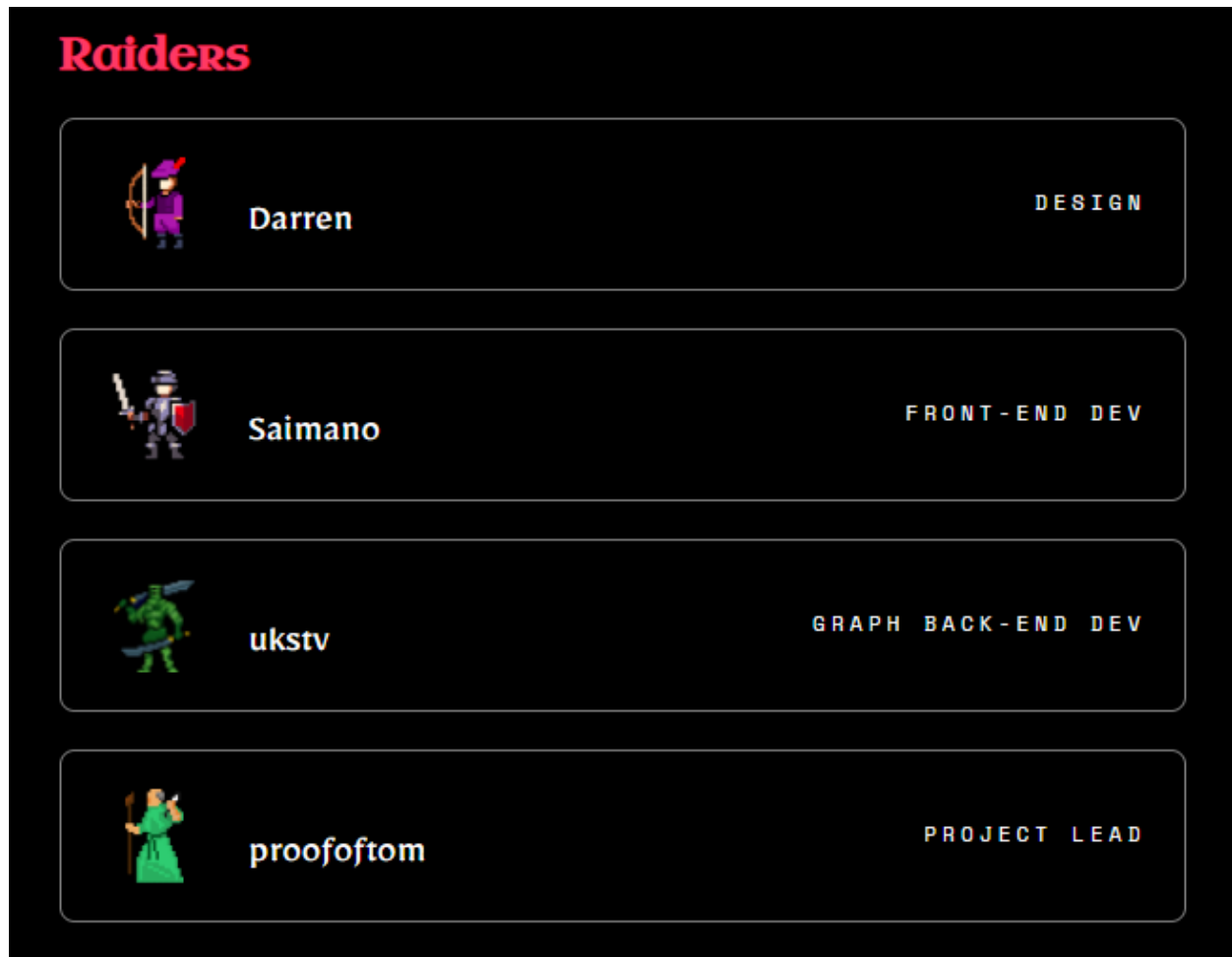
Source: RaidGuild

RaidGuild currently offers clients the following services:

- **Consultations**: Offers strategic consulting services, helping clients validate ideas and implement operational tactics to build, ship and grow their product
- **UX / UI Design**: Designers provide consulting in user experience, feedback and testing
- **Full Stack Development:** Engineers deliver both front and back-end development solutions for dApps.
- **Marketin**g: Members provide consulting in marketing, social media and growth hacking

As it grows, the DAO hopes to expand into related, non-technical fields and add expert writers, sales professionals, business development specialist, community managers, economists, treasury management experts, etc…

_____

Who are the Key Players?

In addition to Raid Guild, other notable Service DAOs include Developer DAO, Braintrust and DxDAO.

DAO	Treasury	Token Holders	Description
DXdao	$58M	536	DXdao: Focused on the development of DeFi protocols
Braintrust	$2M	89	Braintrust: Global talent network with 10% fees and a focus on technical talent
RAID GUILD	NA	NA	RaidGuild: A design, development and marketing agency focused on Web3 projects
Developer DAO	NA	NA	DeveloperDAO: Collective of Web3 developers

Source: DeepDao as of 10.2.22

Note: The above list is not exhaustive. Although generally ranked by size, some smaller projects may be included for illustrative purposes. In addition, while DAOs often span multiple categories, they were only included once in the vertical that is believed to represent the best fit

_____

Chapter 63: Social DAOs

What is a Social DAO?

A social DAO is an online social club, generally organized to bring like-minded people together around a common purpose.

Social clubs are obviously not a new phenomenon. For most of history, we've been joining guilds, salons, country clubs, exclusive houses, etc… as they offer several benefits such as networking, knowledge sharing, status, etc…

Social DAOs take this a step further, offering members several benefits including:

- **Global Exposure**: As remote-first entities, social DAOs can access members from anywhere in the world

- **Investment Opportunities**: Social DAOs often invest in projects that benefit the community or further its mission

- **Governance Rights**: Social token holders have the right to vote on the direction of the organization and how the treasury is managed

- **Discounts**: DAOs often provide members with exclusive access to merchandise, events, NFTs, etc…

- **Financial Reward**: Membership tokens are extremely liquid and easily traded on the open market. In addition, social DAOs can offer members the ability to "stake" their tokens to generate passive income

How do Social DAOs Work?.

To understand how Social DAOs work, let's take a look at Friends with Benefits – an online social club for "creatives" in the Web3 space (e.g. creators, developers and artists). It has over 8,000 members and was founded by Trevor McFedries in 2020.

The DAO's mission is to promote a "web3 world where prosperity is abundant…technology acts as a communal connective tissue… and data and payments are fluid and controlled by the creators".

While there are some real-world events (such as exclusive parties, after-parties and meetups), most of the DAO's communication is conducted online via a Discord server composed of over 2,000 members. The Discord includes channels covering a variety of interests including art, games, music, films, food and technology.

What makes FWB so difficult from traditional social or country clubs is the fact that it also acts as an investment fund. Members have $18M in funds at their disposal to invest in activities that they believe will further the community and creative side of Web3. To date, they have invested in a:

_____

- • Virtual music studio
- • NFT gallery
- • App that allows "token-gating" for real world events
- • Web3-focused blog
- • Real-time community dashboard
- • Series of parties around the world

Membership in the Friends with Benefits DAO is highly exclusive – fewer than 20% of applicants are accepted. To become a member, one must submit a written application, receive approval from the community and purchase 75 tokens (valued at ~$700 today). Fortunately, the DAO offers scholarships for applicants from underrepresented communities.

Key Players

In addition to Friends with Benefits, other notable Social DAOs include CabinDAO, LinksDAO and Krause House

DAO	Description
	Friends with Benefits: Online social club for "creatives" in the Web3 space (e.g. creators, developers and artists)
	CabinDAO: Aims to blend the virtual world with the real one by owning and operating a collection of physical locations. It currently has two properties in Texas ("the container" and "the cabin")
	LinksDAO: Community of golfers pooling funds to purchase a tier-1 golf course (perhaps several courses eventually) to create a global country club
	Krause House: A community of basketball lovers pooling funds to purchase the first fan-owned NBA team

Note: The above list is not exhaustive.

Chapter 64: DAO Tooling

DAO tools are products, platforms and software applications that help communities coordinate operations.

Traditional corporations have long relied on a variety of tools to improve the efficiency of their operations. Popular products in Web 2.0 include SalesForce for sales, HubSpot for marketing, Trello or Asana for product management, GitHub for development, Quickbooks for finance, Gusto for payroll and Slack and Zoom for communication.

DAOs are no different, as they too will require solutions to help them balance efficiency and decentralization as they grow. In fact, they may need even more assistance as they are dealing with challenges that traditional organizations rarely face, including:

- How do you build culture and maintain productivity and enthusiasm in a remote-only workplace?
- How do you distribute ownership of the enterprise without relying on financial markets and investment banks?
- How do you coordinate democratic decision making between hundreds to thousands of stakeholders spread across the globe?
- How do you compensate an inherently unpredictable workforce that can come and go as they please?
- How do you manage a treasury that's potentially worth billions without relying on a bank?

Given these challenges, there is an increasing demand for DAO tooling.

The DAO Tooling Landscape
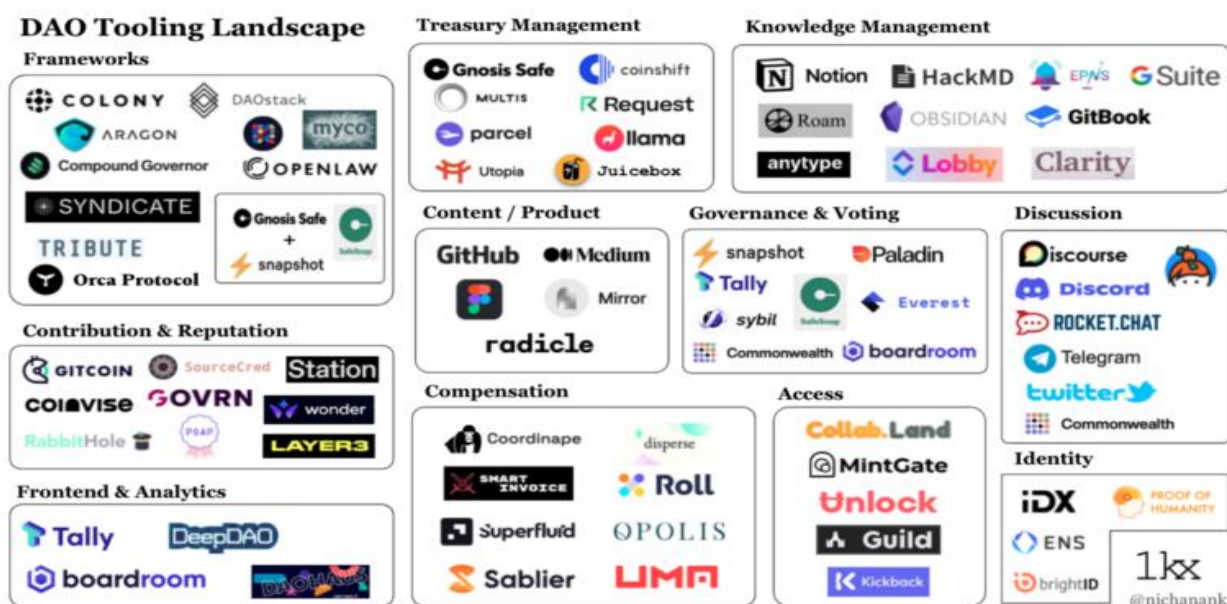
Source: Nichanan Kesopat via Twitter

_____

Despite being a relatively nascent space, the DAO tooling landscape has blossomed – as of late 2022, there are dozens of tooling solutions on the market. While these solutions vary in their utility depending on the size, scope and mission of the organization, most DAOs – at a minimum – would benefit from tooling in five key areas:

1. **Communication**: Tools, such as Discord, that provide a forum for discussing strategy and governance, facilitate remote work and help keep the community active and engaged

2. **Fundraising**: Products, such as Coinvise, that help DAOs launch tokens, coordinate airdrops and customize vesting schedules

3. **Governance**: Solutions, such as Snaphot, that facilitate voting and keep accurate records of the results

4. **Treasury Management**: Tools, such as a Gnosis Multi-Sig, that hold the DAO's funds in a safe manner

5. **Compensation**: Products, such as Coordinape, that help determine fair and equitable contribution for DAO members

In addition, there are several multi-tool frameworks, such as Aragon, that aim to provide most of these solutions in one product.

Let's dive a bit deeper into some of these solutions…

_____

_____

Chapter 65: Communication Tools

What are Communication Tools?

Strong communication is critical to the success of any organization. It is needed to spread the mission, brand and values, ensure employee engagement, solve customer problems, define strategy and coordinate work between multiple departments.

Unfortunately, it's rarer than one would expect, even in the corporate world. Often referred to as "herding cats", successful organizations must harmonize team members with different skills, personalities, strategies and motivations. This exercise becomes even more difficult when dealing with multi-generational and geographically diverse workforces.

According to David Grossman, poor communication cost businesses nearly $40B a year, with an average cost of $62.4 million.

Poor Communication Results in Billions in Losses

Money loss in business industry

$37 billion
The cost of poor communication in companies with 100,000 or more employees.
*Source: Holmes Report 2011

$62.4 million
The average annual cost per company.

$420 thousands
The annual cost in small businesses of 100 employes.

Source: Business2Community

This does not bode well for DAOs who are already at a disadvantage in this area as they have no formal management structure, no physical location and a transient workforce.

In order to get ahead of these challenges, DAOs need to adopt accessible and scalable communication platforms. The best of these will offer:

- Communication Tools: Tools that allow members to share files and communicate remotely via text messaging, voice chat and video chat
- Shared Workspaces: Cloud-based storage solutions that workers can use to save files online and access them from anywhere

_____

- Knowledge Repositories: Shared storage spaces to file key organizational documents including the onboarding procedures, tribal knowledge, key analytics, FAQs and the DAOs mission, vision and values
- Project Management Software: Tools used for project planning, scheduling, resource allocation, metric tracking and product delivery

While not every tool has all these benefits, one that is becoming very popular in the DAO world is Discord – a communication platform that allows members of an organization to communicate over chat, voice and video.

How do Communication Tools Work?

Founded in 2015, Discord is quickly becoming the tool of choice for many DAOs and web3 organizations to facilitate internal discussions, interact with their communities and coordinate operations.

The platform is organized into servers – invite-only spaces for users to chat, hang out, do business and have fun. An organization can create a server for virtually any type of community – from a company to a non-profit to a book club.

The BanklessDAO Discord
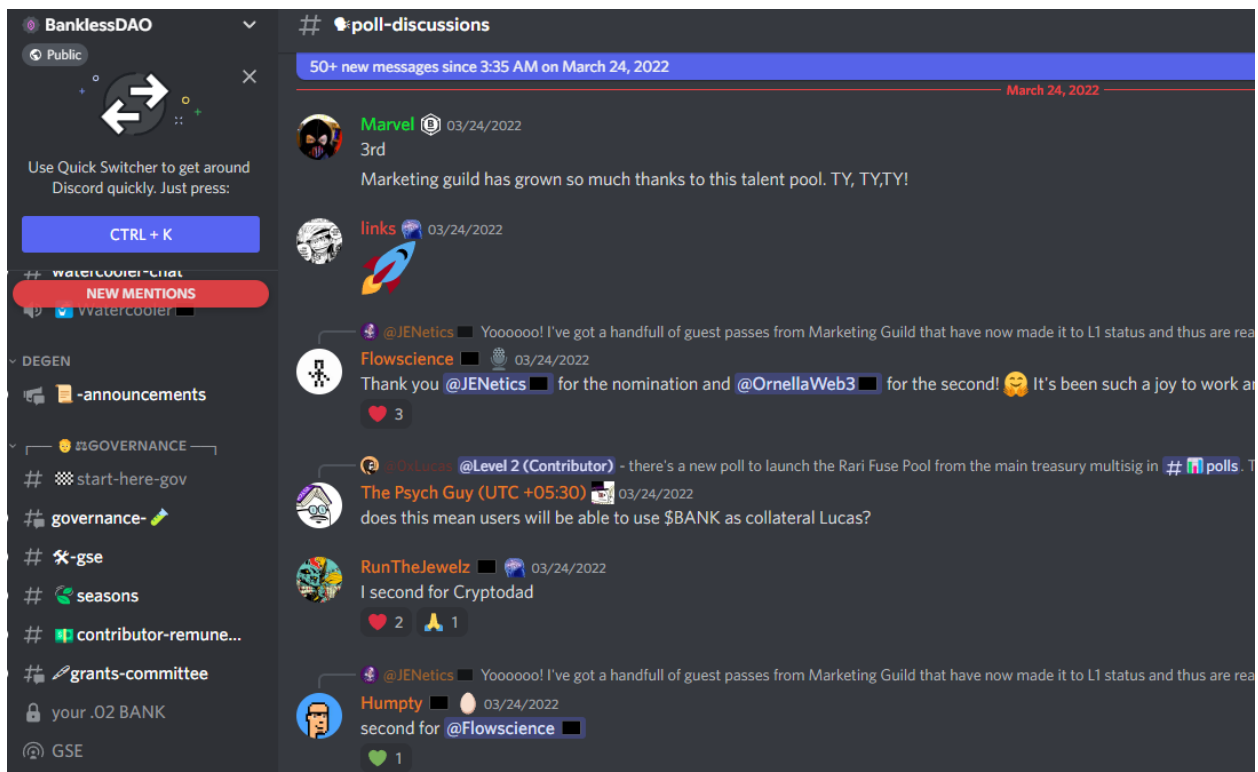
Source: Bankless Discord

Each server is broken up into several channels, each focusing on a functional area of the organization. For example, the BanklessDAO Discord has over 100 channels, including:

_____

- Announcements: Pertinent information related to the DAO
- General: Includes general information about the DAO, FAQ and a book club
- Governance: Forum to discuss ideas and proposals
- Developers Guild: Space for developers to work together and solve problems
- Marketing Guild: Channel for marketers to plan, coordinate and execute strategies
- Treasury Guild: Forum to discuss key issues related to treasury management
- Water Cooler: Open forum to discuss anything, hang out with other DAO members and have fun

There are also dedicated voice channels and a function to allow private messaging.

In theory, Discords are "invite only", but in practice many DAOs make their communities easily accessible by posting an open invite link on their twitter. For example, you can join Bankless DAO's Discord simply by clicking the link provided on their Twitter.

The platform is particularly useful for DAOs when paired with Collab.Land, a tool that provides "token-gating", allowing DAOs to restrict access to token and / or NFT holders.

Discord has 150 million MAUs and generated $130 million of revenue in 2020.

What are Popular Communication Tools?

In addition to Discord and Collab.Land, some of the most popular communication tools include Telegram, GitBook, Notion, GSuite and Asana.

Tool	Description
	Discord: The most popular communication tool for DAOs, a communication platform that allows members of an organization to communicate over chat, voice and video
	Telegram: Highly secure messaging service. While Telegram is very popular in the overall crypto world, it has seen less adoption by DAOs.
	Collab.land: Provides "token-gating" services for Discord and Telegram. Using a bot, Collab.land can check to see if a user has the required cryptocurrencies or NFTs to join a community

_____

_____

GitBook	Gitbook: Online documentation software that allows DAOs to store internal knowledge
Notion	Notion: A project management and note-taking software arranged in a "wiki" format. Several DAOs use it as a knowledge repository
G Suite	Gsuite: Google's cloud-based document sharing service. While GSuite is very popular among Web 2.0 startups as a shared working space, it is less popular in the DAO crowd due to its centralized nature
asana	Asana: Project management tool popular with Web 2.0 startups (especially development teams), Asana is designed to help teams organize, track and manage their work

_____

_____

Chapter 66: Fundraising Tools

What are Fundraising Tools?

Unlike traditional corporations, who generally raise capital through private placements or IPOs, DAOs don't use investment banks or the financial markets to raise funds and distribute ownership.

Instead, they must create and issue their own cryptocurrencies (or NFTs) by creating a smart contract on a blockchain such as Ethereum.

In addition to physically creating a token, DAO founders must also determine its "tokenomics" – a portmanteau of "token" and "economics" which refers to the incentives and economic characteristics of a cryptocurrency (i.e. the things that make it valuable to investors and community members).

When launching a token, founders must consider the following:

- **Supply**: How many tokens will initially be issued? How many will ever exist? What's the schedule for releasing them?

- **Monetary Policy**: Is the token inflationary or deflationary? Is there a mechanism to burn (destroy) tokens?

- **Allocation**: How much of the token will be distributed to founders and investors, and how much will be available to the community? Will there be a vesting or lockup schedule?

- **Distribution**: How will the token be distributed – ICO, IDO, airdrop? How will the founders prevent a "gas war" and ensure a fair and equitable distribution?

- **Utility**: How can users generate passive income from the tokens? Can they stake, mine or yield-farm them?

Like any disruptive technology, the field of tokenomics is constantly evolving. Communities are demanding more sophisticated monetary policy, fairer allocation, more efficient distribution and more utility.

For instance, from 2013 to 2017, the primary mechanism for token distribution was the Initial Coin Offering (ICO) – a method where startups would sell tokens directly to the public, often from their website. As the ICO began to run into legal and regulatory troubles, a new model, known as the Initial Exchange Offering (IEO), became popular. IEOs involve launching the token on a centralized exchange, such as Coinbase or Binance. This soon became prohibitively expensive for many (there were rumors of exchanges charging a minimum of $5 million to list), and we saw this morph into the IDO (similar idea, but for decentralized exchanges). Fast forward to 2021, and we see a variety of distribution methods such as airdrops, parachain crowdloans and seed investments. Some projects have even avoided traditional tokens altogether and opted to launch NFTs with governance rights instead.

_____

_____

The Rapid Evolution of Token Distribution Methods Since 2017
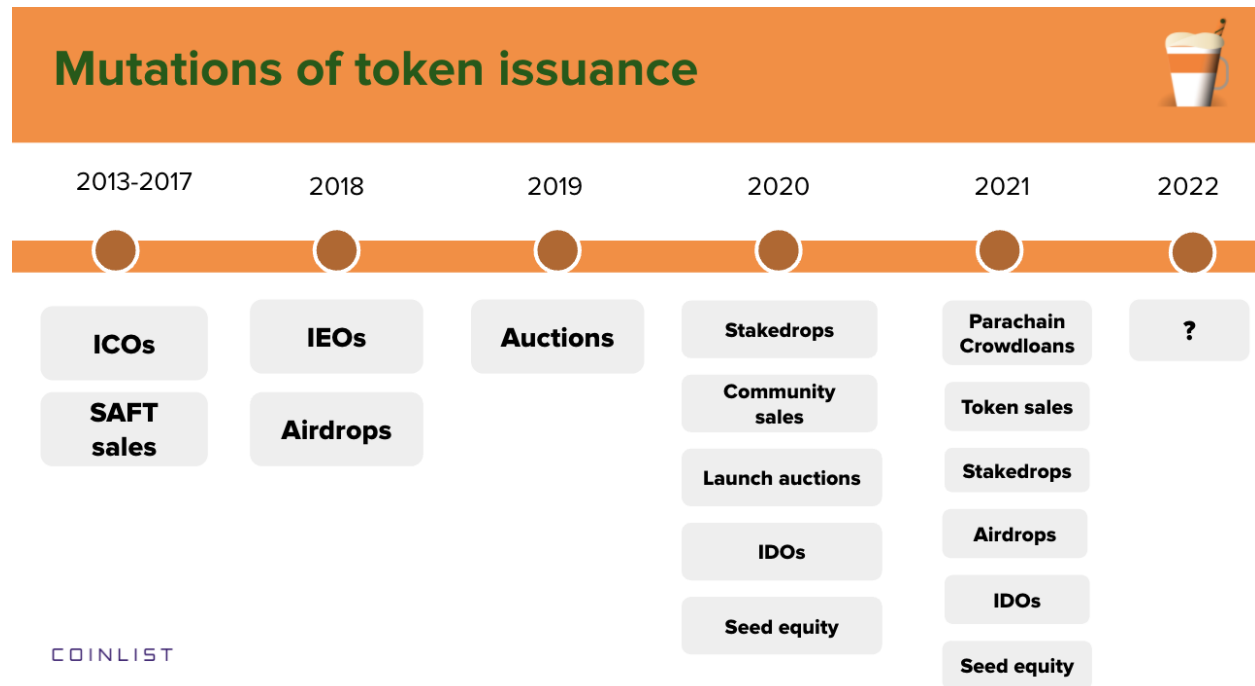
Source: Coinlist

The full scope of tokenomics is well out of the purview of this article, but the important takeaway is that it's a rapidly evolving field, and successful founders must do all they can to stay ahead of the market and maximize value for their communities.

While this may seem daunting, there are fortunately several tools, such as Coinvise, available to help.

How do Fundraising Tools Work?

To understand how fundraising tools work, let's take a look at Coinvise – a platform that makes it extremely easy for users to launch their own cryptocurrency token.

To mint a token, users need to navigate to coinvise.co, connect their wallet and enter the proposed name, symbol, supply and description of the token. Once that information is provided, users simply click "Create", approve the transaction, and receive the funds in their wallet!

The entire process takes about 30 seconds, requires zero technical knowledge and is effectively free (other than gas costs, the platform does not charge a fee or take a percentage).

_____

_____

<u>Coinvise Allows Anyone to Create a Cryptocurrency in Under 30 Seconds</u>

Name

Forefront

This Can Be A Discord Server, Project Or Your Own Name.

Symbol

FF

Your Token Symbol (1-7 Characters), No '$' Sign Required.

Supply

0   Million ⌄

Recommended Supply – 10 Million Tokens.

Treasury

0x7Be8076f4EA4A4AD08075C2508e481d6C946D12b

(Optional) Create Tokens Directly To Your Multisig, Create One Here.

Description

Rewarding the community for creating content on forefront.news

Give Us A Brief Description On How You Would Use The Token.

I understand that these values can't be changed after
deployment and I hereby accept the Token Agreement   ☐

Create

Source: <u>Coinvise</u>

Coinvise currently supports tokens on the Ethereum and Polygon blockchains, and also comes with a variety of additional features to help manage the token's ecosystem including:

- **Token Metrics**: Coinvise provides an informational dashboard that lets DAOs view key token metrics such as the price, market cap, fully diluted market cap and trading volume and also see a list of the top stakeholders by percentage held

- **Airdrops**: DAOs can send tokens directly to thousands of users at once via a unique link, QR code, email list or list of wallet addresses. This has a variety of benefits and is often used to either reward supporters (such as ENS's airdrop of over $500M of tokens to NFT holders) or serve as a fundraising tool (e.g. LooksRare airdropped 120 million tokens to

_____

anyone with a history of using OpenSea, instantly creating a market value of over $300 million)

- **Vesting Schedules**: Coinvise allows the creation of vesting schedules which "lock" tokens up for a specified period of time, making them unable to trade. This is a helpful practice that is common in the corporate world as it allows organizations to retain employees, prevent early investors from selling and show that founders are in it for the long haul

- **Rewards**: DAOs can create rewards (also known as "quests" or "bounties") to compensate users for performing specific actions, such as creating a website, launching a marketing campaign or fixing a bug. Reward programs are helpful in that they incentive community members, benefit early adopters and attract new members

Coinvise is quickly becoming a popular tool in the Web3 landscape and has attracted over 15,000 members and 500+ creators.

What are Popular Fundraising Tools?

In addition to Coinvise, some of the most popular fundraising tools include Mirror, Juicebox and Fairmint.

Tool	Description
	Coinvise: Tool that allows users to create and issue a cryptocurrency in under 30 seconds
	Mirror: Online publishing platform that also allows users to create and distribute tokens and NFTs
	Juicebox: A decentralized crowdsourcing platform that allows DAOs to raise funds from the community for Ethereum-based projects
	Fairmint: Fundraising platform that uses Y Combinator's SAFE format

_____

Chapter 67: Governance Tools

What is DAO Governance?

Corporate governance refers to the system of rules, processes and practices by which companies are controlled – in short, it's how decisions get made.

Traditional corporations rely on hierarchical governance structures. Key decisions are made by the Board, CEO and Executive Team, passed down to middle managers who then relay orders to the rank-and-file workers.

DAOs, on the other hand, adopt non-hierarchical, democratic governance structures, meaning that every member has a say in decision making. In practice, this is often decided by token ownership (i.e. "one token = one vote").

While there are thousands of options for governance protocols, one of the simplest is a propose-discuss-vote-execute architecture:

1. **Propose**: Anyone who owns tokens can make a proposal such as "we should lower our fee from X to Y"
2. **Discuss**: Proposals are often discussed thoroughly amongst the team and amended based on feedback. To avoid unnecessary noise, many DAOs require proposals to pass several internal checkpoints before being finalized
3. **Vote**: Once a proposal is ratified, it is sent to the community to vote on. Communities can decide whether votes need a majority, supermajority, etc… to pass
4. **Execute**: If the vote passes, the decision is encoded in the smart contract to execute

A Simple Approach to DAO Governance
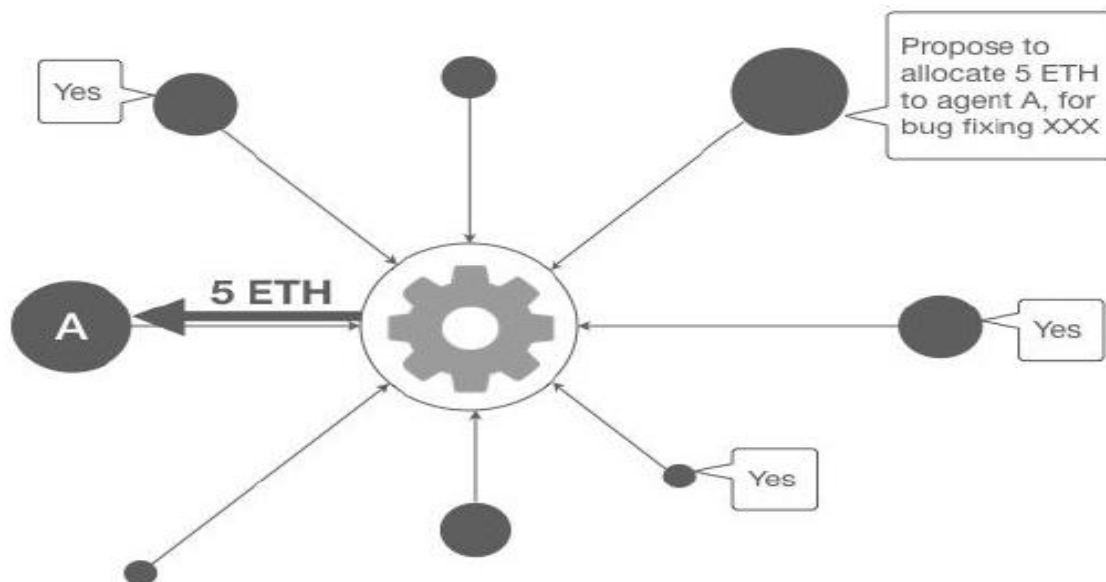
Source: DAOstack whitepaper

_____

While the above graphic represents a good mental model for DAO voting, in practice, the process is often much more complicated as there are as many structures for governance as there are DAO types. For example, DAOs can choose several different voting mechanisms such as:

- **Weighting**: Should voting be based strictly on the number of tokens held (risking plutocracy and bribery) or should additional factors – such as a member's time in the DAO, reputation or past performance – be taken into account?

- **Delegation**: Can users delegate their votes to other members?

- **Type**: Should voting be based on a simple "one token – one vote" model, or should the DAO employ a more exotic mechanism as Quadratic Voting (where members can allocate all of their votes to one or several choices, but each additional vote will count less)

- **Dispute Resolution:** In the event of a dispute, should the organization allow members to quit at anytime and leave with their proportional share of the assets (a process known as "rage-quitting")?

In addition to the voting method, DAOs must decide how they will mechanically record and execute the results. There are currently two main ways of doing this, known as "on-chain" voting and "off-chain" voting:

- **On-Chain Voting**: Votes are recorded directly on the blockchain

- **Off-Chain Voting**: Votes are submitted to a third-party, who calculates the results and then executes the transaction on the blockchain

Both methods have pros and cons. On-chain voting is much safer and more secure, but often comes with a high cost because every transaction on a blockchain requires a fee (and the average fee across all transactions on the Ethereum network is ~$10.00). This risks lowering participation, especially among smaller token holders.

While off-chain voting solves this problem, it is much less secure as it relies on a third-party, which cuts against the Web3 ethos and ultimate goal of decentralization.

As you can see, DAO voting is a complex challenge, forcing members to weight the pros and cons of several options. Fortunately, there are several tools that exist to address these challenges and help organize and motivate participants.

<u>How does DAO Governance Work?</u>

To understand DAO governance better, let's take a look at one of the most popular tools – Snapshot, a tool for off-chain, "fee-free" voting.

To use this platform, a DAO can link their ENS domain to Snapshot to create a "space" – a place where they can host all of their outstanding proposals. Members can then navigate to this space to find the proposal they want to vote on, connect their wallet and cast their vote.

_____

Instead of recording the results directly on the blockchain, Snapshot aggregates these votes and stores them in a decentralized database hosted by IFPS.

Not only does this eliminate fees, but the use of decentralized storage also addresses some of the biggest concerns of off-chain voting. While not perfect, it's relatively transparent (as anyone can easily access the database and verify the results) and secure (as decentralized databases can't be manipulated).

<u>Snapshot Spaces</u>
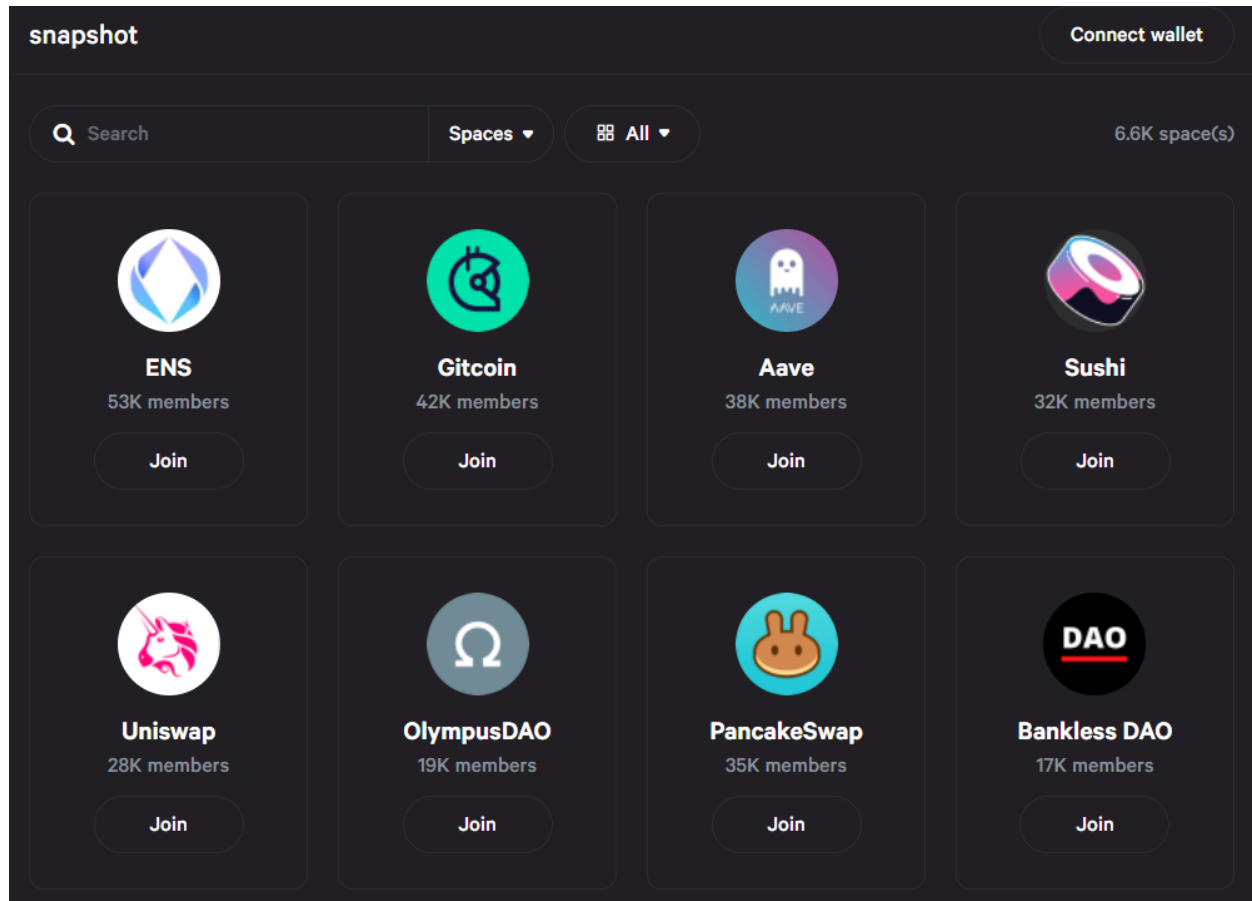
Source: Snapshot.org

Snapshot offers significant flexibility to users – it allows them to delegate votes, choose different weighting metrics (e.g. token-weighted vs. reputation-weighted) and supports several different types of voting methods including:

- **Single Choice**: Each voter can select one option
- **Approval Voting**: Each member can select (or "approve") as many choices as they like, and the choice with the most approvals wins
- **Quadratic Voting**: Members can allocate all of their votes to one or several choices, but each vote will "cost" more tokens (e.g. 1 vote will cost 1 token, 2 will cost 4, 3 will cost 9, etc…)

_____
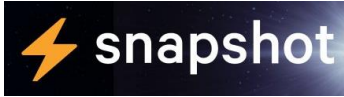
- **Ranked Choice Voting**: Members can rank their choices. If one choice gets a majority of the of the #1 rankings, it wins. If not, the lowest choice is eliminated and the process is repeated again

The biggest problem with Snapshot – and "off-chain" voting in general – is that you still need a trusted third-party to carry out the decision and record it on the blockchain. As such, Snapshot is working on a solution known as "optimistic voting" which will use Layer 2 solutions known as optimistic rollups to count the votes off-chain and then automatically execute them on on-chain without any human intervention.

<u>What are Popular DAO Governance Tools?</u>

In addition to Snapshot, some of the most popular governance tools include Tally, Boardroom, Discourse and OpenLaw. Discord is also frequently used in governance.

Tool	Description
	Snapshot: One of the most popular governance tools, Snapshot allows for off-chain, "fee-free" voting
	Tally: Tool that allows for "on-chain" voting (vs. Snapshot which is "off-chain")
	Boardroom: Full governance platform that provides a variety of tools to manage governance including voting tools (integrates with Snapshot), discussions forums, member profiles and more
	Discourse: Online forum that many DAOs use to discuss governance issues
	Discord: While its primary use is as a communication tool, many DAOs do informal voting through Discord
	OpenLaw: Platform that allows users to create legal agreements that are compatible with Ethereum smart contracts

Chapter 68: Treasury Management Tools

What are Treasury Management Tools?

Unlike traditional corporations – which hold their assets in banks – DAOs store and manage their own funds on a blockchain and access them through a crypto wallet that is known as a "treasury". In essence, is the DAO's "bank".

Treasuries are built through initial token sales, follow-on investments, donations and profits generated by the organization. Many DAOs today have massive treasuries.

The Treasuries of the Top 5 DAOs Hold Over $5 Billion

Source: DeepDAO as of 10.2.22

Treasuries are managed democratically by the members of the community and used to fund operational costs, pay salaries, make investments, etc...

As one can imagine, this is a daunting task, as DAOs face the same challenges as any Fortune 500 company: how to preserve capital, ensure that cash inflows are greater than outflows and minimize risk. In particular, a DAO must decide:

- Cash Flow Management: How much do we pay in salaries? How do we fund operational costs?

_____

_____

- Fundraising: Should we raise more capital? Do we issue tokens to raise capital or borrow?
- Capital Allocation: Should we perform token buybacks? Should we make investments or acquisitions?
- Risk Management: Should we diversify into stablecoins? What assets should we hold?
- Financial Controls: How do we ensure that no one person can steal the funds?
- Reporting: How do we report what's happening in the treasury?

Fortunately, there are several tools available to help members store and manage their funds.

How do Treasury Management Tools Work?

One of the most popular – albeit relatively basic – tools for treasury management is Gnosis Safe, a multi-signature crypto wallet ("multi-sig") developed by the company Gnosis in 2016.

Crypto wallets are software programs that allow users to access their cryptocurrencies and initiate transactions. Unlike physical wallets or bank vaults which hold actual cash, crypto wallets don't technically store cryptocurrencies. Instead, funds are stored on the blockchain and accessed via private keys (which are held in the wallet).

The main benefit to using a crypto wallet is that it gives DAOs full custody over their funds. Unlike a bank account, no external party can restrict access, block transactions or siphon funds. In addition, owners aren't subject to "banking hours", meaning they can access their capital 24 hours a day, 7 days a week (and from anywhere in the world).

As the name suggests, multi-sigs are a special type of wallet that requires two or more private keys to authorize a transaction. While Gnosis offers a variety of options for structuring these wallets, a common setup has 3 owners needing 2 keys to initiate a transaction.

A Gnosis Safe Requires 2 or More Users to Authorize a Transaction

Instruction transaction

Confirm

| 1 | 2 out of 3 confirmations by wallet's owner needed for a transaction. | 2 | Transaction is pending as the other owner needs to confirm. | 3 | Approved transaction will be executed. |
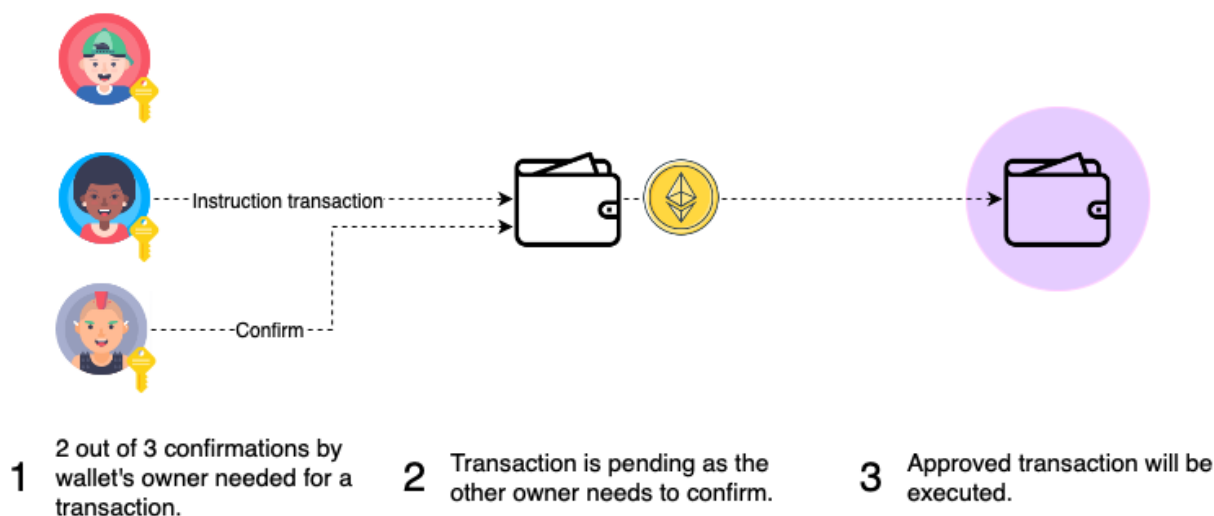
Source: Gauntlet Networks via Medium

_____

Using a multi-sig wallet provides a host of benefits to a DAO:

- **Trust**: As most multi-sigs require a majority of owners to approve a transaction, it reduces the risk that one party will steal the funds

- **Security**: Multi-sigs reduce the risk of cyberattacks by requiring hackers to breach multiple devices

- **Redundancy**: If one owner loses their key, the remaining two can still recover the wallet

In addition to serving as a multi-sig wallet, Gnosis Safe provides users a variety of additional features, such as an enhanced user interface, transaction tracking and the ability to access dApps directly from the wallet.

Gnosis Safe is one of the most popular treasury management solutions – as of December 2021, a total of $86 billion in funds were held in their products. Several, high profile companies including Consensys, ENS, Balancer, Aave and Sushiswap trust Gnosis Safe.

<u>What are Popular Treasury Management Tools?</u>

In addition to Gnosis, some of the most popular Treasury Management tools include Parcel, Superfluid, Sablier and Llama. Juicebox also offers a treasury management solution.

Tool	Description
	Gnosis: The creator of Gnosis Safe, the most popular multi-sig wallet
	Parcel: Tool that allows users to connect a multi-sig wallet and make mass payouts to addresses uploaded in a CSV format. The platform supports automated and recurring payments
	Superfluid: Allows for "streaming payments" – a novel form of payment that sends a constant stream of payments (i.e. every second) to a chosen address. This is impossible with traditional fiat currency and has several potential use cases such as compensation, rent payments, licensing agreements, etc…
	Sablier: Like Superfluid, Sablier is a financial streaming platform. Created in 2019, Sablier supports any ERC-20 token and doesn't charge a fee to use the contract

_____

	Juicebox: In addition to being used as a crowdfunding platform, Juicebox also offers a suite of tools that DAOs can use to manage their treasury on-chain
	Llama: Provides treasury management as-a-service. DAOs can hire Llama to consult on treasury strategy, analytics, financial reporting and treasury workflows

_____

Chapter 69: Compensation Tools

What are Compensation Tools?

Like any organization, DAOs need labor to be successful. Depending on their mission, they may require developers, designers, marketers, operators, finance professionals and / or community managers.

Working for a DAO can be extremely compelling – not only does it provide the opportunity for contributors to "own a piece of the action" and make a meaningful contribution to the development of Web3, it also offers a **level of flexibility that has been historically impossible**. In particular, "employment" at a DAO offers the following benefits:

- **No Geographic Barriers:** As purely online entities, DAOs have no offices or in-person requirements. This means that anyone can choose to work for any DAO no matter where it is located. This not only benefits workers, but also provides a benefit to DAOs who can access talent from anywhere in the world

- **Open:** Most DAOs don't have a hiring process, so anyone can contribute (you just have to show up and start working!). In addition, it's possible to work for a DAO using an anonymous identity, greatly benefiting workers from marginalized groups who have historically faced discrimination (given the proven benefits of workplace diversity, this is a great benefit for DAOs as well!)

- **Flexible**: DAOs don't have employment contracts – contributors can choose to work as much or as little as they like and are also free to move fluidly between DAOs or work for multiple organizations at once. This not only benefits workers but also benefits the DAO as the workforce (and therefore compensation requirements) will naturally expand and contract based on market conditions and the amount of work that needs to be done.

In fact, one could argue that DAOs are the logical extension of the trend towards freelancing and resulting "gig" economy.

_____

Over 1/3rd of US Workforce Performs Freelance Work

Number of freelance workers in the United States from 2014 to 2020 (in millions)

Number of people doing freelance work in millions

Year	Value
2014	53
2015	53.7
2016	55
2017	57.3
2018	56.7
2019	57
2020	59

Sources
Upwork; Edelman; Bureau of Labor Statistics
© Statista 2022

Additional Information:
United States; Upwork; Edelman; 2014 to 2020
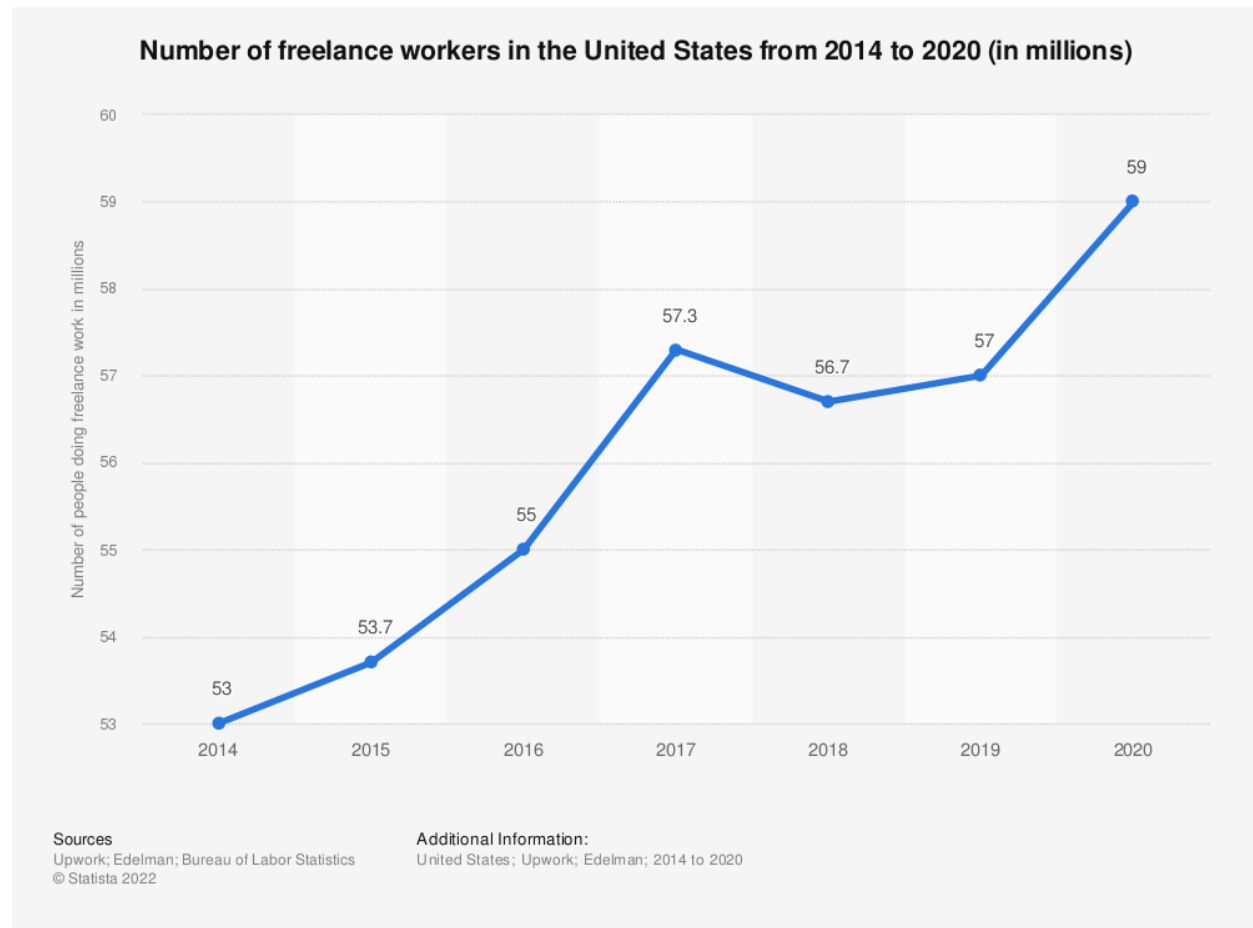
Source: Statista

Unfortunately, this style of employment creates many challenges from a compensation perspective. After all, how do you design a compensation program for members who work erratically? Perhaps more importantly, how do you determine compensation without management? Without HR? Without contracts or negotiations?

To be fair, DAOs are still figuring this out. To date, there are a variety of popular compensation methods including:

1. **Salaries**: In contrast to what was previously discussed, some DAOs – especially well-funded protocol DAOs – still hire full-time workers and follow the standard model that's prevalent in traditional organizations (e.g. base, bonus, equity). Compensation is generally voted on by the DAO and these workers are often subject to employment contracts.

2. **Equity**: Given that DAOs are member-owned, it's possible to not offer any compensation and just hope that contributors are purely incentivized by their ownership stake. While great in theory, this may prove difficult in practice due to the "free-rider problem" (i.e. the tendency for people to let others do the work while still reaping the benefits)

_____

3. **Bounties**: Many organizations are utilizing "bounties", compensation schemes which pay for the completion of a specific deliverable. Under this method DAOs can choose a task – such as creating a new website – specify the price and allow members of the community to nominate themselves. Some DAOs don't even have a nomination process, and simply pay the first person who completes the work.

4. **Point-based Compensation**: Some DAOs are compensating team members with a point-based system. For instance, a DAO could create a formula where attending meetings is worth a certain number of points, completing a task a different number, etc… At the end of each period, the DAO would add the totals and tie this to pay.

5. **Reputation-based Compensation**: Reputation-based schemes put compensation in the hands of the community. Each team within the DAO is allocated a compensation budget and then members of the team vote on whom should achieve what. This can be done subjectively (i.e. by simple votes) or objectively (in combination with contribution-based schemes)

6. **Hybrid**:   Many DAOs are moving towards a "blended" model, which combines a limited number of full-time, contractual employees with a flexible contributor base.

As you can see, DAO founders face a variety of challenges in determining and executing compensation. Fortunately, there are several tools available, such as Coordinape, to assist.

<u>How do Compensation Tools Work?</u>

Coordinape is a reputation-based compensation tool created by Andre Cronje in 2021 to use in his own organization, Yearn Finance. The goal of the tool is to transfer the authority to determine compensation to the membership, allowing contributors to determine fair compensation for their peers.

The platform is built around "circles", groups of members who work together on a regular basis (i.e. teams).

To use Coordinape, DAO contributors connect their wallet to the platform where they can access their circle and see all of their team members.

Each member of the circle is given a certain number of points (called "GIVE") that they can then allocate to their co-workers as they see fit. They can choose to give all of the points to one co-worker, split them up equally or distribute based on some other method that they choose. Members don't even have to allocate all of their points (although the unallocated ones will be destroyed).

_____

GIVE Points Allocation for Yearn Finance
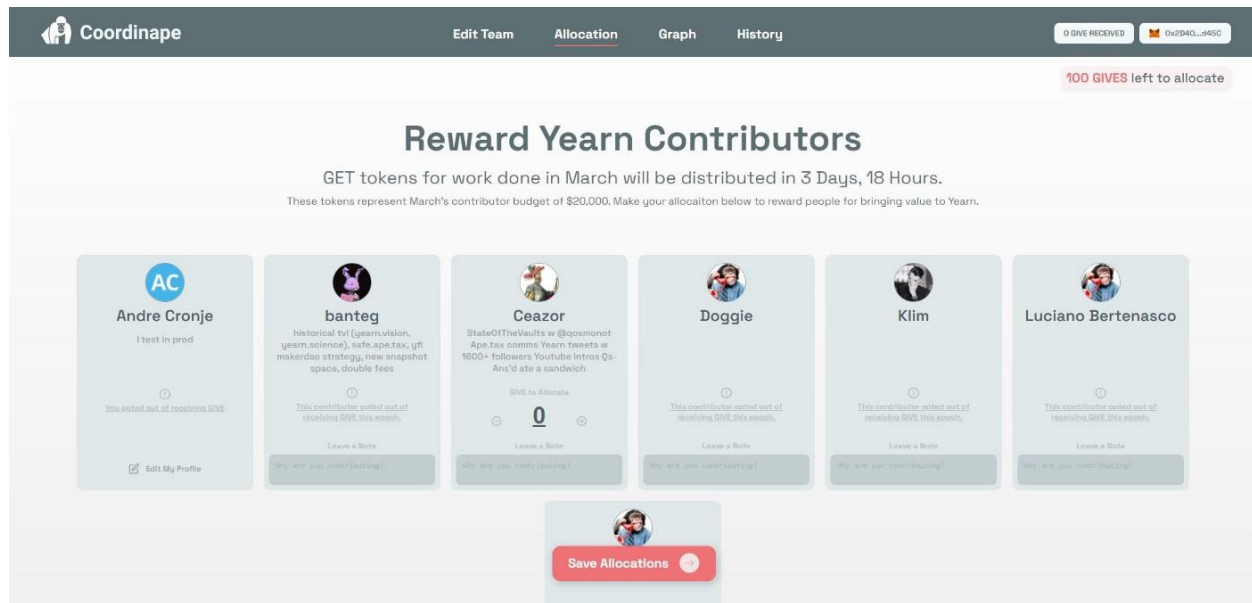
Source: Andre Cronje via Medium

After allocation, each person's GIVE points are transformed into GET tokens, which are used to claim a proportion of the group's allotted compensation budget.

For example:

- The DAO sets the monthly budget for the marketing team at $100,000 USD (in the form of USDC)
- There are 10 members of the marketing circle, and each receives 100 GIVE tokens to allocate (1,000 in total)
- Alice has had a great month, so she receives 250 GIVE tokens from her peers (25% of the total)
- At the end of the period, everyone's GIVE tokens convert to GET tokens, which can be redeemed for USDC
- Because Alice received 25% of the total allocation of tokens, she will exchange her GET for $25,000

Point allocations and the resulting compensation are transparent, meaning that every member of the DAO can see who is getting points, who is giving them and how much everyone is getting paid.

This process occurs once every "epoch" – a time period that can vary from DAO to DAO but is often a month.

Coordinape is establishing itself as one of the premiere reward-based compensation tools, and is used by Yearn, MetaCartel, BanklessDAO, Sushiswap, Gitcoin and DAOhaus.

What are Popular Compensation Tools?

In addition to Coordinape, some of the most popular compensation tools include SourceCred, RabbitHole, Superfluid, Sablier and POAP

Tool	Description
	Coordinape: Reputation-based compensation tool that allows members to vote on how the DAOs budget should be allocated to contributors
	SourceCred: Algorithmically measures participant's individual contributions to a project and displays them in a graph, showing how each contribution ties to the greater effort. DAOs can use this tool to determine compensation for individual members or teams
	Rabbithole: Provides cryptocurrency rewards to users for trying out new dApps, protocols or crypto platforms. As such, DAOs can use the platform as a bounty tool – creating Skills, Tasks and Quests for their members
	Superfluid: Allows for "streaming payments" - a novel form of payment that sends a constant stream of payments (i.e. every second) to a chosen address. This is impossible with traditional fiat currency and has several potential use cases including real-time salary distribution
	Sablier: Like Superfluid, Sablier is a financial streaming platform. Created in 2019, Sablier supports any ERC-20 token and doesn't charge a fee to use the contract
	POAP: Proof of Attendance Protocol (POAP) provides NFTs that allow users to prove they attended a virtual or in-person event. DAOs could use this tool to see who is participating in meetings and adjust compensation accordingly

Chapter 70: DAO Frameworks

<u>What is a DAO Framework?</u>

From a technical standpoint, a DAO is essentially a collection of smart contracts built on a decentralized platform such as Ethereum. One smart contract may issue tokens, another would coordinate voting, a third could set treasury protocols, etc…

While anyone can write these smart contracts themselves (or "fork" the code of an existing DAO), many users find it more convenient to use pre-packaged solutions often called frameworks, launchers or "DAOs-as-a-Service" providers.

Frameworks are "no code" tools that allow users to create a DAO from scratch using a suite of pre-built smart contracts. Nearly anyone – regardless of their level of technical expertise – can log onto these platforms with their wallet, choose from a series of templates, fill out some pertinent information, and click a button to launch a DAO within minutes.

<u>DAO Frameworks Provide Pre-Built Smart Contract Packages That Make It Easy to Launch a DAO</u>
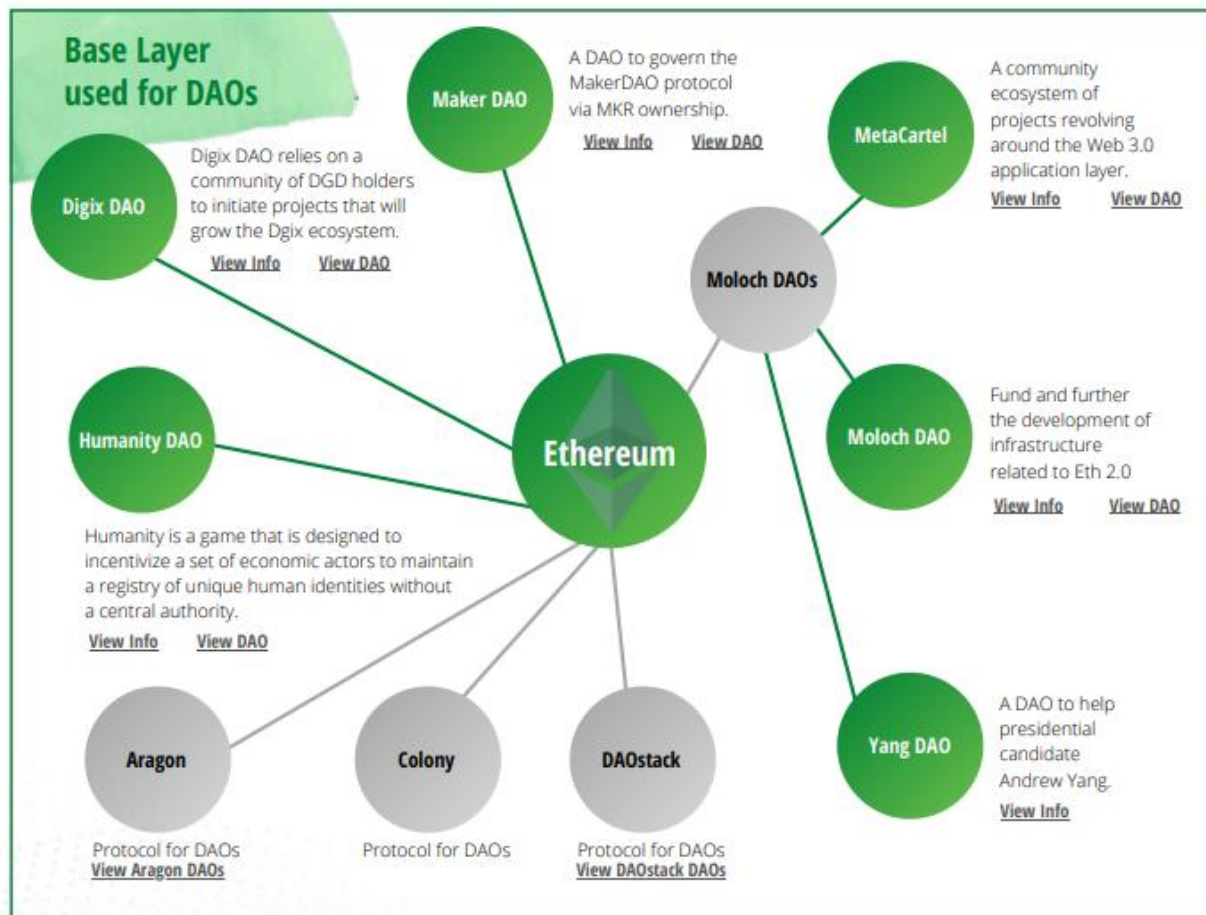
Source: <u>DAOs – A Decentralized Governance Layer for the Internet of Value (George Samman, David Freuden)</u>

_____

While each framework has its own offerings, most offer tools to help users:

- **Create Tokens**: Launch and distribute tokens

- **Distribute authority**: Delegate decision-making authority to certain individuals or groups

- **Coordinate Governance**: Customize voting rights and parameters

- **Facilitate Communication**: Provide forums to make proposals, discuss strategies and coordinate work

- **Manage Treasuries**: Create multisig wallets, monitor treasury analytics and allocate funds

- **Streamline Payments**: Provide payment tools that allow compensation via bounties, tips, salaries or reputation-based schemes

Because every DAO has different needs – for instance, a social DAO will likely have a different voting protocol than an investment DAO – most frameworks provide users a variety of templates to choose from.

While frameworks provide a much simpler user experience, the obvious drawback is the fact is that they can be more difficult to customize to a DAO's specific needs.

Notable frameworks include Aragon, DAOstack, DAOhaus, Colony and OpenLaw's Tribute.

<u>How does a DAO Framework Work?</u>

To understand how frameworks operate, let's take a look at Aragon – a "plug-and-play" tool that allows users to create a fully-functional DAO within minutes. The project was founded by Luis Iván Cuende and Jorge Izquierdo in 2016.

DAOs can choose from several pre-made templates that offer varying governance frameworks, token configurations, dispute-resolution models and voting options. Examples of templates provided by Aragon include the "Company" template (which uses token-weighted voting), the "Membership" template (which uses a one-member-one-vote governance) and the "Reputation" template (which uses reputation-based voting).

_____

Aragon Users Can Leverage Pre-Made Templates to Launch a DAO Within Minutes
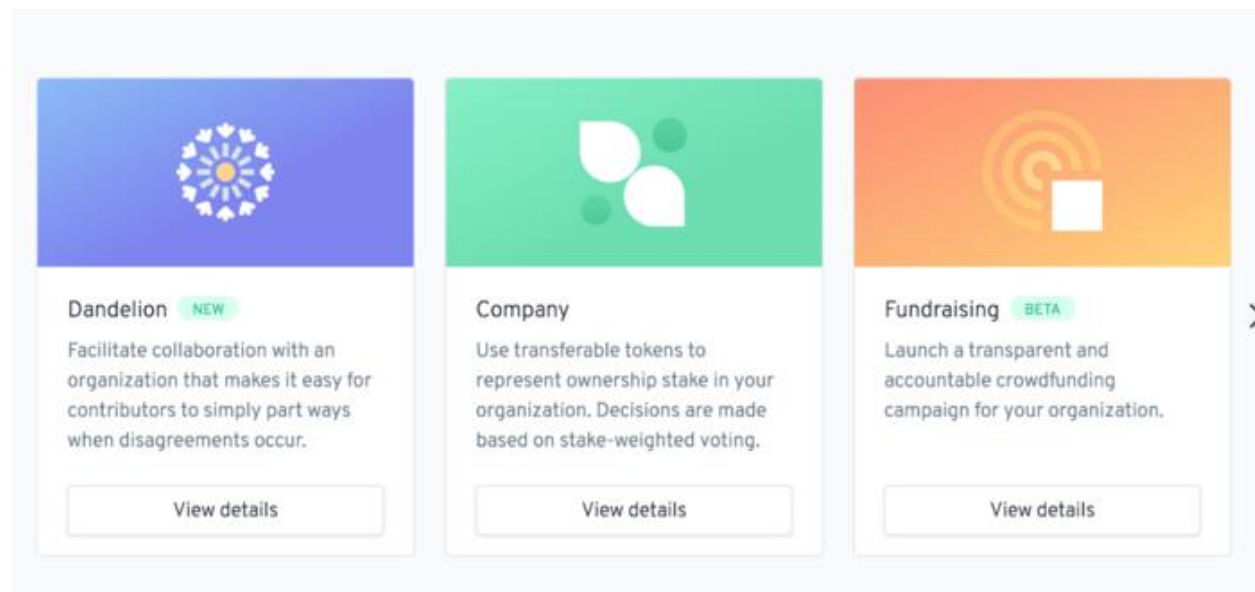
Source: Placeholder VC

Aragon's goal is to become more than just a "launchpad" for DAOs – it ultimately aspires to be a one-stop-shop for all needs relating to decentralized management. As such, the Aragon Network is composed of four main components: Aragon Client, Aragon Court, Aragon Voice and Aragon Govern.

- **Aragon Client:** A plug-and-play solution that allows users to create a fully functional DAO within minutes. Users connect their wallet to Aragon, select a governance template, tweak the voting configurations, enter key token information, select the address of the recipients and then launch the DAO

- **Aragon Court:** Handles subjective disputes that can't be resolved by code. Aragon Court is composed of human jurors who help decide issues. Jurors are required to stake a token known as ANJ to participate and they earn fees if they help successfully adjudicate a resolution

- **Aragon Voice:** The platform's in-house proposal and voting system. Like Snapshot, the tool provides "gasless" voting and is verifiable on IFPS

- **Aragon Govern:** A framework that allows for optimistic or "lazy" governance. In an optimistic governance scheme, anyone can make a proposal (e.g. pay $10 for a picture to use on the website) and it automatically passes if not challenged within a certain number of days. This is ideal for large DAOs that don't want or need to debate and vote on every operational decision

These solutions are designed to work together synergistically. The platform compares this functionality to the current structure of the US government: 1) Voice is the legislative branch,

where token holders make and vote on proposals, 2) Govern is the executive branch, carrying out those decisions and 3) Court is the judicial branch, providing dispute resolution.

The project has achieved impressive traction to date. It is available on both Ethereum and Polygon and is used by more than 3,800 DAOs representing over 300,000 members. Notable users include Aave, Curve and Decentraland.

Unlike several of the other tools previously discussed, Aragon is a DAO itself and is governed by its native ANT token.

<u>What are the Popular DAO Frameworks?</u>

In addition to Aragon, some of the most popular frameworks include DAOHaus, DAOstack, Colony, OpenLaw's Tribute and Moloch.

Tool	Description
	Aragon is the most popular framework with 3,900 DAOs representing over 300K members. Notable users include Aave, Curve, and Decentraland
	DAOHaus supports nearly 800 projects including MetaCartel and Raid Guild. The project is built on Moloch, an open-source collection of smart contracts for DAO governance and operations
	DAOstack focused on addressing governance at scale with its Holographic Consensus model. Notable projects using DAOstack include Gnosis, dxDAO, Liberland and protocols from Polkadot
	Colony focuses on "lazy consensus" (also known as "optimistic voting"), a method where proposals are automatically executed if no one objects during a pre-defined period. This allows for more efficient day-to-day operation
	OpenLaw, through its Tribute platform, combines Moloch smart contracts with legal "wrappers" that customers can use to launch DAOs and register them as official legal entities (such as LLCs). Notable projects include The LAO (a Delaware LLC) and FlamingoDAO
	Moloch is a minimalist set of smart contracts that people can use to create a DAO. It was originally used to create MolochDAO (a grants DAO) and popularized the "ragequit" feature. While technically not a framework as it is defined in this article, Moloch is important to mention because it is used by several DAOs and several DAO frameworks, including DAOHaus and OpenLaw's Tribute

_____

Chapter 71: Problems with DAOs

Although DAOs definitely have their benefits, they also come with their share of challenges. Among the most notable of these are:

- **Lack of legal and regulatory clarity**: Because most DAOs do not register as traditional corporations, they often have no official legal standing
- **Operational Inefficiencies**: Decentralized governance brings its own set of challenges including disorganized decision-making, plutocracy, voter apathy and unfamiliar compensation methods
- **High Fees**: Average fees on popular smart contract platforms can range from $10 to $30, making on-chain voting impractical
- **Usage by Criminals and Terrorists**: One of a DAO's biggest strengths – allowing anonymous individuals to form organizations that exist outside of the traditional financial and legal system – could also prove very attractive for criminals and terrorists
- **Hacks and Scams**: The crypto ecosystem lost over $14 billion to crime in 2021, and DAOs were no exception

We will cover many of these in more detail in Part 8: Challenges Facing Web3, but two are worth looking at a bit more now.

Lack of Legal and Regulatory Clarity

Given that DAOs have no physical location and don't register as corporations, they often exist in a legal state of limbo.

This creates several potential risks, including:

- **Tax Liability**: While it's clear that *individuals* receiving compensation from a DAO or selling governance token must pay taxes, what's less clear is whether the DAO *itself* is a taxable entity. If so, who is responsible? Will members have to split the bill? Although unlikely, a worst-case scenario would find everyone holding a governance token liable for the tax burden.

- **Personal Liability**: One of the benefits of a traditional LLC is that it offers its partners protection from personal liability. For example, if an LLC goes bankrupt, creditors can only seize the assets of the business, and not the owner. DAOs do not currently offer the same level of protection, leaving members at risk. For example, what happens if someone sues a DAO, are the members liable?

- **Inability to do Business**: The legal uncertainty around DAOs brings up another concern – most traditional corporations can't or won't do business with a non-legal entity. This cuts off several lucrative options and potentially hurts the growth of the ecosystem.

_____

Although we are making headway – both Wyoming and Vermont have allowed DAOs to incorporate as limited liabilities companies – we are still in the early days and the laws haven't quite caught up yet.

One entity trying to bridge this gap is OpenLaw (now Tribute Labs), who provides legal "wrappers" for smart contracts and helps DAOs register as legal entities. The platform's most famous project – The LAO – registered as a Delaware LLC in 2020 and complies with the applicable regulations for an investment firm (including KYC and accreditation requirements for its members).

Operational Inefficiencies

Running any business is difficult, let alone one with no headquarters, no managers and no permanent workers. While there are a host of challenges faced by DAOs, some of the more common include:

- Decision-making
- Plutocracy vs. Apathy
- Remote work
- Compensation
- Lack of tooling

Let's look into each of these…

Decision making

While democratic decision making has numerous benefits – including input from multiple viewpoints, bias checks and increasing stakeholder buy-in – it also has several well-documented drawbacks.

_____

Real-Time Photo of DAO Governance
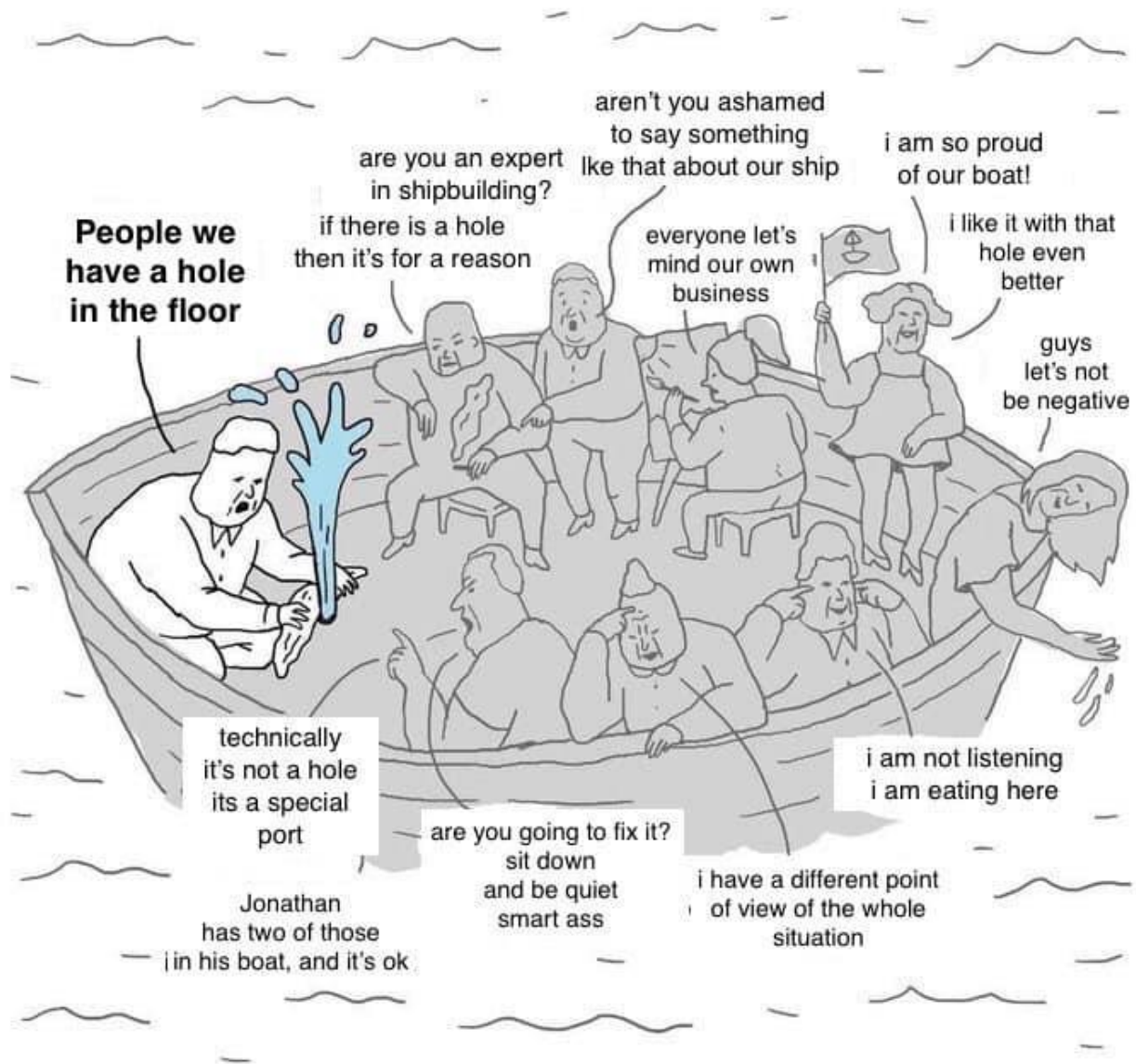
Source: Reddit

Often maligned as "decision by committee", critics argue that is a poor way to run an organization for several reasons:

- **Less Accountability**: Individuals who have less stake in the outcome of a given decision generally spend less time evaluating solutions and are more prone to suggesting extreme solutions

- **Missed Advice**: Groups often fail to consider the experience of the most relevant person in the room

_____

- **Noise**: Without a manager to enforce meeting rules and keep discussions on track, large groups often get bogged down in minutia and waste time

- **Peer Pressure**: Critics argue that social pressure has a major influence on group decisions, and people who have relevant concerns are often reluctant to share them for fear of "rocking the boat"

- **Competition**: Individuals may try to "one-up" each other by suggesting more and more extreme solutions

Plutocracy vs. Apathy

There is a natural push and pull between centralization and decentralization in a DAO. While decentralization has its benefits, critics would argue that *too much* decentralization is just as bad as it means each individual has less at stake. This can slow the pace of decision-making and lead to apathy. Indeed, in one study it was estimated that fewer than 10% of members on Aragon and DAOstack enabled organizations participated in voting (although DAOhaus had a much higher percentage).

Voting Participation is Less Than 10% in Many DAOs

Table 3 Voting statistics by platform and network

	DAOstack			DAOhaus			Aragon		
	total	mainnet	xDai	total	mainnet	xDai	total	mainnet	xDai
Users who vote	4.5%	6.3%	2.1%	38.37%	39.5%	24.32%	-	6.18%	-
Votes per voter	4.6	4.64	3.64	4.26	3.96	7.28	-	4.08	-
Approved prop.	74%	74%	76%	92%	93%	87%	-	81%	-
Positive votes	86%	86%	95%	91%	90%	98%	-	94%	-

Source: A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain - Youssef Faqir-Rhazoui, Javier Arroyo and Samer Hassan

While upping the level of centralization and bringing more structure to the DAO would seem like the simple solution, that brings its own challenges as well.

The most obvious problem with a small set of large token holders is the risk of plutocracy (i.e. a "government by the wealthy").

We've seen this dynamic play out before. Last summer, venture capital firm Andreessen Horowitz – a large stakeholder in the Uniswap DAO – spearheaded and passed a proposal that many members argued benefited them personally.

Ultimately, like most things, there's probably a middle ground here that each DAO will have to find on its own.

_____

<u>Remote Working</u>

While remote working has its benefits, it also comes with its fair share of challenges. Some of the more common are:

- **Poor Mental health:** Working from home can be lonely, and many remote workers report increased levels of stress, depression, feelings of isolation and sleep problems.

- **Distractions:** Home offices provide several potential distractions such as video games, online shopping or social media. In addition, friends, family members and pets often drop in at unexpected times

- **Coordination Difficulties:** It's difficult to coordinate meetings and working groups in large organizations spread out over multiple time zones

- **Lack of Documentation:** In office settings, a lot of experience is shared through "tribal knowledge" – information that is only known by people on the inside of a group. This wisdom is often shared at random times, such as over a coffee break in the kitchen. Because remote workplaces cannot replicate this, they need strong documentation and knowledge management

- **Poor Culture:** Without meeting others in person, remote workers often feel they don't really know their peers

Fortunately, the benefits of remote working appear to outweigh the downsides, and <u>Forbes</u> has shown that remote teams are 35%-40% more productive than their office counterparts. It's also very possible to remove many of these challenges with proper strong operational management. If you'd like to learn more, please check out my article <u>"Kill the Office!: How to Make Remote Teams a Competitive Advantage".</u>

<u>Compensation</u>

Determining how workers are compensated is a major challenge for DAOs. While we've discussed several potential solutions, each of these has a downside:

- **Bounties**: While bounties work well for certain departments and tasks (e.g. paying someone to fix a bug) they work less well for others. In addition, bounties often lack a "qualitative" metric. Sure, you can pay a bounty to someone to build a website, but what if it's ugly?

- **Reputation-based Schemes**: Tools such as Coordinape are vulnerable to a host of problems. In the most benign cases, there's a risk that they will become popularity contents where people award tokens to their friends. The worst cases may see collusion and bribery.

- **Salary**: Salary may be ideal for many positions in a DAO, but it runs counter to the ethos of a free and unconstrained work force. In addition, when determining salary, members may rely on their own personal perceptions of value rather than what is "market"

Ultimately, I believe there's a strong change that DAOs will rely on multiple methods – using certain methods for certain types of tasks and often combining methods. These structures will likely vary from DAO to DAO and it's likely that we will see an entire generation of "DAO ops" professionals arise to coordinate.

<u>Poor Tooling</u>

Traditional corporations have access to a wide variety of tools to manage remote workforces including Zoom, Slack, Google Drive and Trello.

Unfortunately, many of these tools aren't always a great fit for the unique needs of a DAO. In particular, they often come with several concerns such as:

- **Centralization:** Most of these services are centralized, which could be a major hurdle for DAO adoption. For instance, Google Drive is a great knowledge sharing tool, but it's controlled by Google. This defeats the whole purpose of decentralization…in today's world, Google restricting access to your documents may be as bad as a bank confiscating your funds

- **Applicability:** Legacy tools are rarely designed for the specific needs of DAOs. For instance, there are hundreds of tools for payroll management, but only a few that don't focus on traditional salaries or hourly wages. And anything that connects to a blockchain? Forget about it…

- **Cost:** Enterprise grade tools often cost thousands of dollars per month. This is out of reach for many DAOs, and even those that can afford it may have trouble justifying costs in a democratized voting environment

While we have reviewed several solutions to these problems, it's helpful to remember that the DAO tooling space is still extremely early and, as such, DAOs will have to figure it out on their own for a while.

_____

Chapter 72: Why DAOs Will Eat Corporations (and maybe the World…)

<u>Could DAOs Replace Corporations?</u>

While the thought of DAOs replacing traditional corporations may seem ridiculous at first glance, it's important to remember that corporations – at least in the form we know them today – are a relatively new phenomenon.

The first privately-owned corporations appeared during the "Second Industrial Revolution" of the late 1800s to replace the joint-stock company model popularized by entities such as the Dutch East India Company.

These entities were disruptors in their own right, and leveraged new organizational forms and management theories to respond to the rapid economic changes driven by the global shift to automation and mass production.

In particular, they pioneered the use of standardized processes (e.g. the assembly line), regulated working hours, and rigid hierarchies to break down extremely complicated tasks into small pieces that individual employees could easily manage.

<div align="center"><u>Corporations Were Designed for a By-Gone Era</u></div>
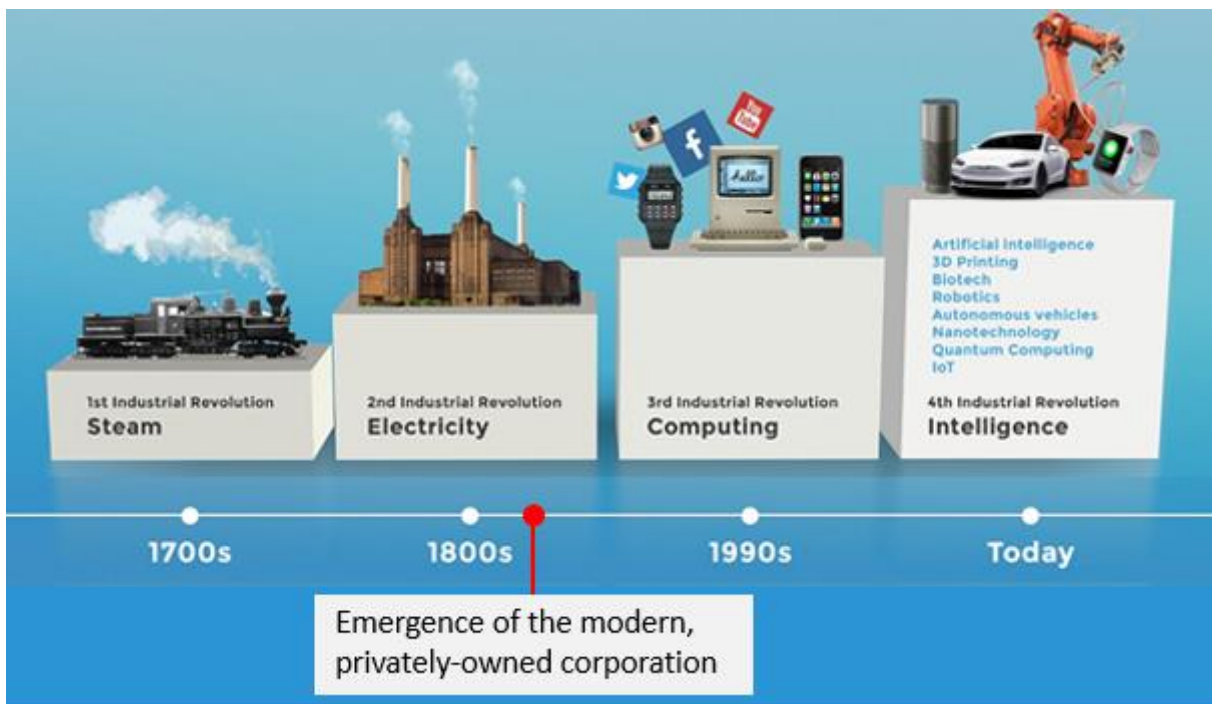
Source: <u>The Waves</u>

While these systems worked exceptionally well for over a century, they have proven less effective in the information age, which rewards speed and agility over hierarchy and process.

_____

_____

To make matters worse, the rigid organizational structure of the modern corporation is also becoming less appealing to workers, who demand more connectivity, ownership and flexibility. Indeed, if you pay attention, you'll notice three important "megatrends" shaping our economy:

- **Increased Pace of Globalization**:   The world is becoming more hyperconnected – 60% of the globe have access to the internet and Americans spend 8 hours a day online

- **Decreasing Trust in Corporations**: Raised during the Great Recession, Generation Z is rejecting corporations

- **Increase in Freelancing**:   We continue to transition to a "gig economy" driven by temporary positions and short-term agreements. Freelancing increased 33% in 2021 and it is expected to account for over half the workforce in the US by 2027

Indeed, the corporation as we know it was designed for a by-gone era, and its structure is being assaulted from all sides by a changing consumer and labor landscape.

DAOs, on the other hand, appear to benefit from all of these trends.

For the first time in history, blockchain technology makes it possible to create an entity that is simultaneously flat, fast, flexible *and* global. Unlike multinational corporations of the past, this new entity won't have to navigate a patchwork of local regulations, contend with international labor laws nor will it face restrictions on international currency transfers.

As such, DAOs could represent the most efficient blend of capital, labor and ideas that the world has ever seen, and may well become the dominant organizational structure of the Fourth Industrial Revolution.
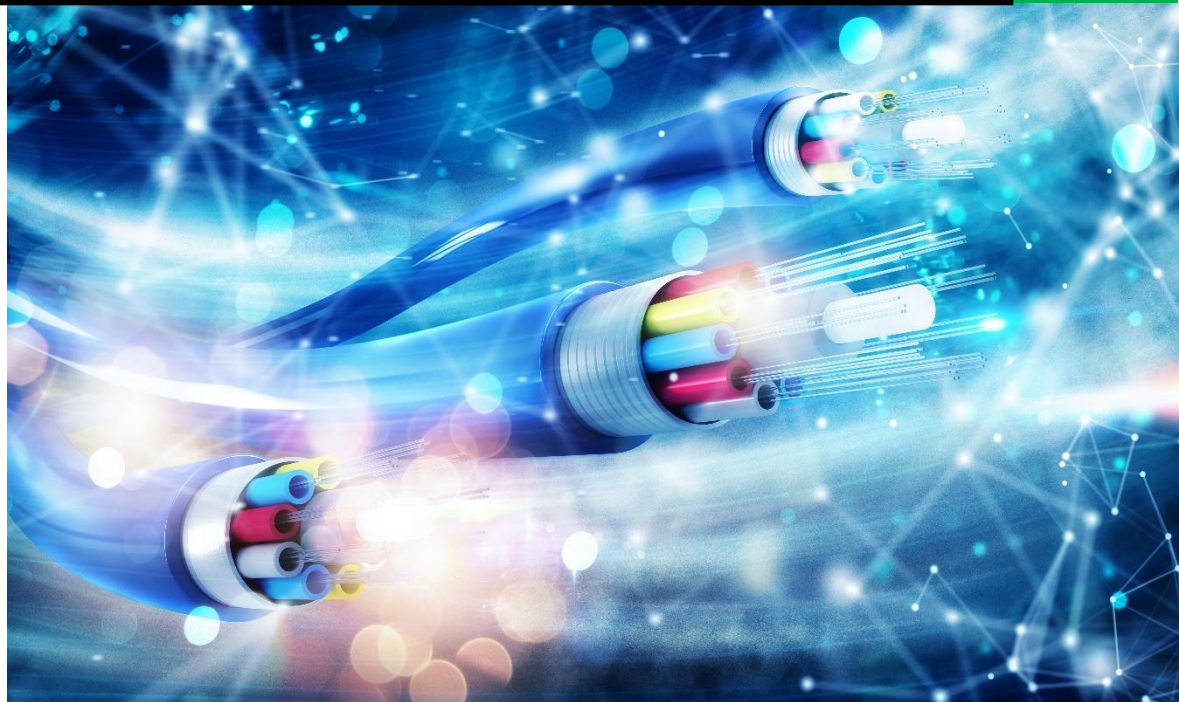
_____

Part 7: Web3 Infrastructure

_____

Chapter 73: Web 3 Infrastructure

To understand how Web3 would work, we first need to understand how the internet works today.

Although the terms are often used interchangeably, the internet and web aren't the same thing.

The internet is the **physical** infrastructure of computers and cables that powers the world wide web – a **digital** collection of webpages and apps that lives on this network.

In 2006, the late Sen. Ted Stevens was relentlessly mocked for saying that "the internet is a series of tubes".

Ironically, Stevens was kind of right. At its core, the internet is nothing more than a collection of computers that are connected to each other through a global network of "tubes" (aka "wires"). In fact, that's where the word comes from – interconnected networks.

These connections allow computers to "talk" to each other to do things such as 1) send an email, 2) get a website or 3) buy goods and services.

To understand how a decentralized internet works, let's take a journey though the evolution of these computers and wires.

<u>Pre-Web</u>

The internet was originally created by the United States Department of Defense as a messaging system that could withstand a first-strike nuclear attack.

The first versions, known as ARPANET, were decentralized – they were little more than groups of computers (fewer than 100 for most of the 70s) directly connected to one another through telephone lines.

_____

_____

The Internet in 1972 Connected a Handful of Computers Through Telephone Lines
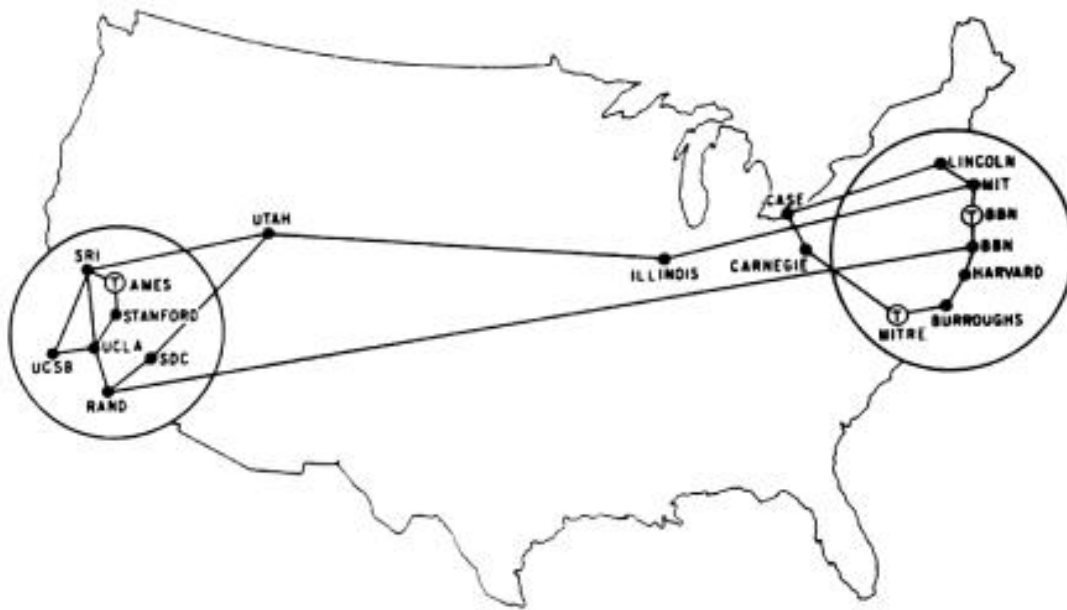
Source: Quartz

While telephone lines proved sufficient for the early internet, they soon ran into problems.

Because computers think and communicate in 1s and 0s – a language called "binary" – all information is sent across the internet in this format. Each one or zero is called a "bit", and 8 bits make up a "byte". For example, in computer language the word "cat" translates to "01100011 01100001 01110100", while a picture of a cat could contain millions of 1s and 0s.

These 1s and 0s *can* be transferred over a standard telephone line by transmitting alternating electrical pulses (1 if the pulse is on and 0 if it is off), but it's not very efficient. Commonly known as "Dial-Up", these networks were limited to 56 kilobytes per second (at that rate it would take over a minute to download a modern iPhone photo and 8 days to download a 4K movie).

As such, the infrastructure eventually expanded into new mediums with much faster speeds, including:

- **DSL (100 Mbps)**: DSL also transmits electrical pulses through existing copper phone wires, but it travels over previously unused frequency ranges, making it much faster than Dial-Up
- **Cable (1 Gbps)**: Cable companies can transmit electrical pulses through the same coaxial cables used to provide TV services
- **Fiber Optic (5 Gbps)**: Fiber optic cables use alternating pulses of light to represent 1s and 0s (light on for 1; light off for 0). They are the preferred medium for long-distance transmission, and 99% of international traffic is carried over fiber optic cables (most of them undersea)
- **Wi-Fi (100 Mbs – 1 Gbps)**: The internet also uses "Wi-Fi", a wireless network that uses radio waves. By adjusting the frequency of these waves, networks also use the binary formula, sending one type of wave to represent a "1" and another to represent a "0". Your smart phone is actually a radio!

_____

_____

- **Satellite (100 Mbps)**: Radio waves can also be used to send data to and from existing satellites

These evolutions increased the efficiency of the network and allowed for the creation of new paradigms such as the world wide web.

Web 1.0

For decades, the internet was primarily used as a messaging device. From the time the first email was sent in 1971 until the early 1990s, the vast majority of the internet's traffic was text based and largely used for academic purposes.

This all changed when Tim Berners-Lee's invented the world wide web.

As the name suggests, the world wide web introduced the first websites to the internet in 1991. Over the next few years, thousands of pages were created that provided users with an alluring medium that allowed for the transmission of pictures, videos and audio. This effectively opened up the internet to everyday users, ushering in a new era of global communication and knowledge sharing.

### Netscape Navigator was one of the First Web Browsers

Source: ARN

_____

_____

The web functioned by linking an interconnected system of webpages through a communication protocol known as the HyperText Transfer Protocol (or HTTP).   HTTP creates a set of rules that allow individual computers to request and receive information from websites through a schema known as the client-server-database architecture.

<u>HTTP Allows Individual Computers to Talk to Websites</u>
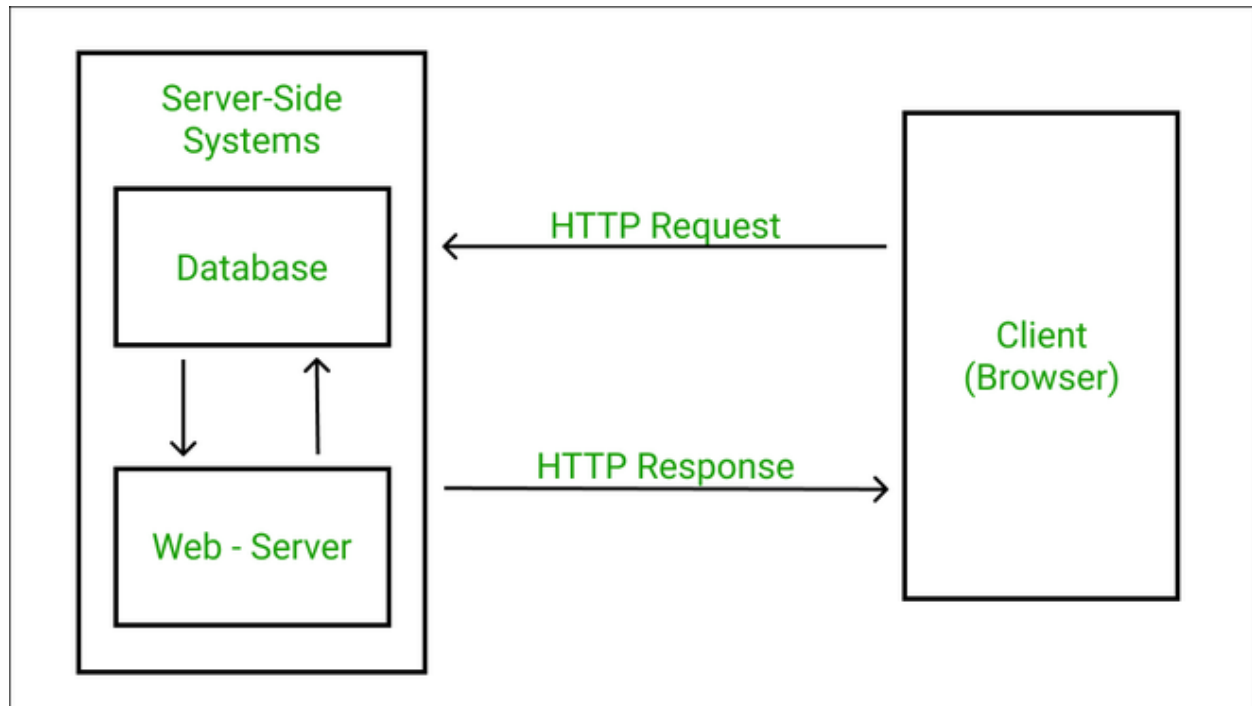
Source: Reem Shaikh via <u>Medium</u>

As the name suggests, there are three key players in this system:

- **Clients:** Clients are individually owned devices, such as personal computers, laptops, tablets or smart phones. Although they do have limited computing power, their primary function is to receive data and present it in a graphically pleasing format to the user (such as a website). Most websites are viewed through browsers (e.g. Google Chrome, Firefox or Safari) which are responsible for sending data requests to servers (and also responsible for receiving the data that is sent back).

- **Servers:** Servers are large computers that have two primary functions: 1) they route data from client requests to the applicable database (and back again) and 2) they perform the complex logical operations that determine what data to show you on YouTube or Facebook.

- **Databases:** Databases store data, which can be anything from photos on Facebook, to credit card number, to health records, to bank account information, to your personal shopping history on Amazon.

So when you want to access a website: your computer sends a request to a server to get information, the server forwards that request to a database, the database gathers the applicable content (e.g. text, videos, photos, comments, posts, tags, likes, etc..) and sends it back to the

_____

_____

server, the server transfers it to your browser, and then your browser organizes everything into a visually pleasing format on your device. While this may seem complicated, it frequently happens in a fraction of a second (often *literally* at the speed of light).

Although revolutionary, the major problem with Web 1.0 was that the pages were "static" – like a newspaper or magazine, users could do little more than passively read what was displayed on the site.

Web 2.0

The next major innovation in the web occurred in the early 2000s with the introduction of interactive webpages.

These sites provided a richer experience, allowed users to interact through social media and encouraged user-generated content.   Popular Web 2.0 sites include social networks (Facebook), video sharing sites (YouTube), blogs (Medium), wikis (Wikipedia), microblogging sites (Twitter), and web applications (Google Docs).

<u>Web 2.0 – the "Interactive Web" – Evolved in the Early 2000s</u>
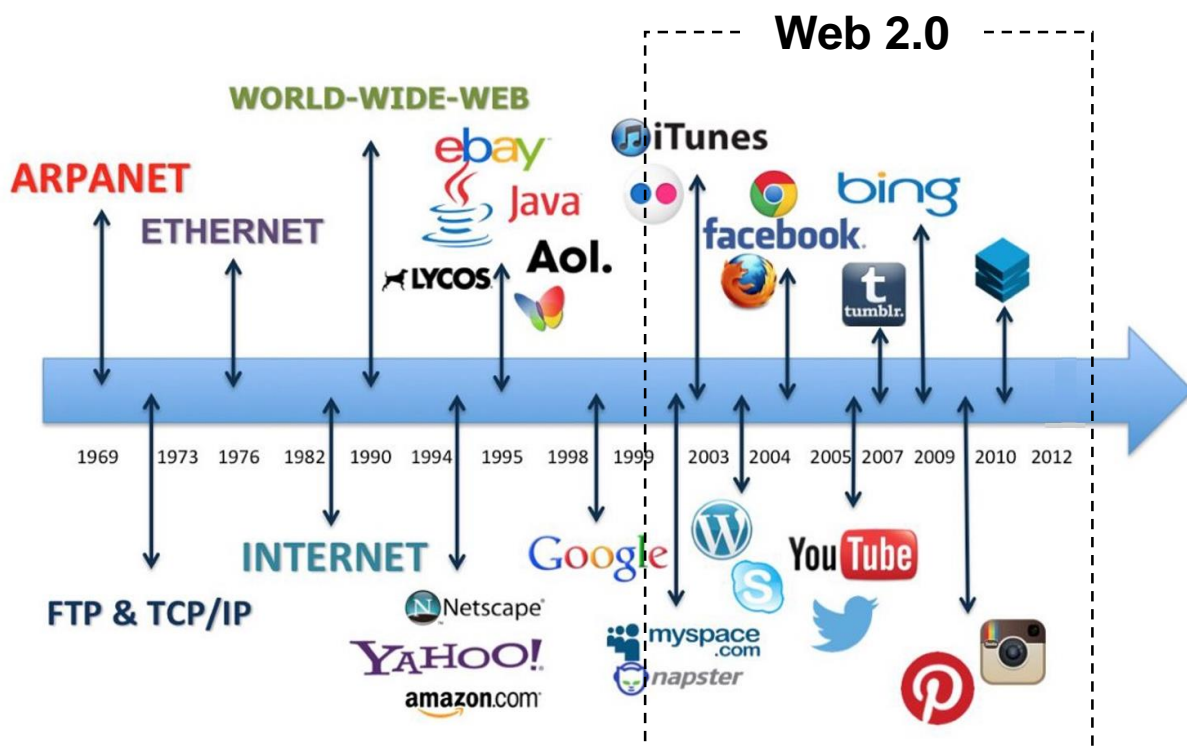
Source: Montasser via Medium

This new breed of website required a lot more storage and computing power to be successful and, as a result, we soon started to see the leaders in each of these categories – such as Facebook for social networking, Amazon for e-commerce, and Google's YouTube for user-generated video – leverage economies of scale to break away from the pack and grab extraordinary market share.

_____

_____

Indeed, today it is estimated that four companies – Amazon, Microsoft, Google and Alibaba – own 67% of all major cloud servers and databases, and they hold many of them in a handful of locations known as hyperscale data centers (multi-hectare facilities designed to host thousands of "room-size" computers).

Map of Microsoft, Amazon and Google's Data Centers

Source: Atomia. Note: Shown data center does not represent Brazil location.

So in reality, the modern internet isn't all that "global" as most of it is effectively stored in a few dozen locations owned by a small handful of companies.

Given that our modern economy runs off of data – we produce 28 trillion bytes every *second* – this should be a major cause for concern…

_____

_____

Web3

The next version of the internet will likely upend this structure. Instead of hosting most of the world's data and computing power in centralized data centers, Web3 intends to "cut out the middleman" with two recent inventions:

- Blockchains – decentralized databases which can replace traditional databases
- Smart contracts – computer programs that can replace centralized servers

When combined, these two technologies are often referred to as "smart contract platforms" (which we covered in detail in Part 3).

This is revolutionary – **for the first time in history, smart contract platforms give users full ownership and control of their data, content and assets**. This means that no one can censor users, seize their assets, block their access, charge them outrageous prices for selling goods online or monetize their data without permission.

To borrow a phrase used by Messari's Eshita Nandini – if Web 1.0 was the "read-only" web, and Web 2.0 was the "read-write" web, then Web3 is the "read-write-own" web.

Web3 Gives Users Full Ownership and Control of their Data, Content and Assets

Source: Myraah.io

While the use of smart contract platforms is groundbreaking, they are not enough on their own to create truly a decentralized internet as they: i) need additional pieces of infrastructure such as wallets and node providers, ii) require the replacement of the traditional "wires" of the internet with a decentralized alternative and iii) still need databases, albeit in a slightly different way.

Although we are probably still some time off from realizing the vision of a fully decentralized web, we've made a lot of headway and are starting to get a sense of what the final product may shape up to look like.

Preethi Kasireddy provides a great overview of this in her article "The Architecture of a Web 3.0 Application":

_____

_____

Key Components of Web3 Infrastructure
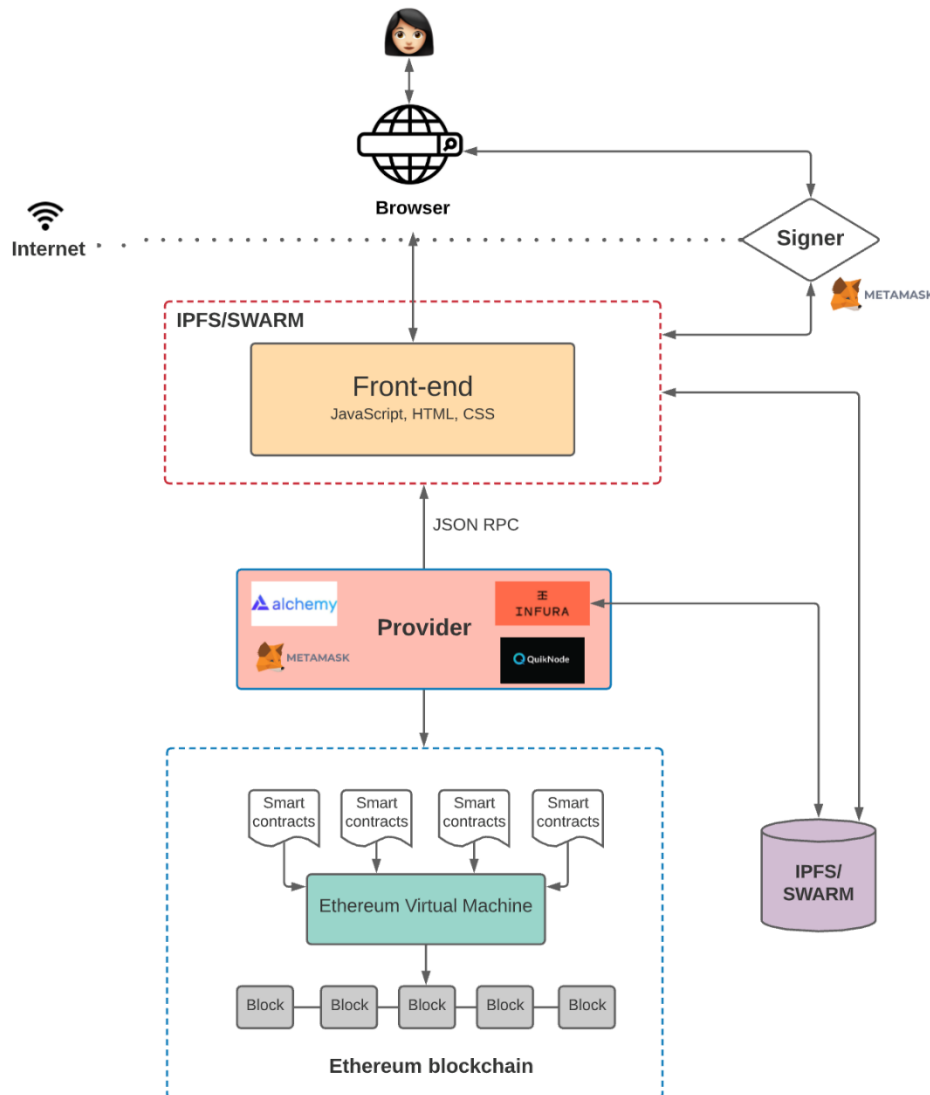
Source: Preethi Kasireddy via preethikasireddy.com

Although the user experience of a decentralized internet will likely stay more or less the same (i.e. users will still visit a website, click a few buttons and get the data they want), what's going on in the background will be very different. In the next version of the internet, when a user wants to access data, she will likely follow the below roadmap:

1. **Browser**: The first step in the user journey will likely remain largely the same, with consumers accessing the internet through a browser (technically, we may all soon access it through virtual or augmented reality devices, but we'll get to that in a second)

2. **Wallet**: Perhaps the biggest noticeable change for the user will be the addition of a digital wallet, which will replace emails and passwords as the primary means to sign into a website

_____

_____

3. **Decentralized Internet**: Once signed in, information could travel through the network over a decentralized internet service provider (ISP) such as Helium

4. **Node Providers**: In order to access a smart contract platform, users need to run a "node". We'll define what that means in a bit, but the key takeaway here is that running a node is challenging and, as such, most users will rely on third-party services known as node providers

5. **Smart Contract Platforms**: Smart contract platforms such as Ethereum will replace traditional servers and databases

6. **Data Storage**: There will still be a need for databases, but decentralized databases such as IFPS or Arweave will work a bit differently than databases today, connecting directly into the "front-end" and assuming more of a support role

In addition to the above, Web3 will require several tools designed exclusively for blockchains such as decentralized domain name servers, Layer 2 solutions, querying tools, oracles, bridges and decentralized computers.

In the interest of clarity, we won't expand on these here but will instead dive deeper into them in the next section…

_____

_____

Chapter 74: Virtual worlds

While it's definitely possible to access Web3 from a traditional browser, in the future we will likely experience it through the "metaverse".

Much as the World Wide Web is an intertwined network of billions of websites, the metaverse is an interconnected system of virtual worlds. Users will be able to freely navigate between these spaces and access whatever type of content they desire.

<u>The Metaverse is an Interconnected Network of Virtual Worlds</u>
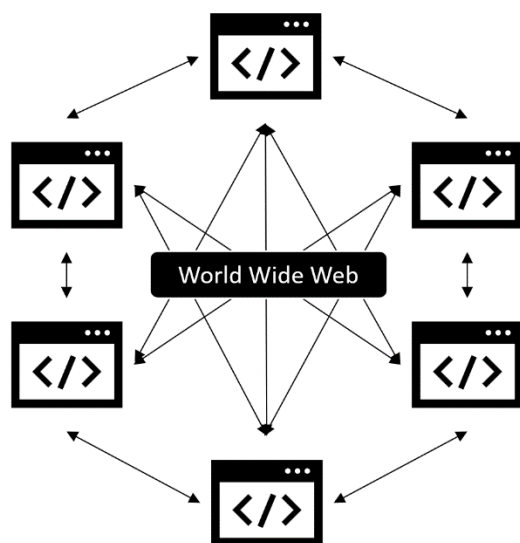
The world wide web is a network of interconnected websites
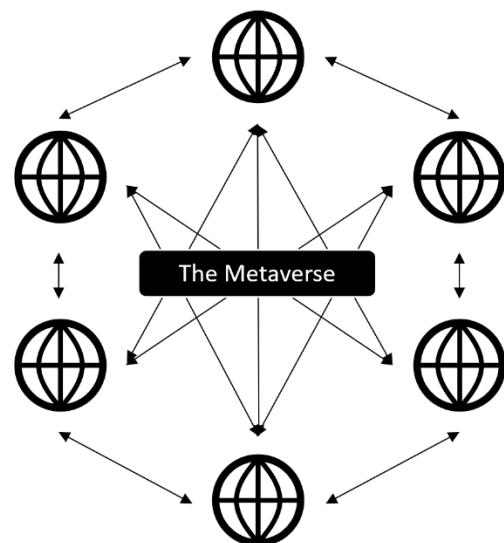
The world wide web is a network of interconnected virtual worlds

We've already discussed virtual worlds in Chapter 28, but as a reminder they are immersive 3D spaces that allow users to explore, interact with other users, create and trade digital goods, participate in meetings, attend events, play games and build in-world objects and landscapes.

Virtual worlds often host their own self-sufficient economies which include:

- **Land** which can be bought, sold, rented and developed
- **Digital Goods** which can be consumed and traded
- **Native currencies** to buy and sell goods and services

Although many virtual worlds are currently PC and / or mobile-based, it is expected that most will transition to virtual and augmented reality as the technology continues to mature.

_____

_____

Chapter 75: Wallets

Wallets serve as a user's gateway to Web3.

The term itself is a bit of a misnomer, as they do so much more including:

- **Provide Access to Funds:** As the name implies, wallets grant users access to their funds
- **Connect with dApps:** In Web3, wallets replace passwords – once you connect to your wallet you can automatically use this to connect to any decentralized application ("dApp")
- **Interact with dApps:** Once you are on a dApp, wallets allow you to use your coins for a variety of purposes, such as spending them in games, staking them on a smart contract platform, buying NFTs, gambling with them, trading them on decentralized exchanges, etc…

To understand the importance of wallets better, let's look at MetaMask, the most used wallet on the Ethereum network.

How do Wallets Work?

The most popular wallet is MetaMask, an Ethereum-based online – or "hot" – wallet. "Hot" wallets are always connected to the internet. While this makes them less secure, it also makes them much easier to use than "cold" wallets (such as Ledger Nano) which aren't connected to the internet.

Source: Verum Capital

_____
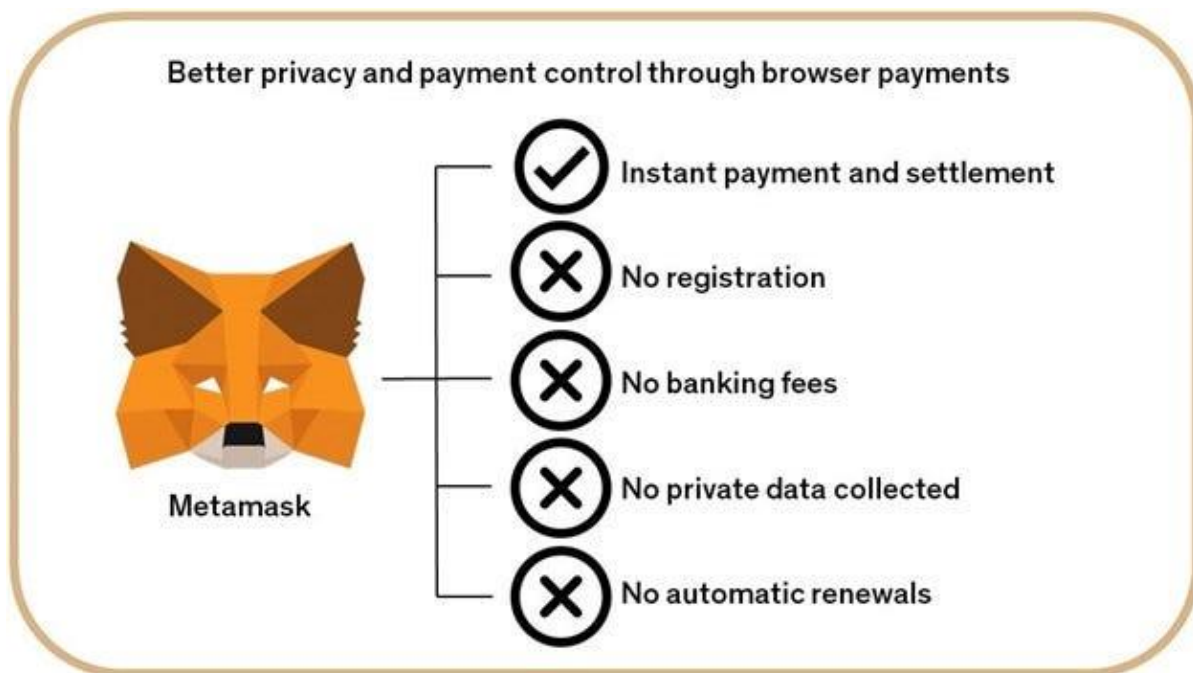
Metamask is free to use, easy to setup and – perhaps most importantly – is completely anonymous (all anyone will ever see is a number).

As discussed above, the product has three key functions. It serves as a wallet, a connection point and a Web3 "browser".

1.   Wallet

Like all crypto wallets, MetaMask does not hold cryptocurrencies (remember that they are stored on a blockchain), but instead holds a user's private keys. The user maintains full control over these keys (and therefore their funds), and they can't be forcibly confiscated by anyone (unless someone physically coerces you to give up your password).

Although MetaMask is closely connected to the Ethereum blockchain, it does not limit the wallet to Ether. The wallet can host a vast selection of different ETH-based currencies and tokens built using, for example, the ERC-20 and ERC-721 standards.

2.   Connecting to dApps

One of the cool things about Web3 is that you don't need passwords.

Once you are logged in, wallets such as MetaMask give you access to a variety of Web3 services – anything from DeFi exchanges to NFT marketplaces to online banks to games.

3.   Interacting with dApps

Once connected to a dApp, users can spend their coins in games, stake tokens in gambling applications, make loans, etc…. For instance, through MetaMask, users can:

- DeFi: Buy, sell, trade, stake, borrow or lend cryptocurrencies
- NFTs: Buy, sell, trade, stake, borrow or lend NFTs
- DAOs: Vote in DAOs
- Web3: Play blockchain games, stream songs, purchase articles, etc…

Basically, you can do almost anything you can do on the internet with Metamask!

Key Players

Although MetaMask is the market leader, there are several popular crypto wallets including Rainbow, Wallet Connect, Coinbase Wallet and Phantom.

Wallet	Description
METAMASK	Metamask is the most popular wallet and is designed for the Ethereum ecosystem (which includes all Layer2s such as Polygon, Optimism and Arbitrum)

_____

coinbase | Wallet	Coinbase wallet is non-custodial wallet developed by the exchange Coinbase. It supports the Ethereum, Binance and Solana ecosystems
WalletConnect	Wallet Connect is an open-source protocol that allows users to connect cold wallets such as Ledger to dapps
rainbow	Rainbow is an alternative to Metamask and primarily serves the Ethereum ecosystem
Phantom	Phantom is Solana's most popular wallet

_____

## Chapter 76: Decentralized Domain Name Servers

What is the DNS?

Every device on the internet has a unique address – called an IP address – that helps other computers identify it. Unfortunately, this address is represented with a string of numbers such as "198.61.190.243".

As you can imagine, human beings aren't very good at remembering random strings of numbers, nor do they provide any context as to what's on the site. That's why the Domain Name System (DNS) was created – it serves as the "phonebook" of the Internet and translates IP addresses into human readable names.

For instance, let's say you wanted to look up www.facebook.com.

1. Your computer would send a request for www.facebook.com to a DNS server
2. The DNS server would look up the name www.facebook.com, find its IP address and send it back to you
3. Your computer would then use this new IP address to make a request to directly to Facebook's servers
4. Facebook would send the requested webpage back to your computer
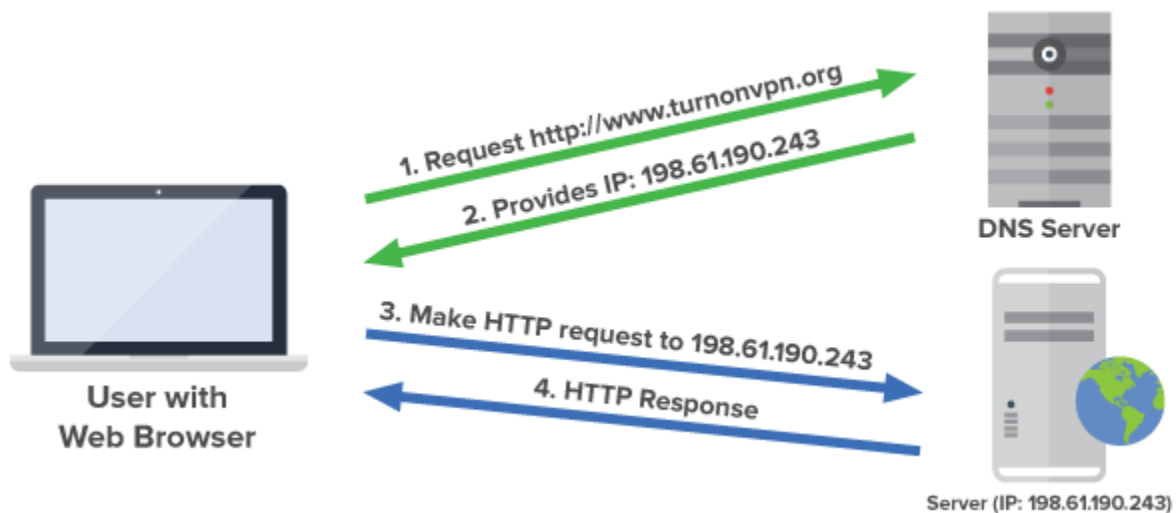
Source: Devopedia

The Domain Name System is not just one server, but instead a global collection of servers. That way, if one doesn't know the address you're looking for, it can route it to another one. This also provides redundancy in case a single server is attacked or goes down.

_____

_____

While the DNS is extremely important to the internet, it has one major flaw – it's centralized. This creates numerous risks including the lack of privacy, the potential for censorship and security vulnerabilities.

As such, decentralized DNSs such as the Ethereum Name Service, aim to supplant this ~40 year old system and become the "phonebook" of the blockchain.

How do Decentralized DNS services work?

The Ethereum Name Service (ENS) is virtually identical to the internet's DNS system, in that it translates human-readable names into computer addresses

For instance, without ENS, if you wanted to pay your friend in cryptocurrency, you'd have to know the public address of her wallet, which might look something like "0x787192fc5378cc32aa956ddfdedbf26b24e8d78e40109add0eea2c1a012c3dec". ENS allows users to create "nicknames" – such as "Alice.eth" – and attach them to their wallet, allowing anyone to send any Ethereum enabled token to that address.

ENS operates using two main components, a main "registry" and a collection of "resolvers". The registry contains all the "nicknames" (called domains) registered on the system and the address of their respective resolvers. The individual resolvers contain the information necessary to match each domain to its actual Ethereum address.

_____

_____

The ENS Registry Contains Individual Resolvers That Can Translate Each Domain

ENS Registry

eth
- owner: 0x1234...

inigomontoya.eth
- owner: 0x34567...
- resolver: 0x45678...

metamask.eth
- owner: 0x56789...
- resolver: 0x67890...

alice.metamask.eth
- owner: 0x7890A...
- resolver: 0x890AB...

Resolvers
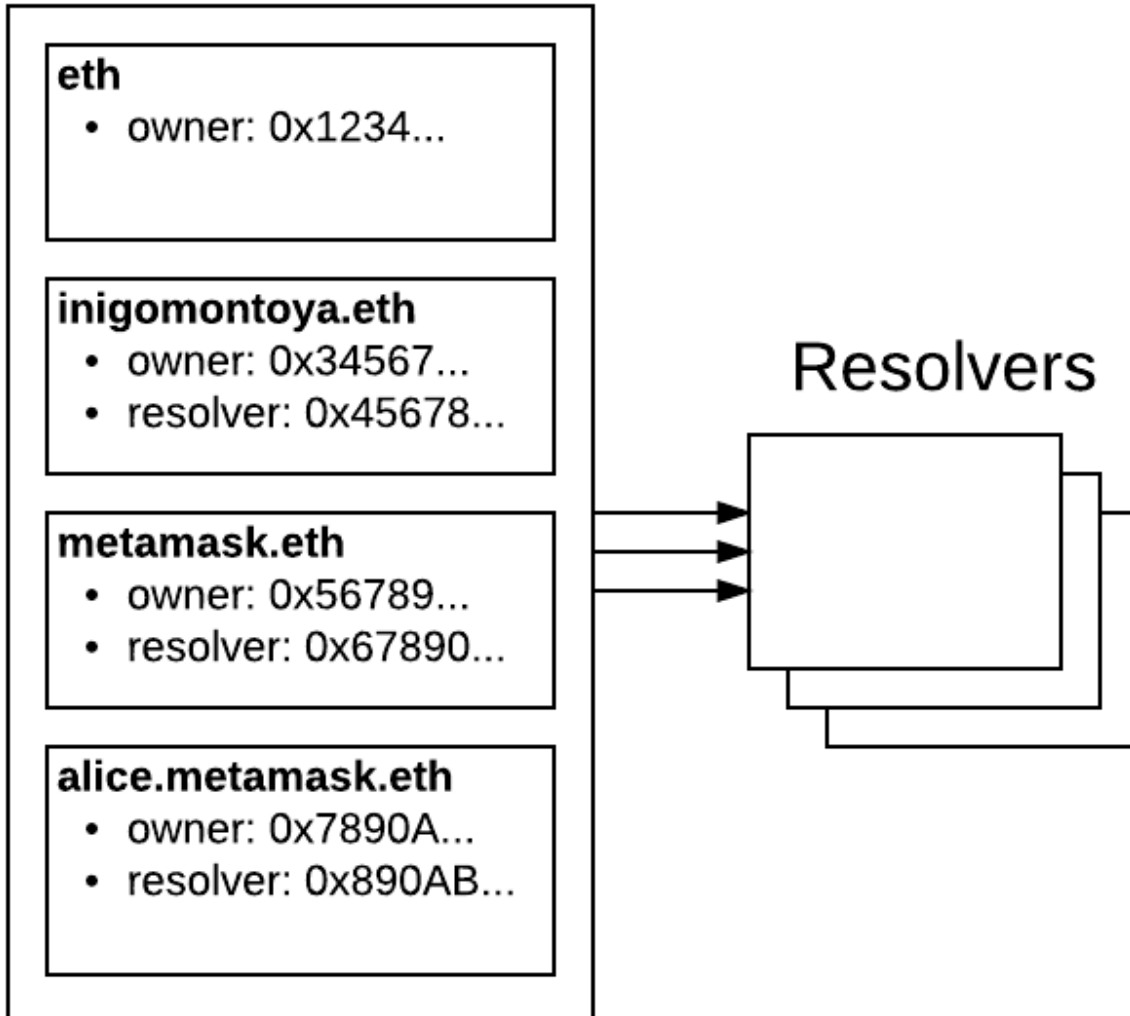
Source: ENS

So if someone wanted to send 10ETH to "alice.eth" using Metamask:

1. The user would open their Metamask wallet, hit the "send" button and add "alice.eth" as the recipient's address
2. The system would then query the main registry to find out which resolver is responsible for "alice.eth"
3. The register would return the applicable resolver
4. The system would then query the resolver for the correct address, which would return "0x787192fc5378cc32aa956ddfdedbf26b24e8d78e40109add0eea2c1a012c3dec"
5. Metamask would then use this new address to complete the transaction

Like the DNS, this all occurs "under the hood", so from a user perspective they simply type "alice.eth" in the address and the money is on its way.

_____

While ENS originally only worked for .ens names, in late 2021, the protocol announced that it would also be integrating traditional domain names into the system. This opens up a world of potential as it makes it possible to register urls such as "alice.com" to a wallet and allow it to receive cryptocurrencies.

Key Players

Notable players in the decentralized DNS space include ENS, Unstoppable Domains, Bonfida, Handshake and Namecoin.
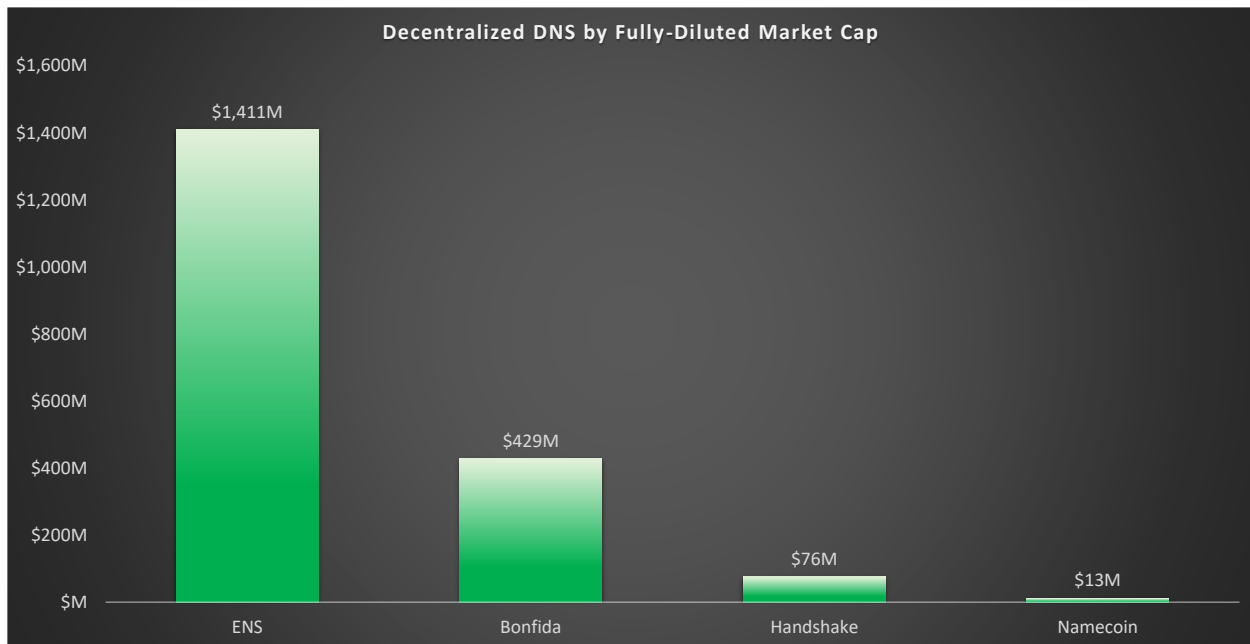
Source: Coinmarketcap as of 10.2.22

Protocol	FD Market Cap	Description
ENS	$1,411M	Ethereum Name Services provides .eth names for the Ethereum blockchain
UNSTOPPABLE DOMAINS	NA	Unstoppable Domains does not have a token, but it is one of the more popular players in the space and it provides customized, crypto-focused domain names such as .crypto and .zil
	$429M	Bonfida provides .sol domain names for the Solana ecosystem

_____

Bonfida		
handshake	$76M	Unlike many other competitors, Handshake provides a decentralized service for registering top-level domains (e.g .com or .org). Because it is not supported by iCann, users need a browser extension to use the service
namecoin	$13M	Launched in 2011, Namecoin is one of the earliest iterations of a decentralized DNS

_____

_____

Chapter 77: Decentralized Internet

How Does the Internet Work?

We discussed previously that information travels over the internet via wires (and sometimes via radio waves).

Map of all Internet Cables on Earth

Source: International Telecommunication Union (ITU)

These wires are owned by companies known as Internet Service Providers (ISPs) which are split into three levels, also known as "Tiers":

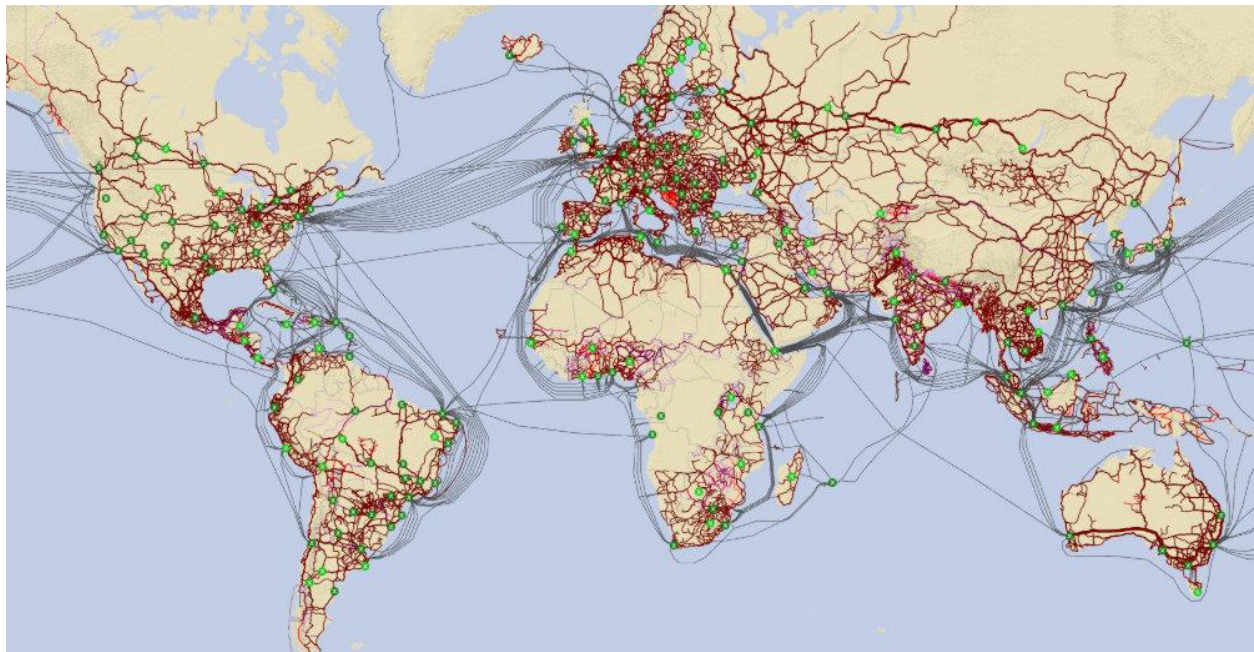- **Tier 1 - International:** Tier 1 internet providers form the "backbone" of the internet. They are responsible for maintaining the high-speed cables that cross continents and major oceans. These providers do not deal directly with end users, and instead charge national and regional networks for carriage. Notable Tier 1 ISPs include AT&T, Verizon, China Telecom, PCCW, Singtel, NTT, Telstra, British Telecom and Deutsche Telekom.
- **Tier 2 – National and Regional:** Tier 2 providers provide a bridge between the first and last mile. They pay Tier 1 networks for transit and sell transit to Tier 3 networks (and sometimes directly to large companies and governments). Major Tier 2 providers include Comcast, Virgin Media, Cox Communications and CTS Telecom
- **Tier 3 – Local:** Tier 3 providers are responsible for connecting homes and small businesses to the internet. As such, they are often known as the "last mile". The bulk of these connections run through the wires provided existing cable TV networks (although fiber optic service is growing)

As mentioned previously, the vast majority of global internet traffic is routed through a handful of Tier 1 providers. This presents several problems including: i) the ability to charge high premiums

_____

_____

and extract monopolistic profits, ii) the power to block or censor traffic and iii) vulnerability to failures and outages (e.g. the entire island of Tonga lost its internet connection for over five weeks due to a damaged undersea cable).

Decentralized ISPs, such as Helium, aim to fix this by allowing users to host their own internet access points.

How does a Decentralized Internet Work?

Helium is a decentralized wireless network powered by cryptocurrency. The company was founded in 2013 by Shawn Fanning of Napster, Amir Haleem, and Sean Carey, and is backed by a notable list of investors that includes Pantera Capital, Khosla Ventures and a16z.

Unlike traditional ISPs, transmission occurs over a global network of independently owned "hot spots" – small devices that can send data over long distances using radio frequencies. Owners can purchase these gadgets for around $500 and transmit the signal to nearby internet-enabled devices (this is similar to the Wi-Fi hotspot on your phone, but ~200x more powerful).

Helium has made significant progress to date and deployed nearly 1 million devices across 182 countries. This makes it the world's largest user-owned wireless network.

The Helium Network Hosts Nearly 1 Million Hotspots Across 182 Countries
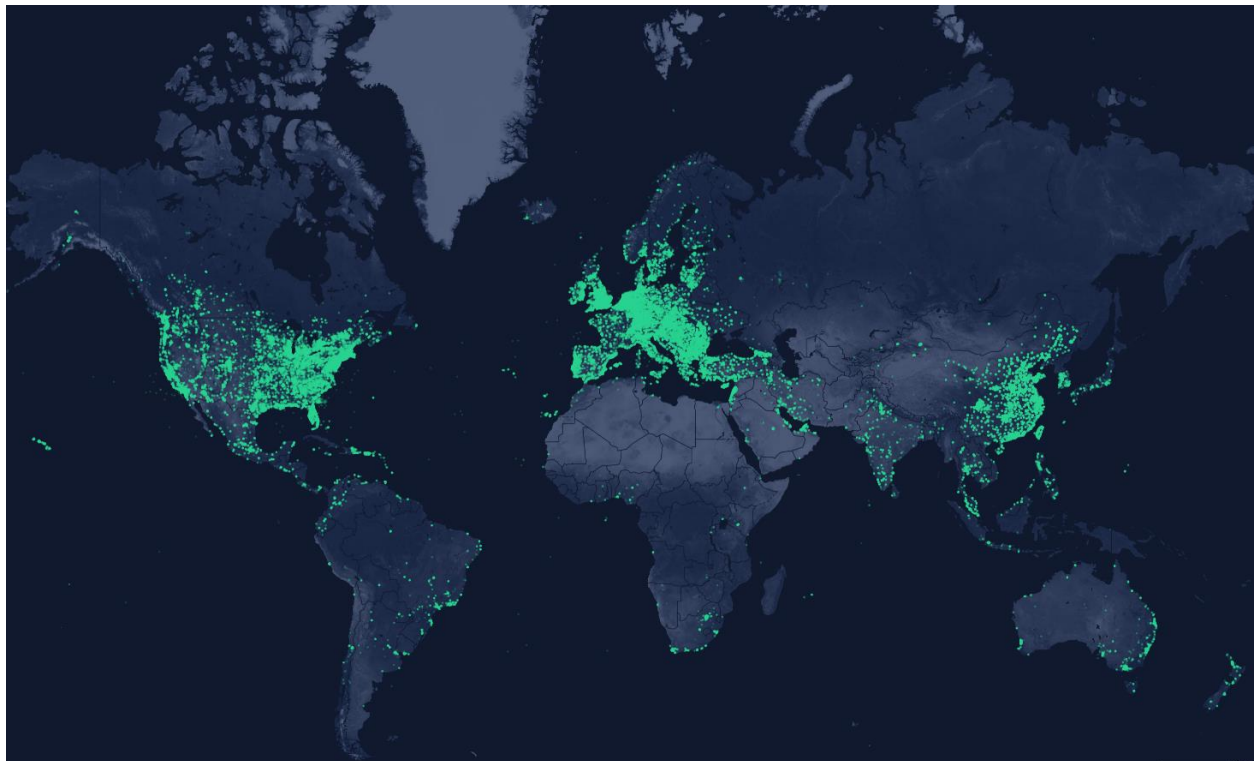
Source: Helium

Although many have tried to disrupt the existing network of ISPs, Helium is the only company to make headway on this endeavor.

_____

_____

This is largely due to its novel use of cryptocurrencies as an incentivization mechanism. In exchange for hosting hotspots, Helium providers are rewarded with the project's native coin, HNT. While earnings can vary greatly from user to user, some hosts have reported making upwards of $2,000 a month.

To ensure the stability of the network, the protocol uses a process known as "Proof-of-Coverage", which randomly pings hotspots to verify that they are in the correct location and actively transmitting a signal.

Helium, also known as "the People's Network", eliminates many of the traditional concerns of centralized ISPs and may help:

- **Lower Fees**: Transitioning from the current oligopoly of ISPs to a highly-competitive, decentralized network should significantly reduce prices in the long-run.
- **Eliminate Censorship**: Anyone can use the Helium network, it can't censor transactions and the network can't be shut down by a third party
- **Reduce Failures and Outages**: The use of multiple, overlapping hotspots reduces reliance on a single point and helps reduce the risk of outages

At the time of writing – October 2nd, 2022 – Helium's fully-diluted market cap is $1.1 billion.

_____

_____

Chapter 78: Node Providers

What is are Node Providers?

A "blockchain" is little more than a collection of computers – called "nodes" – that maintain an identical copy of a shared database. These nodes are responsible for hosting the blockchain, adding transactions and ensuring its security (and are often paid handsomely for this privilege).

Nodes are the only devices that can interact with a blockchain. That means if you want to use one, you must either:

- Set up and run your own node
- Connect to nodes provided by third-party services such as Alchemy or Infura

Most people lack the time, patience or technical knowledge to host their own node and, as such, the vast majority of users choose to use third-party providers (even as early as 2019, Infura was handling over 12 billion API requests per day).

Most Users Connect to Ethereum Network via a Third-Party Node Provider Such as Infura
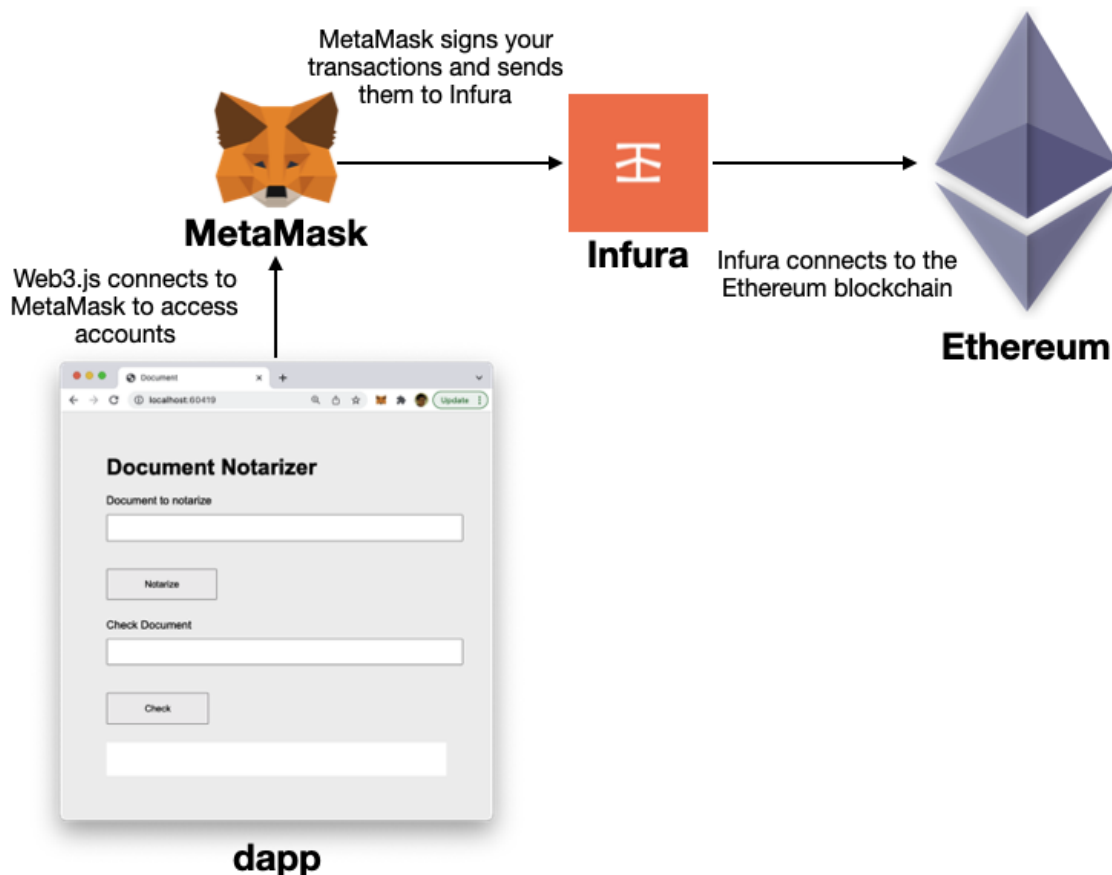
Source: Wei-Meng Lee via Medium

_____

_____

Unfortunately, most of these providers are centralized and, as such, are seen by many to be blockchain's dirty little secret.

For instance, Infura is owned and operated by ConsenSys (the in-house development studio of Ethereum) and hosted on cloud services owned by Amazon. This creates several problems including:

- **High Costs**: Infura's entrenched position gives it significant negotiating power and allows it to charge prices that are often above market
- **Frequent Outages**: Dependance on Infura represents a single point of failure for Ethereum and has resulted in several outages, including major ones in November 2020 and April 2022
- **Potential for Censorship**: In an attempt to block two separatist regions of the Ukraine in March 2022, Infura accidentally restricted access for users in Venezuela

Even Michael Wuehler, the co-founder of Infura admits that "If every single dapp in the world is pointed to Infura, and we decided to turn that off, then we could, and the dapps would stop working."

Fortunately, decentralized alternatives such as the Pocket Network are emerging to remove this chokepoint.

How do Decentralized Providers Work?

Founded in 2017 by Michael O'Rourke, the Pocket Network functions as a decentralized "marketplace" for nodes.

Instead of owning the nodes directly like Infura or Alchemy, the network simply connects users (Web3 applications that need to connect to public blockchains such as Ethereum, Solana or Polygon) with independent node providers (known as "Service Nodes" on the platform).

The Pocket Network is a Marketplace for Decentralized Nodes

Source: Eden Block

_____

_____
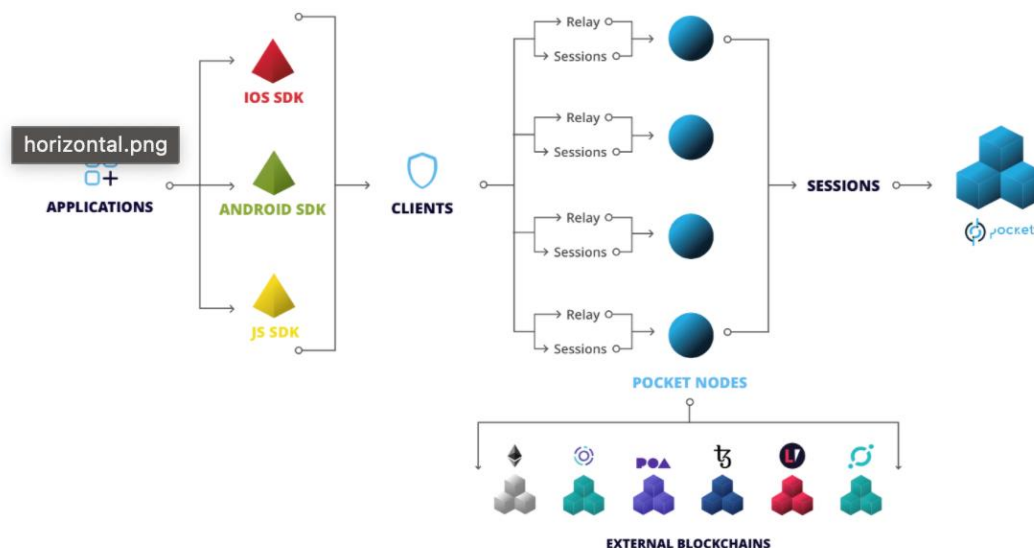
Pocket Network's marketplace is driven by the platform's native token, POKT. To use the service, both customers and Service Nodes must stake POKT as collateral. Once deposited:

- Users can make a request to the Pocket Network to connect to a blockchain
- Requests are routed through Pocket's software, which connects users to a random Service Node. These nodes are rotated out every hour, and the network immediately replaces any node that crashes or goes offline
- Service Nodes connect users to the blockchain of their choice and relay the appropriate data
- Another set of nodes, known as Validator Nodes, verify the legitimacy of the work performed by the Service Nodes
- If the transaction is legitimate, it is finalized, if not, the Service Node is heavily penalized and its collateral stake is slashed

Upon completion of the transaction, Pocket debits the payment from the user's staked collateral and sends 89% to the Service Node, 1% to the Validator Node and keeps 10% for itself (via its user-owned PocketDAO).

Using Pocket offers several benefits to Web3 applications. In addition to being decentralized, it is often up to 10x cheaper than traditional providers, highly resistant to outages and it offers multichain support to over 50 networks including Ethereum, Solana, Polygon, BSC, Avalanche and NEAR.

As a result, the network has grown considerably over the last few years – it currently hosts nearly 50K nodes over 30 countries and performs over 6 billion relays per week.

<u>Key Players</u>

While not an exhaustive list, key players in the node provider market include:

<u>Node Provider</u>	<u>Description</u>
	Infura is one of the largest node providers, serving over 400K developers at companies such as Uniswap, Brave, Compound, Metamaks, Open Zepplin, Gnosis
	Alchemy is another centralized player that boasts over 10+ million end users, $100B+ of transaction volume and counts Opensea, 0x, Aave, Meta, Adobe, Yearn, Maker, the Graph and dY/dX

_____

_____

QuickNode	Quicknode is a node provider that focuses on scalability and speed. The projects claims that it is faster than competitors in 65% of its locations
POKT	Pocket Network is a decentralized API marketplace connecting to over 50 blockchains
Ankr	Ankr is another decentralized node marketplace that supports almost 27 networks
Chainstack	Chainstack is a node provider that focuses on supporting larger businesses with its enterprise-grade software
BLOCKDAEMON	Blockdaemon is a node infrastructe provider that focuses on institutions such as banks, investment funds and governments

_____

_____

Chapter 79: Smart Contract Platforms (Layer 1s)

Smart contract platforms serve as the foundation of Web3. They are the computers that set the rules for the ecosystem and allow users to create, store and trade cryptocurrencies and digital assets such as NFTs. Every time that you make a trade on Uniswap, lend money on Aave, mint an NFT on Opensea or vote in a DAO you need to use (and pay) a Layer 1 such as Ethereum.

Keeping with the ethos of Web3, smart contract platforms are decentralized and distributed, meaning that they aren't controlled by any one party, they can never be shut down and anyone can use them at any time.

As of October 2022, the largest smart contract platforms by fully-diluted market capitalization are Ethereum, BNB Chain, Cardano, Solana and Avalanche.

Ethereum Leads the Market with over 49% Market Share
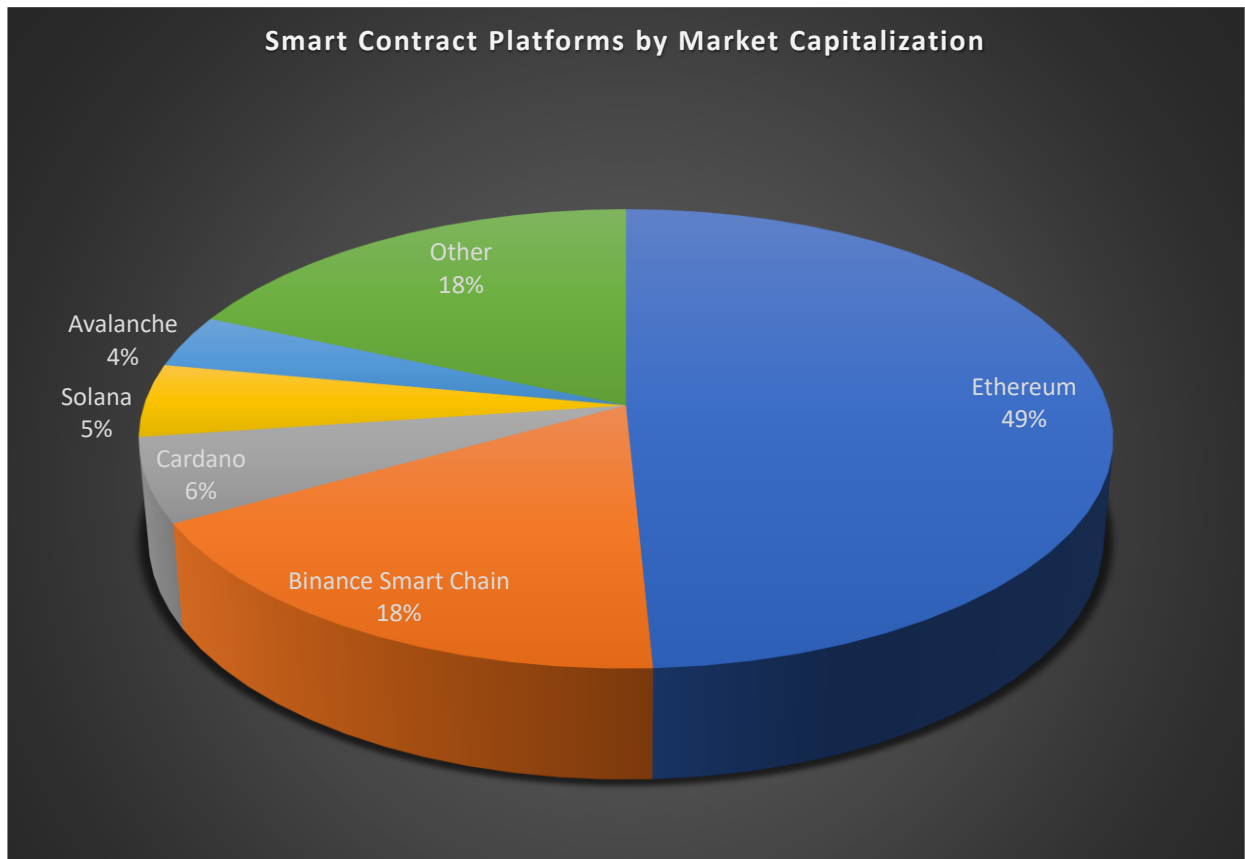
Source: Coinmarketcap as of 10.2.22

Protocol	Market Share	Description

_____

_____

	49%	Despite losing a third of its market share in 2021 due to high fees, Ethereum is still the undisputed king of Layer 1s. And with the upcoming release of Ethereum 2.0, it will likely continue to be the dominant force in the space
	18%	BNB Chain is the native smart contract platform of the crypto currency exchange Binance. Despite capturing a relatively large share, it's criticized for being highly centralized
	6%	Cardano is one of the original "third-generation" blockchains. Despite having limited traction, it has a strong fan base and consistently ranks in the top 5 in fully-diluted market capitalization
	5%	Solana is a single-chain protocol that boasts the fastest speeds (>50,000 TPS) and lowest fees (<$0.00025) of any major smart contract platform
	4%	Although its growth has recently slowed, Avalanche was one of the fastest growing chains in 2021 and it still retains a strong presence in DeFi

We've already covered smart contract platforms in detail in Part 3, so if you still have questions I'd highly recommend going back to review.

_____

_____

Chapter 80: Rollups (Layer 2s)

With the exception of Solana (which has its own challenges), most smart contract platforms are currently unable to handle the massive data and computational requirements that will be required for blockchain gaming, the metaverse and mass distribution of NFTs.

For instance, Ethereum can only handle around 25 transactions per second (vs. Visa's 1,700) and the average fee for using Ethereum is ~$10 (and that's the mean for *all* transactions – NFT transactions, which are generally much more complex, can often cost users several hundred dollars).

The most likely solution to these problems is the use of "Layer 2" networks – secondary protocols that are built on top of existing blockchains.

While there are many different types of Layer 2 solutions (which are discussed in much greater detail in Chapter 18), one flavor that is showing extraordinary promise is rollups.

Rollups temporarily remove data from the underlying blockchain, perform computations on that data and then insert the results back into the chain. This removes a ton of congestion from the network and results in faster processing times and lower fees.

Because rollups execute off-chain, they can't be fully trusted – after all, how do we know that the architects of the rollup aren't being malicious? As such, they need a way to prove to the main network that they're not being malicious. There are currently two different ways of doing this:

- **zk-rollups**: When returning data to the main chain, zk-rollups submit a cryptographically secure "validity proof" to the network, showing that all calculations are valid. The mechanics of this proof are out of the scope of this article, but for reference it is called a "zero-knowledge proof" because it can be used to prove something is true without relaying any additional data (that's where they get the name "zk")

- **Optimistic rollups**: Optimistic Rollups take the opposite approach. Instead of submitting a proof, it is assumed that the data is correct BUT users can easily check this through a "fraud proof", which means that there is a 7-14 day waiting period that allows validators to review and reverse the transaction if they suspect fraud

In general, zK rollups are faster but offer less functionality, while optimistic rollups have more functionality but are also slower due to the potential of fraud challenges.

As zK rollups mature and more functionality is added, many expect for them to become the dominant L2 solution for ETH.

In fact, Vitalik wrote: "In general, my own view is that in the short term, optimistic rollups are likely to win out for general-purpose EVM computation and ZK rollups are likely to win out for simple payments, exchange and other application-specific use cases, but in the medium to long term ZK rollups will win out in all use cases as ZK-SNARK technology improves."

_____

_____

Major optimistic rollup solutions include Optimism and Arbiritum and major zK- rollup projects include ZKSync, Loopring and Starkware.

<u>Arbitrum is the Largest Rollup Provider with 50% Market Share</u>
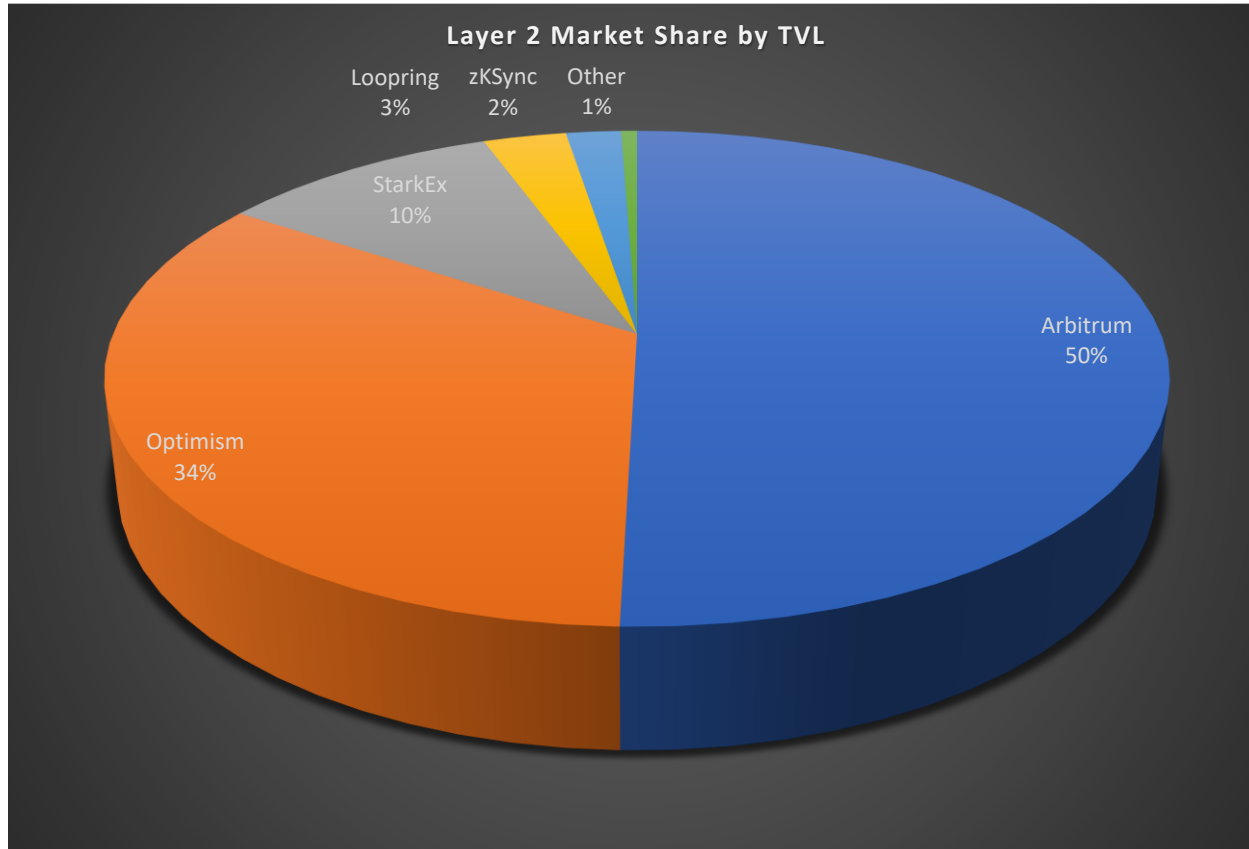
Source: <u>L2Beat</u> as of 10.2.22

Project	Market Share	Description
	50%	Arbitrum is the largest optimistic rollup and largest rollup protocol overall with over 50% market share and nearly $3B Total Value Locked in DeFi

_____

_____

Optimism logo	34%	Optimism is the second largest optimistic rollup protocol, hosting notable projects such as Metis Andromeda and Boba Network
STARKEx logo	10%	StarkEx is the largest ZK rollup provider hosting notable projects such as dYdX, ImmutableX, DeversiFi and Sorare
LOOPRING logo	3%	Loopring is a decentralized exchange that hosts its own zK rollup technology
zkSync logo	2%	zKsync is a zK rollup provider focused on SNARKs, a slightly different technology than StarkEx

_____

_____

Chapter 81: Data Storage

What is Data Storage?

Technically, blockchains *are* databases. But they aren't very good databases as they can only hold small amounts of information. For instance, a recent study estimated that it costs $40K to store 1MB on the Ethereum network – that's roughly 1/3rd of the size of the average photo taken by an iPhone!

As such, the images for most NFTs aren't actually stored on a blockchain, only a URL that *points* to these images is. The actual .jpeg (image) file is stored on a third-party database.

To reduce concerns of centralization, we are now seeing the development of decentralized databases, which aim to preserve the integrity of NFTs by using the same underlying technology to split, encrypt and store data across multiple locations. This offers several benefits, including:

- **No Censorship**: There's no centralized third party that can remove your data or tell you what you can and can't store
- **No Single Point of Failure:** Because identical copies of your information is scattered and stored across multiple nodes, there is little chance of outages, data loss or distributed denial of service attacks ("DDoS" where malicious actors use bots to overload a site with traffic)
- **Lower Costs:** Decentralized storage may ultimately turn out to be much cheaper and more efficient than our current "cloud" infrastructure

Two of the largest decentralized storage services are IFPS and Arweave.

How Does Decentralized Storage Work?:

To understand how decentralized storage works, let's look at the largest player in the space – Filecoin.

Launched in 2017 by Stanford Computer Scientist Juan Benet and backed by Sequoia, Union Square Ventures and Digital Currency Group, Filecoin is a decentralized data storage network.

The protocol allows users to store data – such as NFTs, audio and video content, metaverse and gaming assets and even Web 2.0 data sets – on its IFPS network. IFPS is a global, peer-to-peer marketplace that relies on an independent network of miners to provide unused space on their hard drive to customers in need of storage.

To maintain the system, the project relies on an independent network of three different types of miners:

- **Storage Miners:** Storage Miners lend their unused hard drive space to store customer data. In return, they are paid in Filecoin's native token, FIL. To ensure security, the platform breaks down customer data into fragments and stores them across the network

_____

_____

- **Retrieval Miners**: Customers pay Retrieval Miners a fee in FIL to fetch their data for them (to be implemented)
- **Repair Miners:** Repair Miners are responsible for the maintenance and health of the network (to be implemented)

<u>Overview of the Filecoin Ecosystem</u>
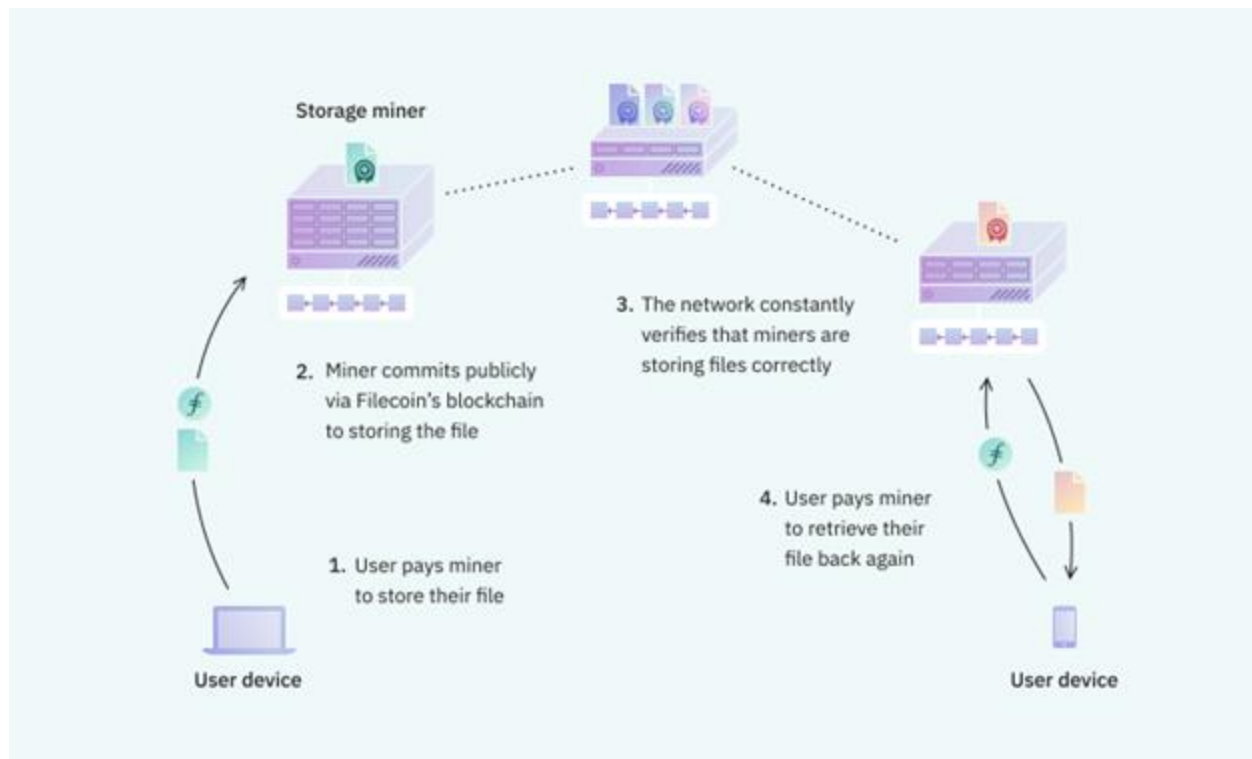
Source: <u>Filecoin</u>

In order to ensure that miners upload and continuously store data, Filecoin uses cryptoeconomic incentives. Miners are required to provide collateral in FIL and periodically asked to provide two types of cryptographic proofs:

- **Proof of Replication:** To ensure that storage providers have uploaded the correct data, the network requires miners to provide a zero-knowledge proof that demonstrates that they have received the data and are indeed hosting it on their computers
- **Proof of Spacetime:** To ensure that miners *continue* to store that data (and not delete it), the network will periodically require miners to verify a *random* piece of data

If a miner fails to pass either of these tests, they will lose their collateral.

The protocol had a strong year in 2021, and according to their <u>website</u>, experienced significant growth across several key metrics during the period of January 1st, 2021 to January 1st, 2022. In particular:

- Storage Miners: Grew from 856 to 3,600+ (321%)
- Network Capacity: Expanded from 1.69 EiB to 14+ EiB (8x)

_____

_____

- Unique Clients: Increased from 584 to 703 (20%)
- Storage Deals: Grew from 699K to 1M+ s (43%)
- Total Data Stored: Expanded from 1.578 PiB to 25+ PiB (15x)

Filecoin is trusted by numerous Web3 projects – including OpenSea, Magic Eden, Polygon, Solana, Metaverse AI and Audius – and it generated over $1.4B in revenue in 2021. (*Note: Filecoin's revenue has declined substantially in 2022 due to a decrease in fees*)

Who are the Key Players?

In addition to Filecoin, other notable players in the space include Arweave, BitTorrent, Storj and Siacoin.
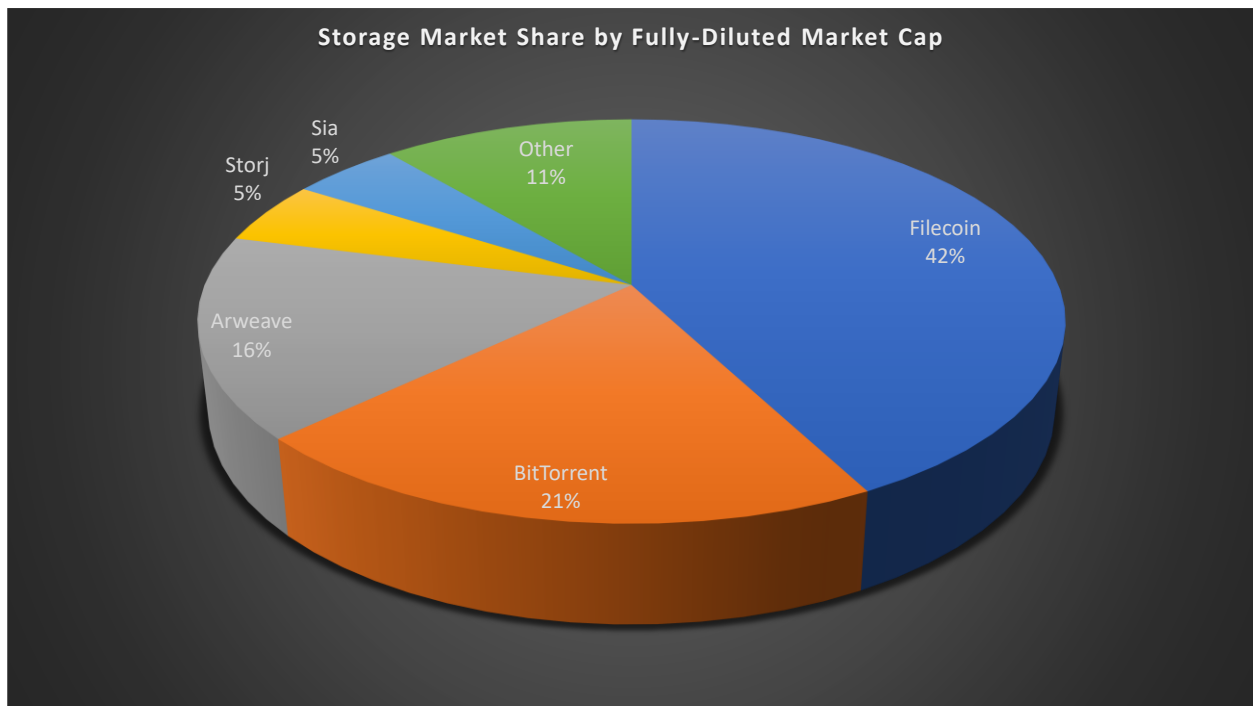
Source: Coinmarketcap as of 10.2.22

Project	Market Share	Description
Filecoin	42%	Filecoin is the largest and most used pay-as-you-go storage provider
BitTorrent	21%	BitTorrent is a decentralized storage provider hosted on the Tron Network

_____

_____

	16%	Arweave is the largest and most used permanent storage provider
	5%	Storj is another pay-as-you-go provider. Proponents say it has a better encryption process but critics say it's not decentralized enough
	5%	Siacoin provides pay-as-you-go storage, and while many consider it to be more technically advanced and feature rich, it has not achieved Filecoin's traction

_____

Chapter 82: Querying Tools

What is Data Aggregation?

Like a blockchain-based version of Google, data aggregators use a process called indexing to make it easy for developers and users to quickly search a blockchain for important data.

Indexing is method of organizing information to make data easier to find. As the name implies, it's very similar to the index at the end of a book – instead of going through every page in a book, the index allows us to quickly scan an alphabetical list to find the page number of the information we need.

Google became a multi-trillion-dollar company by mastering the art of indexing, and when it comes to blockchains, the process may be just as important.

Unfortunately, there are two main problems with current indexing strategies:

- It can be very time consuming and redundant for blockchains to do it themselves
- Many existing aggregators are centralized

So how do we solve this problem in a decentralized manner? One possible solution comes through a protocol called The Graph.

How do Data Aggregators Work?

While the project is sometimes called the "Google for blockchains", a better way to think about The Graph is as a decentralized network of thousands of Googles. Created by Yaniv Tal the project is an open-source, fully-decentralized indexing protocol for blockchain data.

There are several key players in The Graph's ecosystem:

- **Consumers:** The end-users of The Graph that initiate search requests and pay fees to the Indexers
- **Indexers:** These are the "workhorses" of the network that provide indexing services in exchange for a fee. Indexers are independent providers that operate in a decentralized marketplace known as the Query Market. To incentivize proper behavior, indexers must stake GRT (The Graph's native token) tokens as collateral.
- **Delegators:** Loan GRT to indexers to stake and receive a portion of the profits

_____

_____
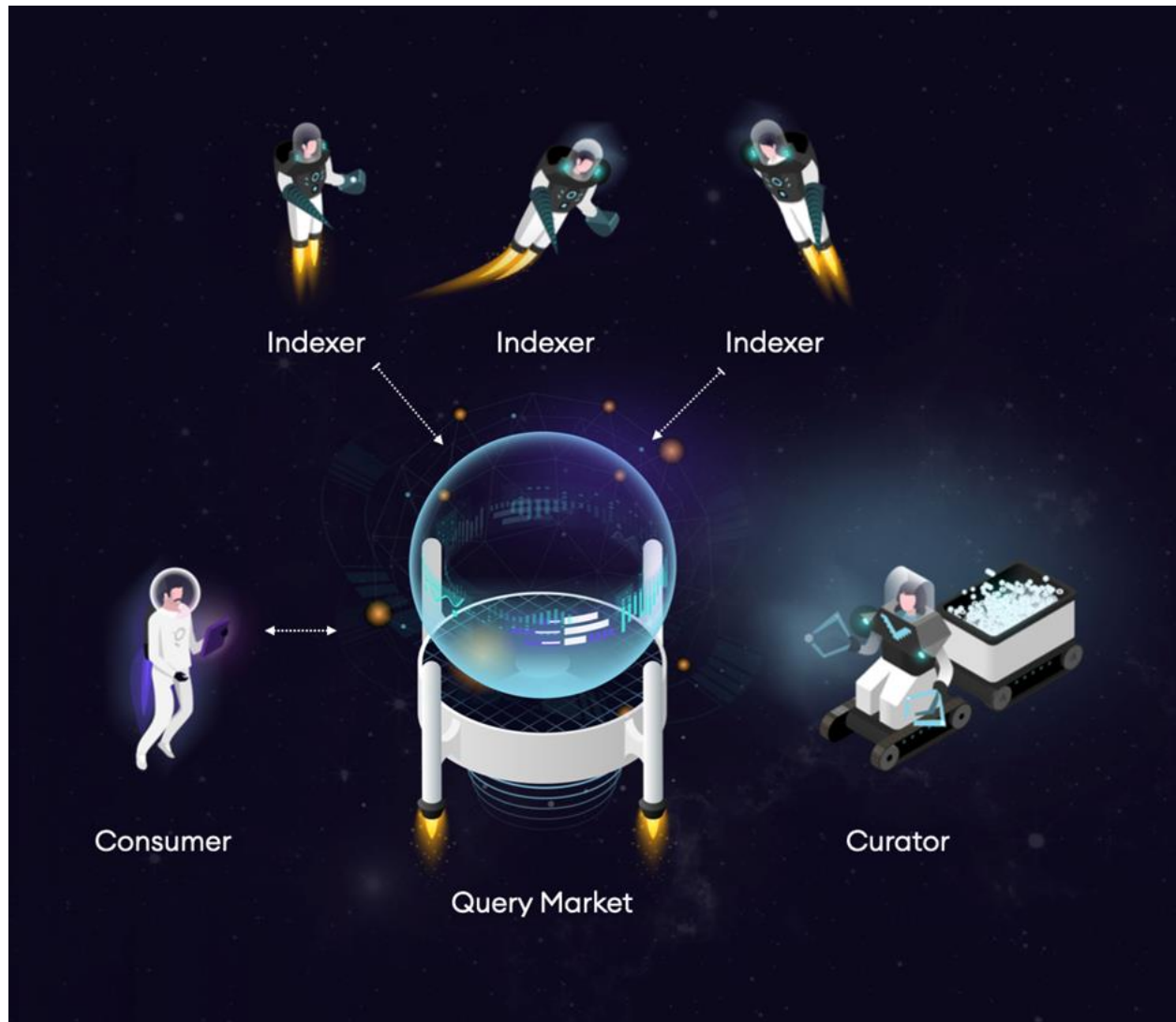
Source: The Graph

In addition to the above, the network also hosts curators, who find promising networks to index and fisherman and arbitrators, which serve as a form of quality control.

At the time of writing – October 2nd, 2022 – The Graph's fully-diluted market cap is $1 billion.

Who are the Key Players in the Data Aggregation Market?

While The Graph currently dominates decentralized data aggregation, its biggest competition still comes from centralized providers such as Scout, BigChainDB, Dune Analytics and Google's BigQuery.

_____

Chapter 83: Oracles

What are Oracles?

Blockchains have a major limitation – they are unable to access data from external systems. This is by design, like a computer without an internet connection, they maintain their isolation to guarantee security and streamline efficiency.

Unfortunately, the vast majority of potential use cases for smart contracts require a connection to the outside world. Exchanges need accurate price information, insurance needs data to make decisions on policy payouts and many apps require market information to determine settlements.

The solution to this problem is known as an oracle, a separate piece of infrastructure that bridges a blockchain to real-world data. Oracles can source a variety of information including, price reports, weather, sporting scores, results of elections, geodata, random numbers, etc…

Oracles became very popular in 2020 and were among the best performing assets in crypto that year.

Oracles were some of the Best Performing Assets in 2020

($ in millions)

Asset		Ticker	FD Market Cap	Circ Market Cap	30 Day %	YTD %
Chainlink		LINK	$9,620	$3,680	81%	452%
Band Protocol		BAND	$747	$153	535%	3296%
Nest Protocol		NEST	$603	$97	130%	N/A
DIA		DIA	$180	$6	N/A	N/A
DOS Network		DOS	$170	$22	323%	4125%
Zap		ZAP	$29	$14	1272%	3229%
Tellor		TRB	$27	$26	171%	400%
Total			**$11,376**	**$3,997**		

As of Aug. 6, 2020

Source: Messari

The main challenge with designing oracles, however, is that if any oracle is compromised, the entire system is compromised. As such, we need to leverage a decentralized oracle network to guarantee security.

How do Oracles Work?

To understand how oracles function, let's take a look at Chainlink, a decentralized blockchain oracle network built on Ethereum.

_____

The project was founded by Sergey Nazarov in 2014 and launched an ICO in 2017 to raise $32M. The project has a very strong management team and recently onboarded Eric Schmidt as an advisor.

Oracles Allow Blockchains to Access External Data
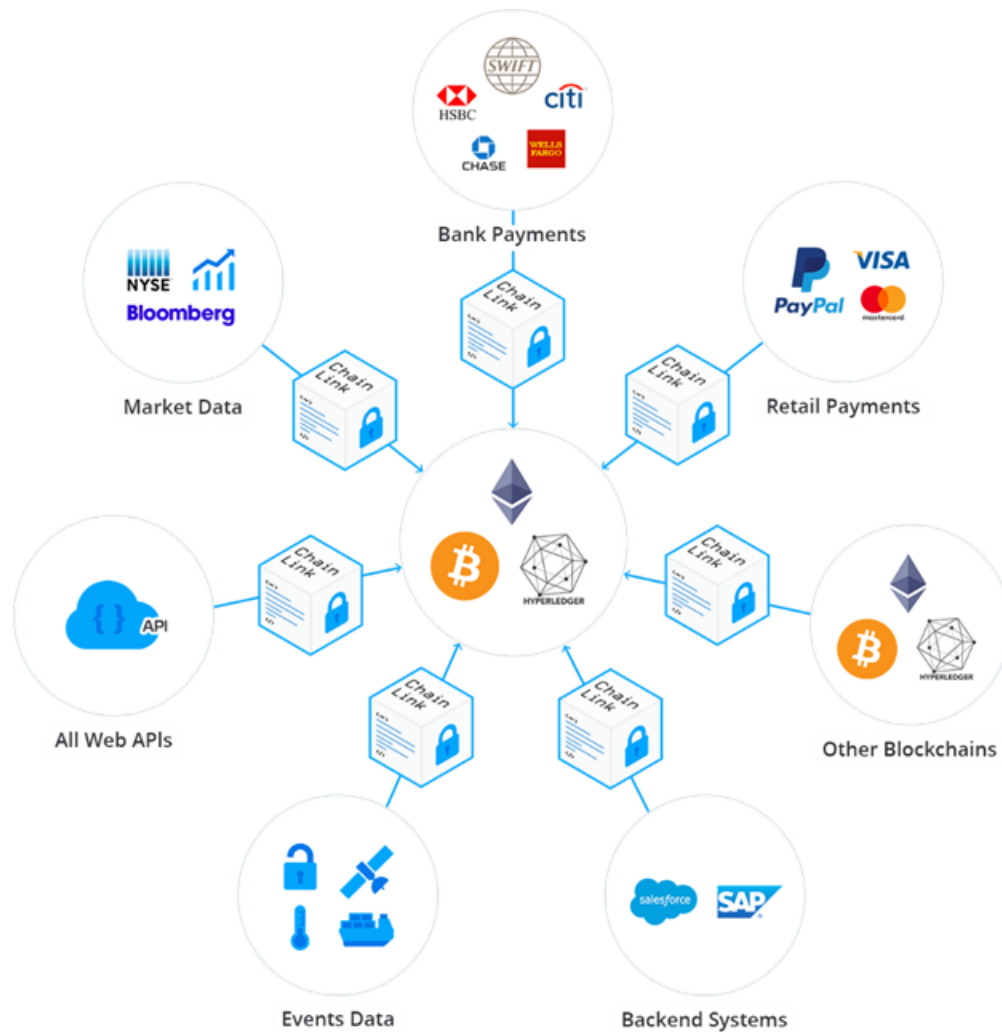
Source: Chainlink

As a decentralized oracle network, Chainlink relies on hundreds of independent oracles to provide relevant data.

As an example, let's say that Sushiswap wants to show the price of Ethereum on its site. They would:

1. Create a request for data from the Chainlink network to obtain the price of ETH
2. Submit this request along with payment in the form of Chainlink's native token, LINK
3. Chainlink will then automatically select the best oracles based on 1) their reputation and 2) their ability to find the necessary data

_____

_____

4. Oracles will find the requested data (e.g. the price of ETH) and send it back to Chainlink. Oracles must stake LINK tokens as collateral to ensure proper behavior
5. Chainlink will aggregate the results, choose the most accurate answers and discard outliers. Oracles that are deemed to be negligent and / or malicious may face penalties and lose some or all of their collateral
6. The information is routed through Chainlink to the Sushiswap
7. Sushiswap can then populate their site with the current price of ETH

Chainlink has achieved strong traction since launching and currently dominates the oracle space with nearly 1,500 partners. For comparison, the next largest network has fewer than 200.

Who are the Key Players in the Oracle Market?

Chainlink dominates the oracles space with 68% market share.

Market Share by Number of Oracles

Other 20%

Band 4%

Berry 8%
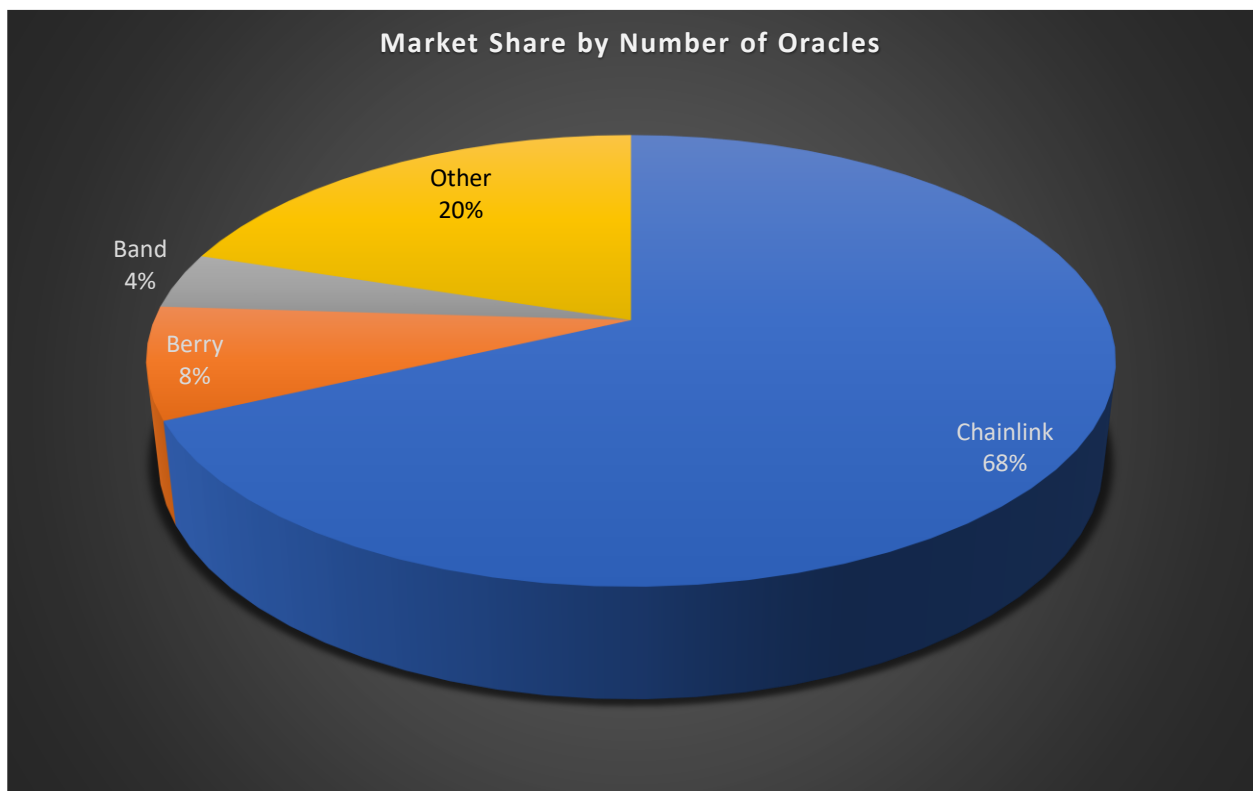
Chainlink 68%

Source: Coin98Analytics as of 7.2.22.

_____

_____

Other notable players include Berry and Band Protocol.

Project	Market Share	Description
Chainlink	68%	Chainlink is the undisputed leader in the oracle market with 68% share
BERRY	8%	Berry is an oracle network designed for BNB Chain, created because Chainlink was originally focused on Ethereum
Band Protocol	4%	Band is a direct competitor to Chainlink that claims to have lower fees. Critics argue that this comes at the expense of security

_____

_____

Chapter 84: Bridges

What are Interoperability Protocols?

While Ethereum remains the dominant chain in DeFi, its share has declined from over 90% to approximately 60% due to the emergence of several "alternative L1s" such as Solana, Binance Smart Chain and Avalanche.

<u>Multiple Players are Entering the Smart Contract Space</u>
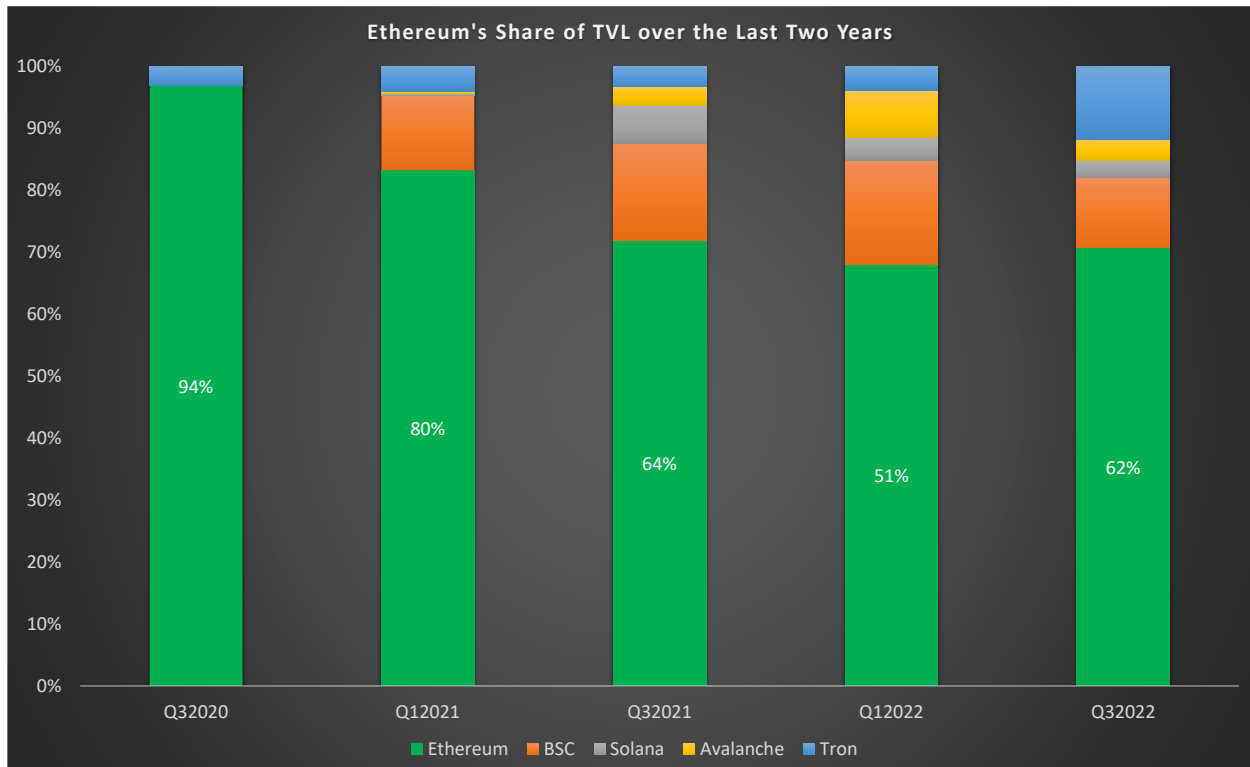
Source: Defillama as of 10.2.22

While arguably good for the long-term health of the ecosystem, this explosion of smart contract platforms has created significant short-term problems. Perhaps most pressing is the problem of interoperability.

Because blockchains have different protocols, they cannot communicate with each other. While this independence has many benefits, it also creates significant challenges for users that want to move tokens and / or data between chains.

Interoperability protocols are systems designed to solve this problem by allowing the transfer of information and assets between two or more blockchains.

_____

How Do Interoperability Protocols Work?

There are four main types of interoperability solutions:

- **Atomic Swaps**: Atomic swaps allow two parties to directly trade tokens from different blockchains via a virtual escrow account
- **Wrapped Assets**: Wrapped assets are a synthetic version of one blockchain's token designed for use on another blockchain. For example, wrapped Bitcoin is an Ethereum token that represents Bitcoin on the Ethereum blockchain
- **Cross-Chain Bridges**: Cross-Chain bridges transfer tokens directly from one blockchain to another
- **Cross-Chain Swaps**: Like an interoperable version of Uniswap, cross-chain swaps use liquidity pools to trade assets between different blockchains

To understand these solutions better, let's look at some of the most popular interoperability protocols:

What are Atomic Swaps?

Atomic swaps were one of the earliest interoperability solutions.

These swaps use smart contracts to allow two parties to directly trade tokens from different blockchains without using a centralized intermediary.

To perform an atomic swap, each user locks their tokens up in a virtual safe known as a Hashed Timelock Contract (HTLC), and when both tokens have been received the trade is executed. The HTLC is also time-based, meaning that both parties must satisfy their end of the deal within a predefined time frame.

While the direct nature of atomic swaps ensures that they are decentralized, they are extremely inefficient as potential users need to find a willing counterparty for every trade.

What are Wrapped Assets?

A wrapped token is simply a synthetic version of a token designed for use on another network. Wrapped Bitcoin (wBTC), for example, is pegged to the price of Bitcoin but designed to work on the Ethereum network.

The process of wrapping uses a "lock and mint" system. When a user transfers assets from Blockchain A to Blockchain B, those assets are "locked" on Blockchain A via a smart contract. Once locked, identical copies of these tokens are "minted" (i.e. created) on Blockchain B. If the user wants to get her original tokens back, then the copies on Blockchain B are destroyed and she can resume using the tokens on Blockchain A.

_____

Steps in the working of a wrapped token
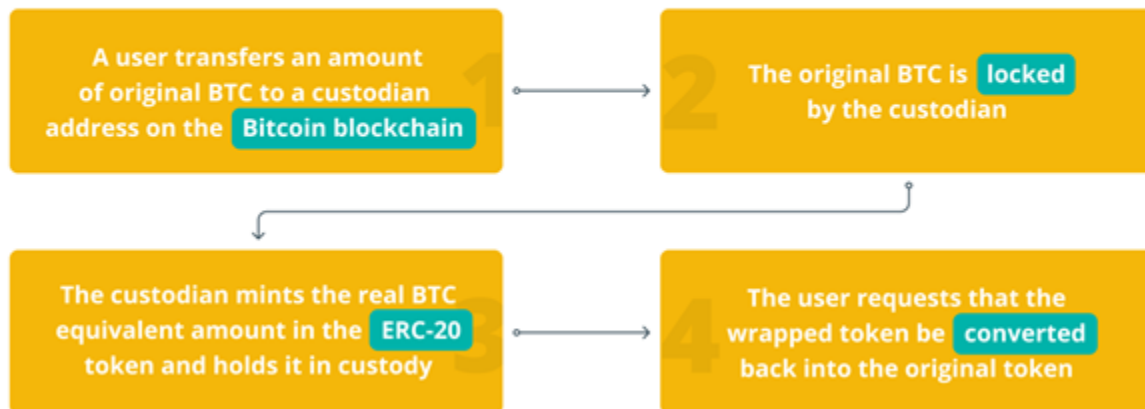
Source: Cointelegraph

Unfortunately, many existing wrapping services require a third-party custodian to orchestrate the "lock and mint" system and, as such, are centralized.

One project trying to fix this is Ren Protocol, which is attempting to create a decentralized wrapping service by relying on a network of 10,000 nodes to provide storage space and custody user assets.

What are Chain Specific Bridges?

Chain-specific bridges are dedicated bridges that operate directly between two blockchains. For example, Polygon's PoS bridge allows users to transfer assets from Ethereum to Polygon and vice versa.

Like wrapped assets, the PoS bridge uses a "lock and mint" system. When you deposit funds into a bridge, they are locked on Ethereum and copies are created on Polygon.

Most major blockchains have chain specific bridges, with Polygon, Arbitrum and Optimism being the most popular bridges for Ethereum.

_____

_____

Most Popular Bridges from Ethereum
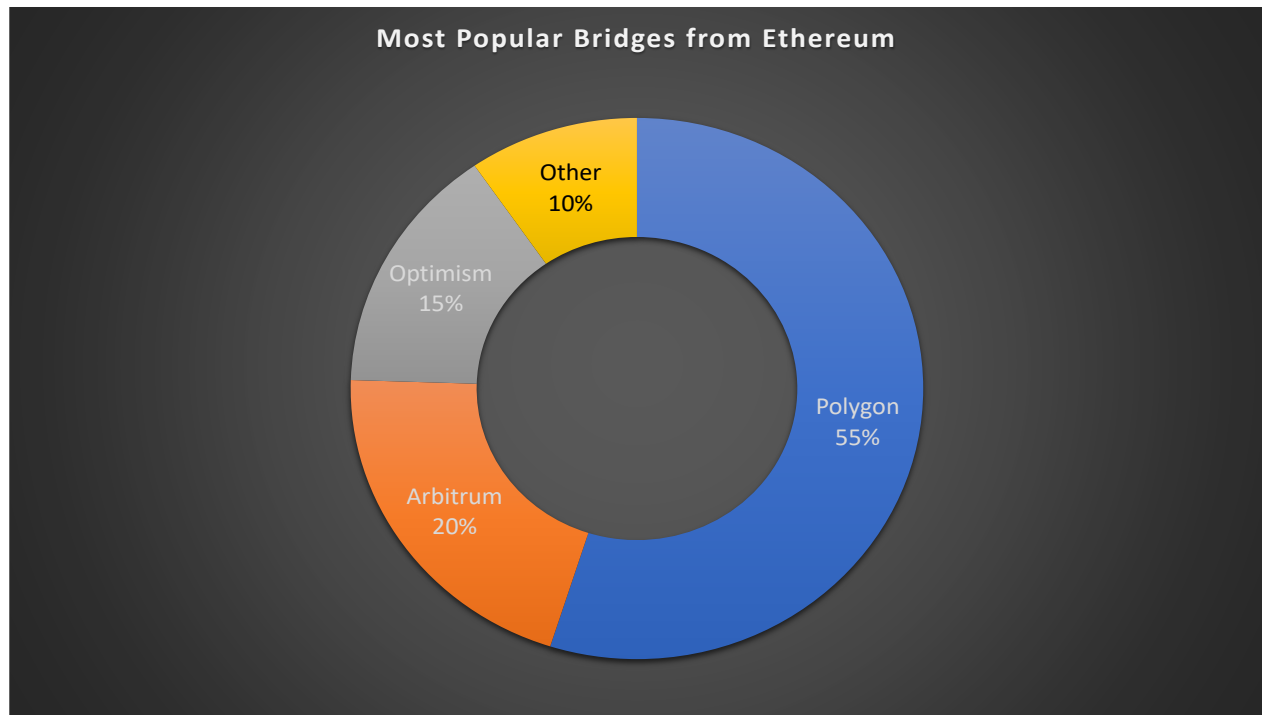
Source: Dune Analytics as of 10.2.22

The main drawback to chain specific bridges is that they are generally limited to the two chains in question, making them difficult to scale.

What are Cross-Chain Swaps?

Much like an interoperable Uniswap, cross-chain swaps use a series of liquidity pools to trade native assets between different blockchains.

One prominent example of such a protocol is Thorchain. Thorchain's pools are composed of three assets – the tokens that a user wants to trade and RUNE, the network's native token.

So if a user wanted to swap Bitcoin for Ethereum, the trade would first go through a Bitcoin-RUNE pool, and then a RUNE-Ethereum pool.

Source: Finematics

_____

_____
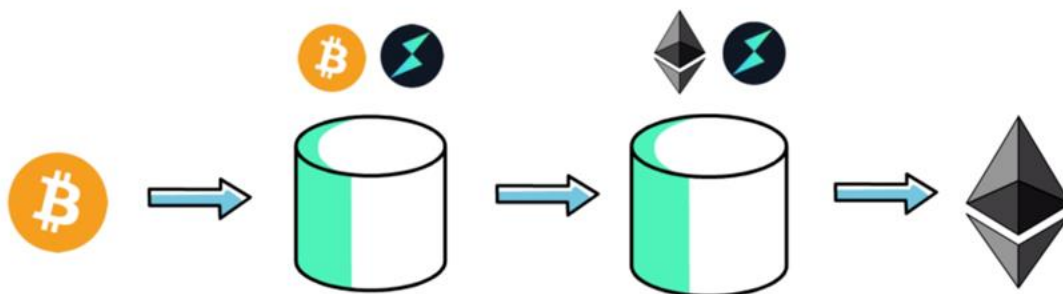
There are a few downsides to this method, however:

- Swaps can take a long time because they effectively require three transactions: Asset A to the A-Rune liquidity pool, the A-Rune liquidity pool to the B-Rune liquidity pool and the B-Rune liquidity pool to asset B
- Unlike Uniswap, where swaps can be bundled into large transactions, trades on Thorchain lack composability

Who are the Key Players in the Interoperability Solutions Market?

Wrapped Bitcoin, Just Cryptos and Multichain are the most popular bridges today, representing over 80% of the total value locked in interoperability solutions.

Market Share of Bridges by TVL

Label	Value
wBTC	44%
JustCryptos	21%
Multichain	16%
Other	8%
Portal	4%
PolyNetwork	3%
Orbit Bridge	2%
hBTC	2%

Source: Defi Llama as of 10.2.22

_____

_____
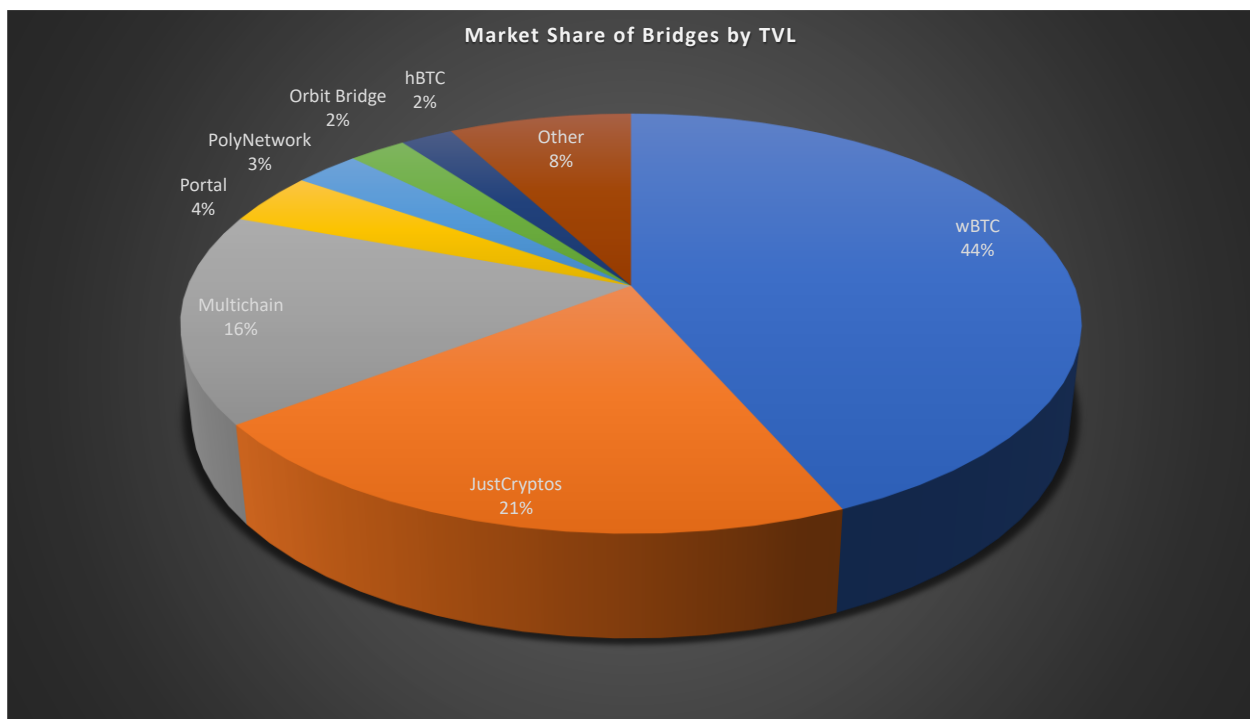
Project	Market Share	Description
	44%	Wrapped Bitcoin (wBTC) is a wrapped asset that is pegged to the price of Bitcoin but designed to work on the Ethereum network
	21%	Just Cryptos is a bridge supporting the Tron network
	16%	Formerly known as Anyswap, Multichain is a cross chain swap that leverages liquidity pools
	4%	Portal is a rebranding of Wormhole, Solana's bridge to Ethereum. It recently made headlines for suffering a $300M+ hack
	3%	Poly is a cross-chain bridge that has integrated with over 20 blockchains. The project made headlines for being the victim of a $600M hack in 2021 (the largest hack ever recorded at the time)
	2%	Orbit bridge supports 16 blockchains such as Ethereum, BNB, Polygon, and Avalanche
	2%	hBTC is a wrapped version of Bticoin that is custodied by the Huobi exchange

_____

_____

What is the Future of Interoperability Solutions?

Interoperability remains an unsolved problem – the market is nascent and there are numerous technical challenges (perhaps the most insidious is security, as nearly $2 billion in funds were stolen from bridges in the first half of 2022). While there are several potential solutions, all have tradeoffs and none have achieved escape velocity.

Given the likelihood of a multi-chain future, however, this is an area to keep a close eye on. In the coming months, it is likely that we will see an influx of new players and will also see existing solutions continue to evolve.

Many would argue that this is one of the holy grails of the space, as a protocol that can efficiently solve this problem will likely garner a 12-figure enterprise value.

_____

_____

Chapter 85: Decentralized Computers

What are Decentralized Computers?

Web3 may represent the biggest computing challenge in history.

Over the next decade, we will likely see the online world expand in both breadth (connecting to billions of IoT devices) and depth (as we begin to realize the vision of the metaverse – a collection of VR-powered virtual worlds).

As such, vast amounts of processing power will be required to create entire digital economies composed of game engines, simulated environments, video streaming, spatial computing, holographic displays and virtual and augmented reality experiences.

Fortunately, blockchains offer a potential solution to this problem through a concept known as decentralized (or "shared") computing. Shared computing lets individuals lend the unused computing resources on their personal devices (e.g. processing power, storage space, network bandwidth) to those who need it in exchange for compensation through cryptocurrencies.

Shared computing offers several benefits including:

- **More Processing Power:** By relying on a global network of computers, shared computing platforms hope to aggregate more processing power than any single entity could on its own

- **Faster Speeds**: Preliminary tests have shown that distributed computing networks are 20% faster than centralized ones, and this number may continue to grow as networks scale

- **Lower Costs**: Because distributed computing models can aggregate from a variety of sources, they are often significantly cheaper than centralized suppliers. According to Jules Urbach, the CEO of Render, "when you have really cheap GPU power and you want to render something 5,000 times—and the cost is 1/100th what it was before—that becomes tractable."

- **More Security:** Because identical copies of your information is scattered and stored across multiple nodes, there is little chance of outages or data loss.

- **Passive Income**: Processors can lend their unused computing power to earn passive income

Avivah Lithan, a vice president at Gartner Research believes that shared computing represents "blockchain at its best — peer-to-peer networks where underutilized servers are traded" and compares it to a "Uber" for computers.

One of the interesting projects leveraging this model is known as Render Technologies.

_____

_____

How does Shared Compute Work?

Founded in 2016 by Jules Urbach, Render is building a shared computing network that helps "render" visual effects and 3D graphics.

Rendering is the process used by computers to create 3D visual displays with texture and detail. This process is extremely difficult and computationally intensive, and often requires hours to render a single object or frame. For example, according to Pixar's Peter Collingridge:

> "Pixar has a huge "render farm," which is basically a supercomputer composed of 2,000 machines, and 24,000 cores. This makes it **one of the 25 largest supercomputers in the world**. That said, with all that computing power, **it still took two years to render Monster's University**."

The Render System Flow
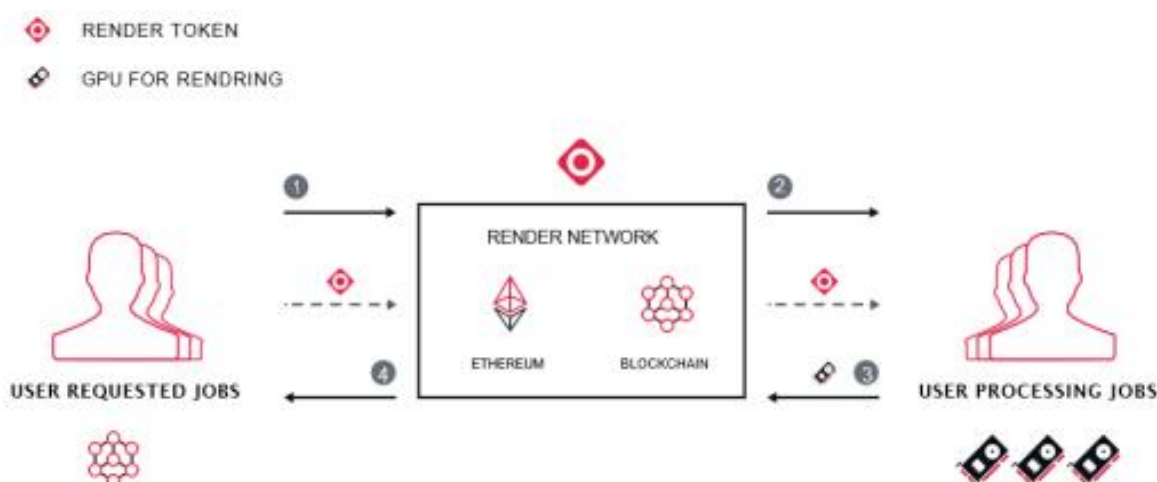
Source: RNDR user manual

Render operates as an automated marketplace –a sort of "AirBnB" for computing power – where:

- Users who want to lend their unused computing power sign up for the network as "Node Operators" and install the required software
- Content creators submit their job requests along with payment in the platform's native token, RNDR
- The Render network automatically assigns these jobs to the appropriate Node, matching the Creator's need with the Node's capabilities
- Node operators run Render's "OctaneRender" protocol to complete the work
- Once complete, the escrow is released and Nodes receive compensation in RNDR

The network can be used to create several digital assets including videos, NFTs, high-resolution images, metaverse assets and 3D animations.

At the time of writing, Render's market cap is roughly $242 million.

_____

_____

<u>Who are the Key Players offering Shared Compute?</u>
Shared computing has made significant progress in the last year. In addition to RNDR, other notable projects include LivePeer, Akash and Golem.
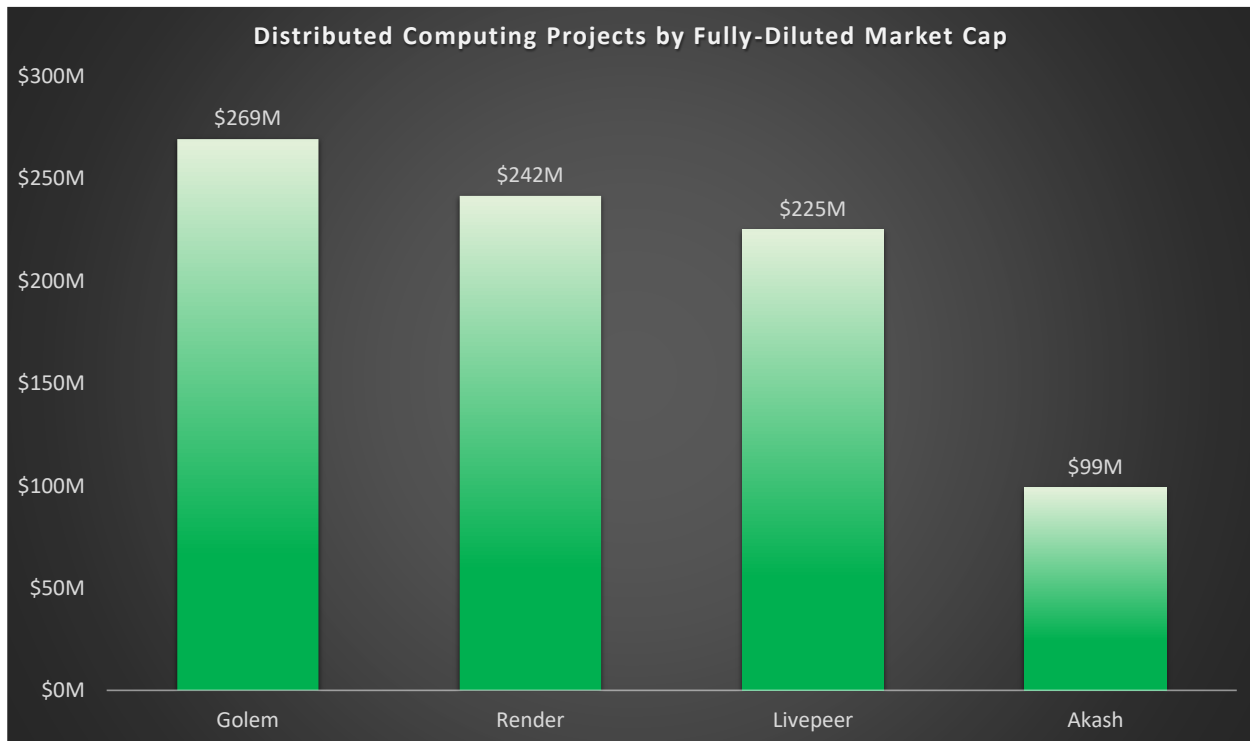
Source: Coinmarketcap as of 10.2.22. Note: Excludes Layer 1s, shared storage and networking.

Project	FD Market Cap	Description
golem	$269M	Golem provides processing power for AI machine learning, scientific testing and rendering
rndr	$242M	Render provides distributed rendering services
livepeer	$225M	Distributed platform that focuses on transcoding live and on-demand video
akash	$99M	Akash provides decentralized cloud computing, relying on unused capacity from existing data centers

_____

Part 8: Challenges Facing Web3

Chapter 86: What are the Problems with Web3?

While the potential of Web3 is immense, the space also has its share of challenges. Among the most notable of these are:

- High fees
- Limited traction
- Volatility
- Environmental concerns
- Limited interoperability
- Miner-Extractable Value (MEV)
- Poor user experience
- Usage by criminals and terrorists
- Hacks and scams
- Lack of legal and regulatory clarity

Let's take a deeper look into each of these concerns...

Chapter 87: High Fees

"Gas" refers to the fee required to execute a transaction on the Ethereum network. Whether you want to transfer a token, vote in a DAO, loan your assets on Ethereum or mint an NFT, you must pay gas to incentive the miners to approve your transaction and include it on the blockchain.

Because space on the Ethereum network is limited – it can only execute around 25 transactions per second – priority is determined by an auction process. This means that gas can get very expensive when the network is busy.

Unfortunately, network usage has grown significantly over the last few years, which has caused fees to spike.   For much of the first half of 2022, average fees exceeded $30. While we are in a bit of a lull at the time of writing, the 200-Day Moving Average transaction fee remains close to $10.00, a substantial increase from the $0.18 recorded three years prior.
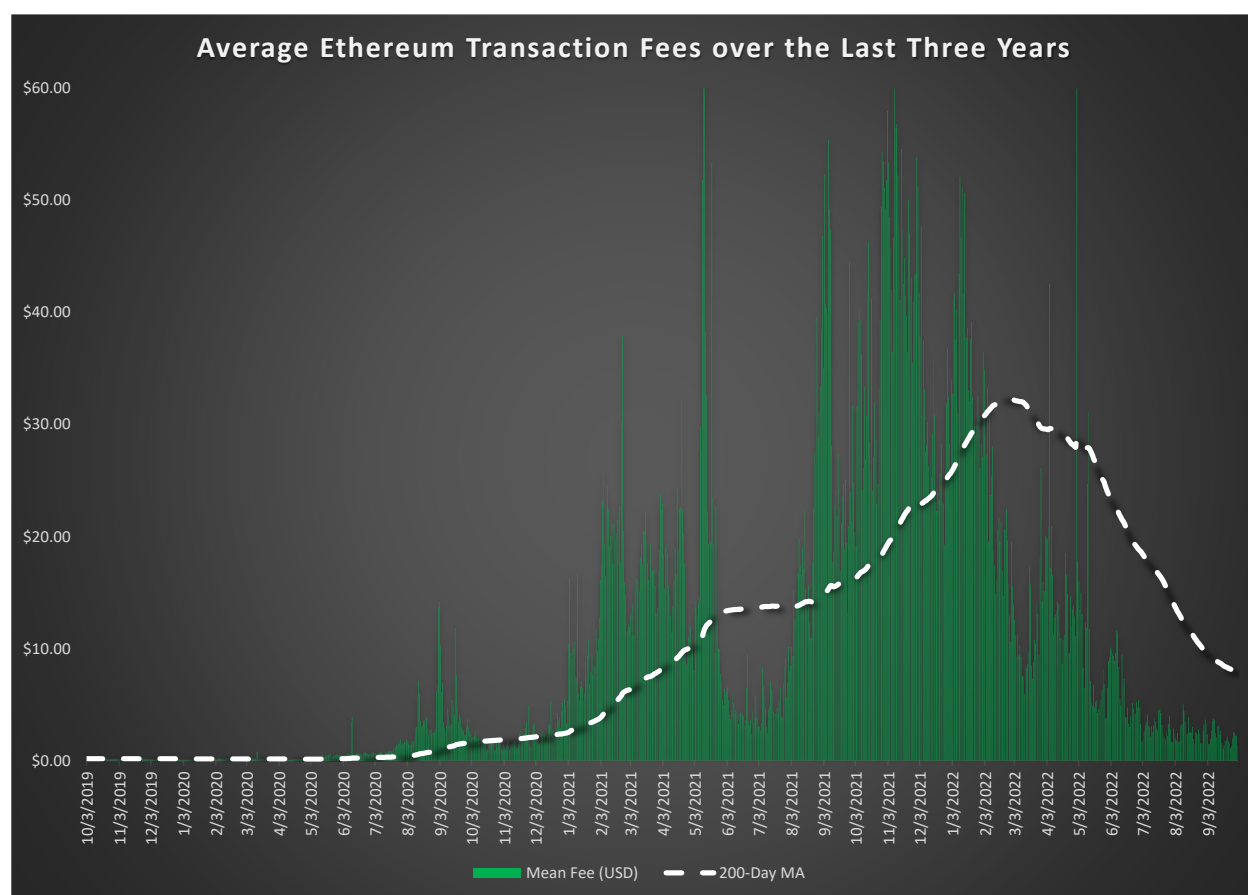
Source: Coinmetrics as of 10.2.22

Keep in mind these are average fees for *all* transactions, including simple ones like a token transfer. As some transactions – such as minting an NFT or borrowing / lending ETH – are generally much more complex, it is not uncommon to see fees of several hundred dollars.

In fact, in times of extreme congestion, commonly known as "gas wars", fees can be in the thousands. The most notable example of this occurred during the Bored Ape Yacht Club's April 30th launch of Otherside, where users had to pay a minimum of $6K in fees to purchase land!

Unlike in traditional finance, transaction fees are independent of the transaction amount (i.e. it costs the same to send $1 or $1 million), so while this may not effect high-dollar users, it's effectively crowding the average consumer out of the market.

These high fees have spawned the creation of many alternative blockchains – such as Avalanche, Solana, Cardano, Polkadot and BNB Chain – that offer significantly lower fees and transaction times. For this reason, they are often known as "Ethereum Killers".

Chapter 88: Limited Traction

One of the most common criticisms of Web3 is that there are no "real-world" use cases.

At first glance, I can see how someone could think that. After all, most vendors don't accept Bitcoin and it's too volatile (and slow) to be used as money anyway, the NFT market seems to just be a bunch of rich kids spending hundreds of thousands of dollars on pictures of monkeys and most DAOs are unbelievably disorganized and inefficient.

None of this should come as a surprise, however, because disruptive technologies are – by definition –notoriously inefficient when they begin. As such, they are often relentlessly mocked.

Early skeptics of the internet believed that online companies would never turn a profit, and Clifford Stole of Newsweek argued that "no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works."   Even early users of the telephone thought it was useless because the signal could only travel a few miles.

<u>Newsweek's Early Opinion of the Internet</u>

Source: Newsweek

While there has undoubtedly been a lot of absurdity and hype in the crypto market, when we dig a little deeper we can see several burgeoning use cases:

1. **DeFi:** Decentralized exchanges have recorded nearly $1.5 trillion in trading volume over the last year. While this is just a fraction of the $14 trillion boasted by centralized exchanges, there is one major difference – DeXs can't restrict users based on their geographic location. As such, when China banned cryptocurrency trading in 2021, many users were still able to get their money out using Uniswap

2. **NFTs:** Nearly $40 billion of NFTs have been sold since 2020. While one may argue that this interest in digital apes, punks and goblins was just a fad, they're missing one major point – the creators of these NFTs were paid a royalty each time they sold. While this is common practice for recording, television and movie stars, it had previously been all but impossible to employ for visual artists

3. **Decentralized Infrastructure:** While it has long been a dream to create a user-owned internet, every attempt has failed because users aren't incentivized to host their own infrastructure. Helium changed this through the use of cryptoeconomic incentives, growing a network of 1 million connected devices that spans 182 countries.

4. **DAOs:** Most talent networks such as Upwork charge contributors up to 40% for participating in the platform. By organizing itself into a decentralized autonomous organization, Braintrust was able to build a 700,000 member, $100M+ volume talent marketplace that only charges 10% fees

5. **Fair Marketplaces:** Content marketplaces such as Spotify and iTunes often charge artists up to 30% of their sales. Combined with the cut taken by the major labels (UMG, Sony and Warner Music Group), the average musician takes home less than 10% of the revenue they generate. Decentralized marketplaces such as Audius change this and allow artists to earn up to 90% of sales

6. **Permanent Webpages:** "Link rot" – the phenomenon where you try to access a webpage and receive the 404 "page not found" error – is a major problem in today's web. Because of the high cost of ongoing server maintenance, it is estimated that over 30% of links posted on social media will be dead within two years and over 98.4% will fail after twenty. Companies such as Arweave are using cryptocurrencies to pioneer new solutions that allow a user to pay once and receive hosting forever.

7. **Play-to-Earn Gaming:** While the project ultimately crashed, the blockchain-based game Axie Infinity recorded over $4 billion of sales, allowing many users to earn thousands of dollars a month in cash collecting and selling virtual goods (more than the average income of a teacher, construction worker or office assistant in the Philippines, the game's most popular region). This would have been all but impossible for many "Web 2.0" games, which often restrict the ownership and transfer of digital items

8. **Borderless Currencies:** During the early days of its war with Russia, the Ukraine was hampered by a series of restrictions that made the transfer of fiat money into the economy complicated and slow. As such, the nation turned to crypto, raising over $100 million in Bitcoin, Ethereum and other tokens to fund its defense.

While this may not seem like a lot in the grand scheme of things, it's progress. After all, the criticism after the last market crash in 2017 was that there were "no uses cases" for cryptocurrencies. At least now we've progressed to "barely any use cases".

Chapter 89: Volatility

Cryptocurrencies are notoriously volatile – Bitcoin alone recorded swings greater than 2 standard deviations an average of almost 20x per year over the past 5 years.

Bitcoin has swung more than 2 SDs almost 20 times a year since 2017
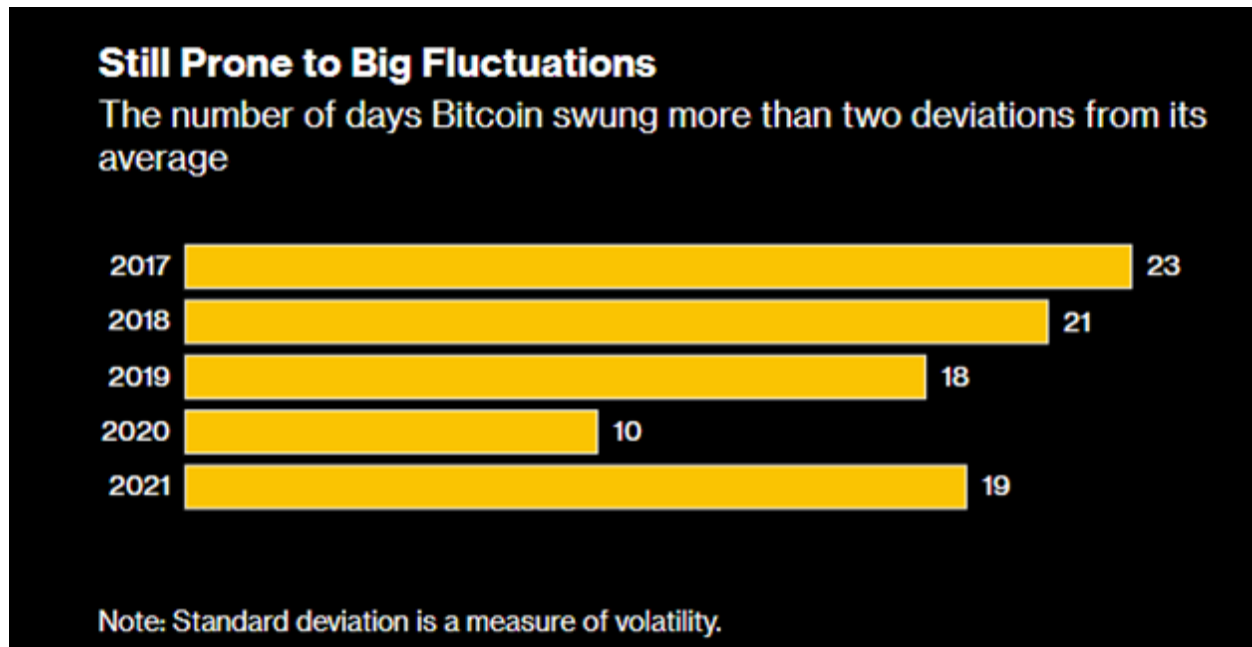
Source: Bloomberg

Many critics argue that this volatility will be their ultimate downfall. After all, something can't function as a medium of exchange if its value fluctuates wildly from one day to the next. Imagine waking up not knowing whether the coins in your digital wallet could buy you a new car or a cup of coffee.

This concern is a big driver of the demand for stablecoins, which offer many of the benefits of cryptocurrencies while maintaining a 1:1 peg to traditional currencies such as the USD, Renminbi or Euro. Because they maintain a constant price, these assets can be used for everyday transactions such as paying salaries, making loans, buying goods and services, etc… Many of the most popular cryptocurrencies today are stablecoins, with Tether and USD Coin commanding the third and fourth largest market caps at $68 billion and $47 billion, respectively (as of 10.2.22).

Ironically, many cryptocurrency disciples believe that stablecoins won't be necessary in the long-run, as they argue that "volatility" is simply a matter of perspective. Given that we price goods in the United States in US dollars, we measure "volatility" by that standard (i.e how much did an asset go up or down in dollar value). But if you were to measure using Bitcoin as the baseline, you could argue that it's the dollar that's volatile!

Indeed, purists argue that's the direction we're headed. They believe that once cryptocurrencies gain widespread adoption, businesses will begin to use them to price goods and services. When

_____

this happens, there will be no more volatility as a 10 satoshi cup of coffee will always be worth 10 satoshis, no matter what happens to the Dollar, Yen or Won (FYI – a "satoshi" is the smallest unit of Bitcoin, worth 1/100millionth or a BTC).
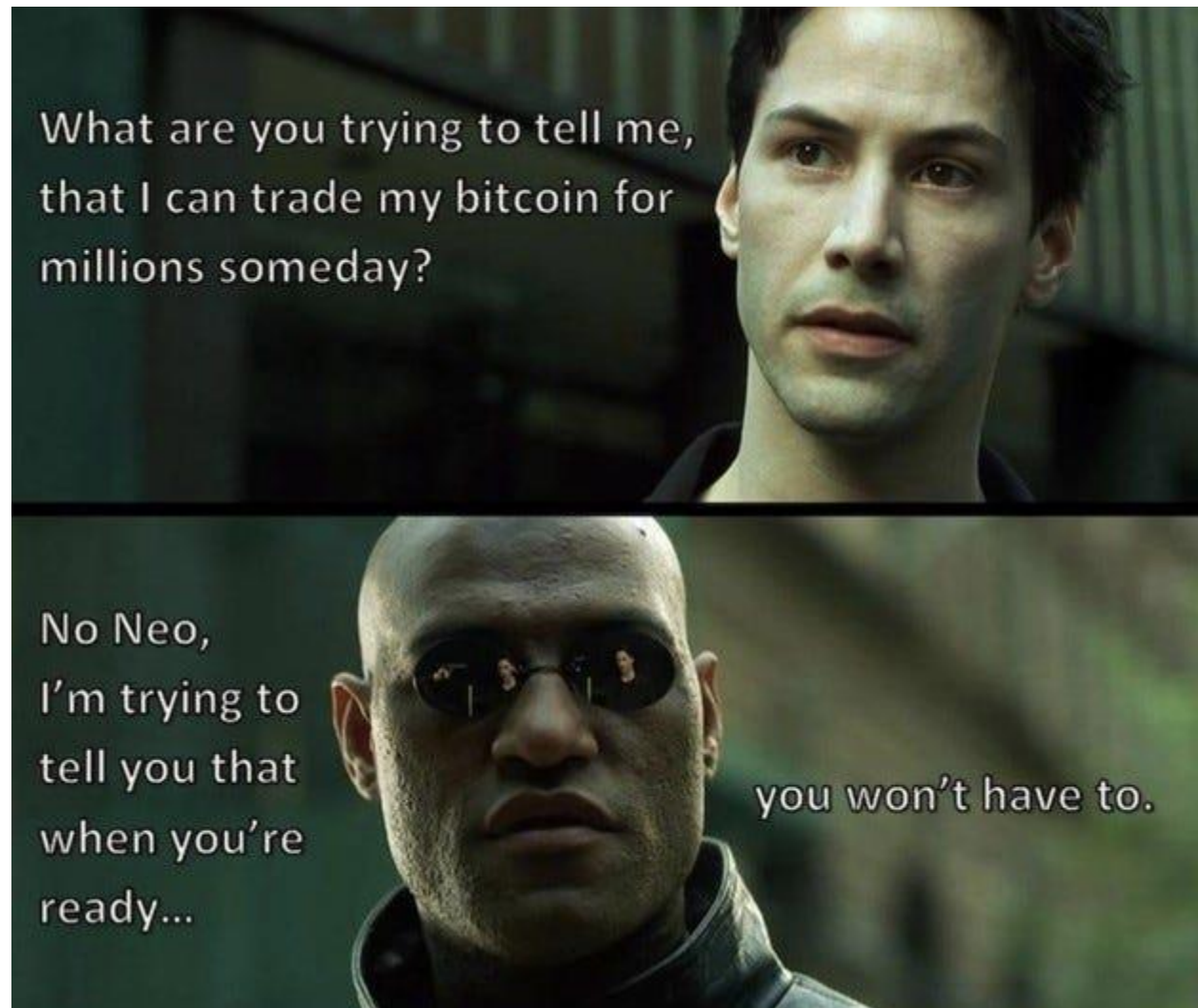
While this might seem far-fetched it should be noted that this is already happening on a limited scale. Many Web3 goods, such as NFTs, are already natively priced in Ether and not USD.

_____

Chapter 90: Environmental Concerns

Proof-of-work consensus mining uses a significant amount of energy. It has been estimated that each transaction uses enough electricity to power the average American home for a month. When you add all the transactions together, the cost is staggering – Bitcoin alone consumes approximately 150 terawatt-hours per year.

That's nearly 10x the amount Google uses and more than many countries including Malaysia, Sweden, Ukraine, Argentina and Norway!

<u>Bitcoin consumes more energy than many countries</u>
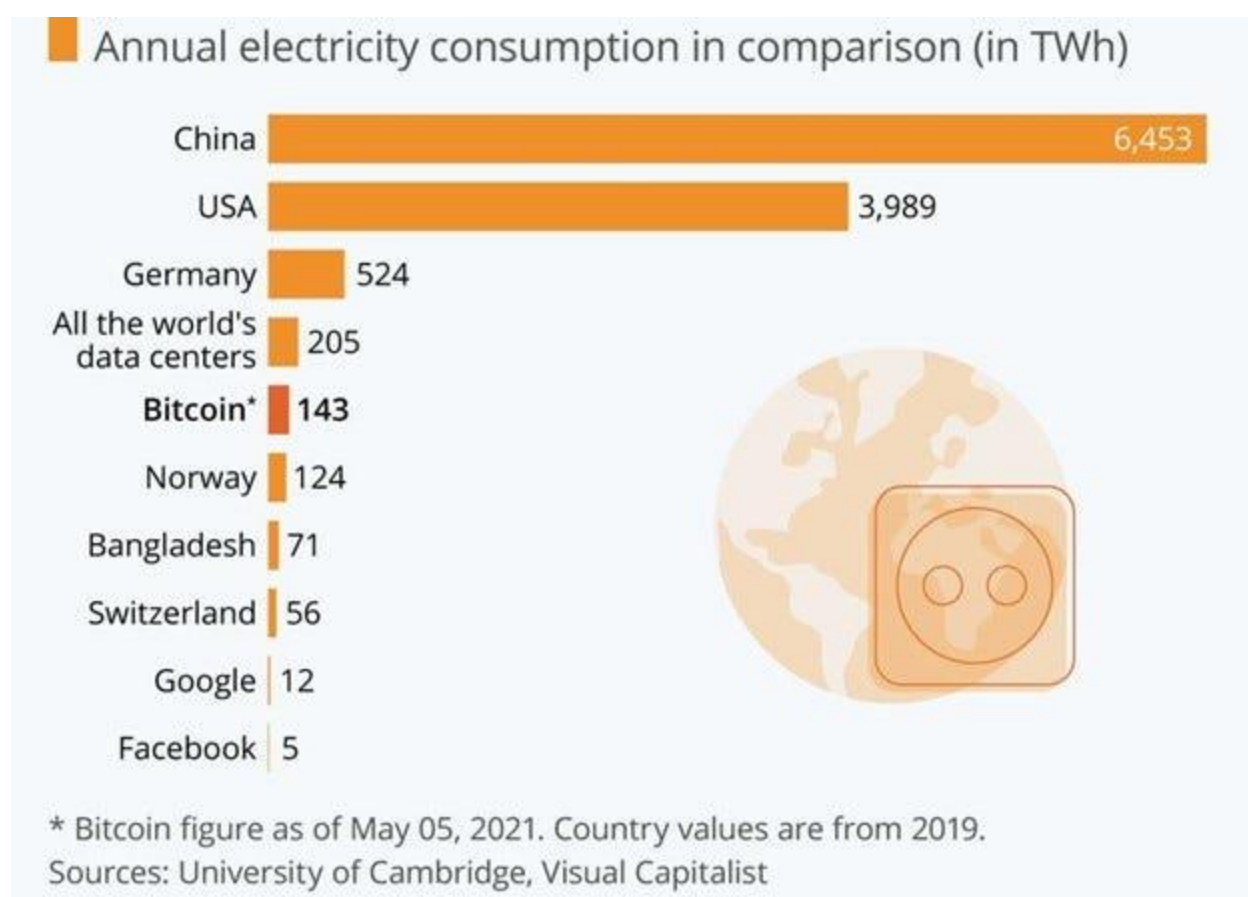
Source: <u>Forbes</u>

Fortunately, these statistics may not be as alarming as they seem at first glance. First of all, energy expenditure does not necessarily equate to environmental impact. In fact, because miners are incentivized to find the cheapest source of energy possible, many rely on alternative sources such as wind or solar. Some estimates believe that 40% to 75% of the energy to power proof-of-work mining may come from renewable sources.

Second, many newer cryptocurrencies are adopting a proof-of-stake model (and Ethereum recently transitioned to one in September of 2022), which uses almost no energy.

Chapter 91: Interoperability Challenges

While Ethereum may have had a monopoly on the smart contract space in 2020, its share has been steadily eroded by the emergence of several new competitors. As such, consumers are now using multiple "alternative L1s" such as Solana, BNB Chain, Avalanche, etc…

<u>The Smart Contract Space Now Has Several Major Players</u>
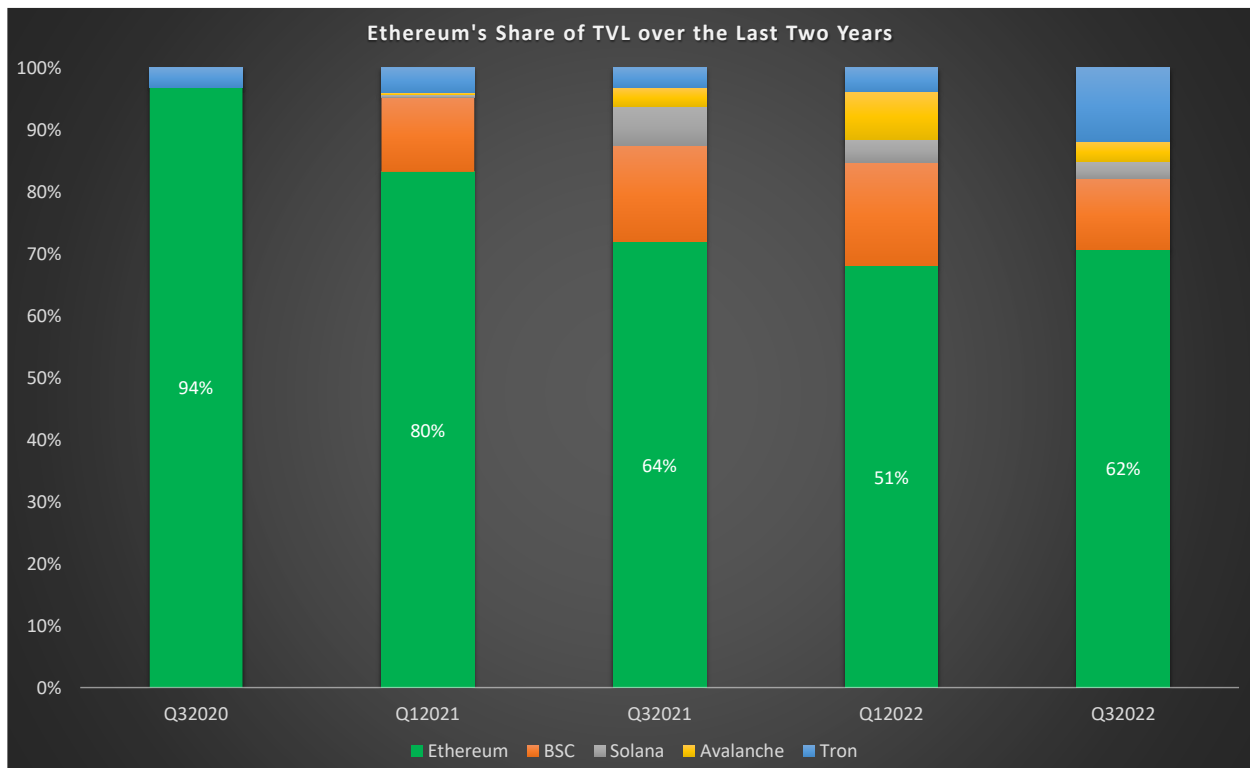
Source: Defillama as of 10.2.22

While arguably good for the long-term health of the ecosystem, this explosion of smart contract platforms has created significant short-term problems. Perhaps most pressing is the problem of interoperability.

Because blockchains have different protocols, they cannot communicate or transact directly with one another. For example, you can't directly buy an Ethereum NFT using a Solana token.

As such, the ecosystem has developed several "workarounds", such as bridges, that *appear* to allow users to transfer tokens from one chain to another. Unfortunately, bridges don't actually work this way and instead "lock" the tokens on one chain and create an entirely new set of tokens on another.

This means that if you want to swap 100 ETH tokens for 5,000 SOL tokens via a bridge, you're actually doubling the number of tokens in existence. The original 100 ETH is "locked" on the Ethereum blockchain and 5,000 new SOL tokens are issued on the Solana blockchain.

While this isn't in a problem *in theory* – as the average user can't access these "locked" tokens – hackers frequently find ways to penetrate the system's security and steal them. Indeed, in the first half of 2022 alone, criminals have stolen almost $2 billion from bridges!

<u>Bridges are a Major Source of Crypto Hacks</u>

Source: Elliptic
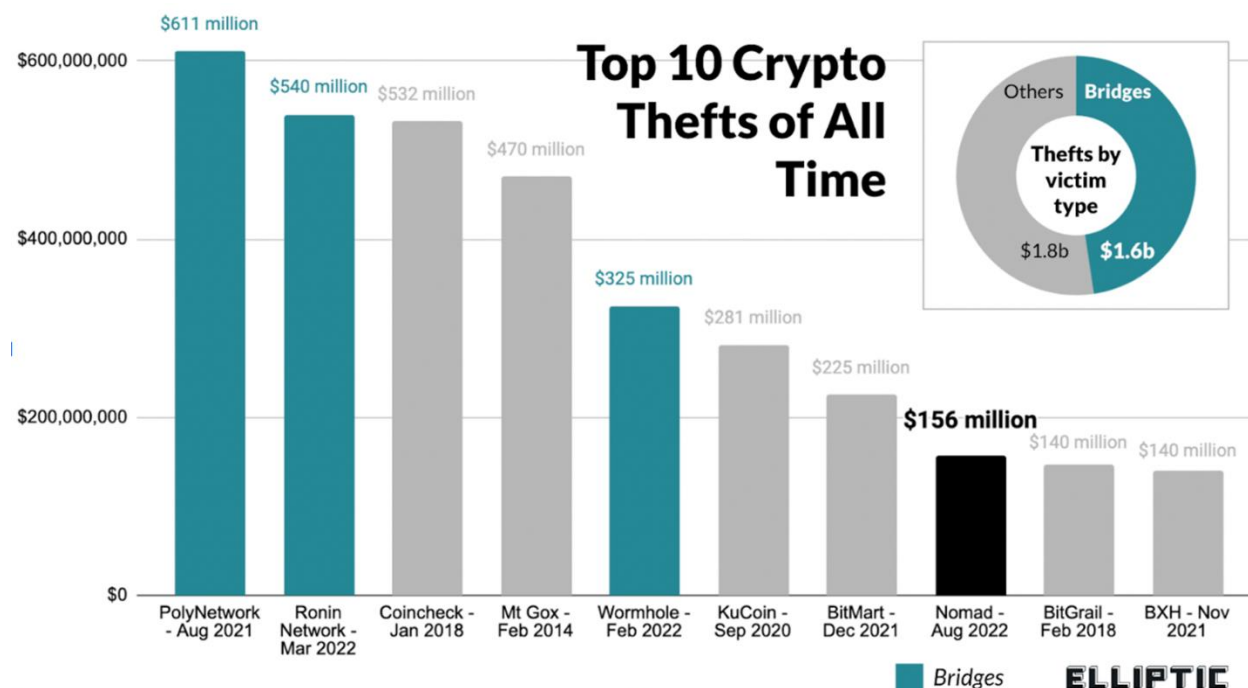
While some may argue that the solution to this problem is simply developing bridges with better security, others argue that it's a Sisyphean task, as having hundreds of thousands of individual vaults containing billions of "locked" tokens will be impossible to defend and always serve as an enticing honeypot to hackers.

Even Vitalik himself argues that bridging is ultimately impossible, stating that while "**the future will be 'multi-chain', it will not be 'cross-chain'**".

While the jury is still out on whether it's possible, there are nevertheless hundreds of talented teams working on creative and novel solutions to the interoperability challenge.

Given the likelihood of a multi-chain future, any protocol that can efficiently solve this problem will likely garner a 12-figure enterprise value.

Chapter 92: Miner-Extractable Value (MEV)

As discussed previously, cryptocurrencies are secured by miners (or "validators" for Proof-of-Stake systems) who gather transactions, verify them and include them in the next block.

Because each block can only contain a limited number of transactions, miners generally choose which transactions to include based on an auction process. Those who offer to pay the highest fees will be included first.

Unfortunately, miners aren't technically *forced* to follow this rule and ultimately have full discretion over which transactions to include, which to ignore and how to order them. When miners abuse this power to personally profit, it's known as Miner-Extractable Value (MEV).

There are a host of MEV tactics, but a common one is known as frontrunning. To see how this works, let's imagine that you noticed that ETH was trading for a lower price on exchange A than it was on exchange B. Seeing a great arbitrage opportunity, you put in an order to buy ETH on exchange A and then sell it on B. Once you place the order, it gets sent to the miners who put it in a transaction queue.

Once this transaction is in the queue an unethical miner could now see what you are trying to do and decide to ignore your request and make the same trade himself, stealing your profit opportunity in the process.

As mentioned, there are several of MEV tactics and, to make matters worse, many of them are now employed by automated bots. As such, MEV is becoming a substantial problem that is estimated to cost users over $1 billion annually.

Chapter 93: Poor User Experience

One common criticism of Web3 is that the user experience pales in comparison to Web 2.0.

This is understandable, as Web3 transactions are quite different than what we're used to and can seem rather complicated at first glance. For instance, in order to buy an NFT, a user needs to:

1. Register on a centralized exchange, such as Coinbase or Binance
2. Provide KYC information such as a passport photo, driver's license and / or utility bill to confirm their identity
3. Use the centralized exchange to purchase Ethereum
4. Set up a wallet via Metamask
5. Transfer their Ethereum to their Metamask wallet
6. Go to OpenSea or LooksRare and connect their wallet
7. Search for an NFT they like
8. Click to purchase it
9. Approve the gas fees and sign the transaction

I'll admit, when I first tried buying NFTs I was definitely nervous navigating all these steps.

But once I did it, I realized how simple it was. In fact, once you're used to it, navigating Web3 is much easier than navigating the traditional web because:

- You don't need passwords – once you have a wallet setup it can connect to any site
- The checkout process is simple as you don't need to input a credit card, check for fraud, etc..

That said, more work needs to be done to either educate the public or streamline the onboarding experience.

_____

Chapter 94: Usage by Criminals and Terrorists

Several of the core benefits of decentralized economies could also be seen as weaknesses. The fact that they allow anonymous individuals to form organizations that exist outside of the traditional financial and legal system could be a recipe for disaster. Indeed, critics argue that the crypto space is the ideal venue for:

- **Tax Evasion**: Because cryptocurrency transactions are anonymous, people could use them to evade taxes

- **Criminal Activity**: Transactions can't be regulated, which means that criminals could create decentralized organizations to sell drugs or weapons

- **Funding Terrorists**: Terrorists groups could theoretically form a DAO to receive funding from anonymous sources

While all of these are definitely possible – and even *seem* logical at first blush -- the data simply doesn't support these fears. In fact, only 0.15% of all cryptocurrency transactions are connected to criminal dealings.

Illegal Activities Represent Only 0.15% of Cryptocurrency Transactions

Illicit share of all cryptocurrency transaction volume | 2017–2021
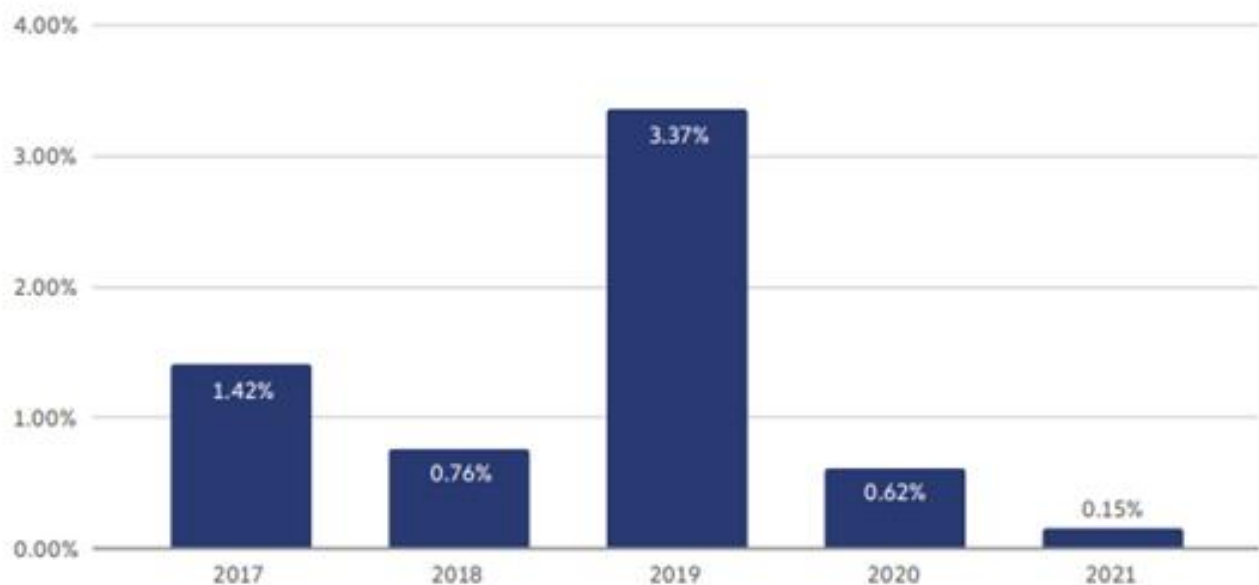
Year	Illicit Share
2017	1.42%
2018	0.76%
2019	3.37%
2020	0.62%
2021	0.15%

Source: Chainalysis 2022 Crypto Crime Report

_____

A big part of the reason for this is probably **because cryptocurrency transactions aren't actually anonymous**, they are "pseudonymous" – meaning that if anyone can tie you to your address, they can see *all* of your transactions. This has proven a boon time and time again to law enforcement, who have used the transaction history to track down several high-profile thieves. In 2022 alone, the Department of Justice seized $3.6 billion from crypto hackers.

Ironically, given the fact that all transactions are recorded forever on a digital ledger, cryptocurrencies may ultimately reduce crime, fraud and tax evasion.

Chapter 95: Hacks and Scams

Crime is an ongoing problem in the cryptocurrency space. According to blockchain data firm Chainalysis, over $14B was stolen in 2021 across the broader ecosystem.

<u>Criminals Received Over $14B in Cryptocurrencies in 2021</u>

Total cryptocurrency value received by illicit addresses | 2017–2021

Legend: Malware, Terrorism financing, Stolen funds, Scam, Sanctions, Ransomware, Cybercriminal administrator, Fraud shop, Darknet market, Child abuse material

- 2017: $4.6B
- 2018: $4.4B
- 2019: $11.7B
- 2020: $7.8B
- 2021: $14B
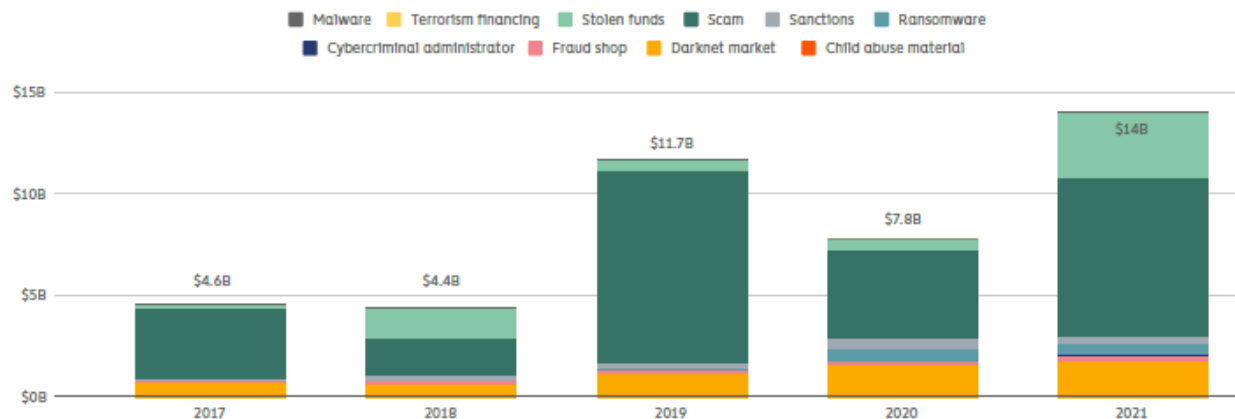
Source: Chainalysis 2022 Crypto Crime Report

Three of the most popular methods used by criminals include:

- **Malware**: Malicious software that infiltrates a user's computer, generally gaining access to his or her private keys
- **Code Exploits**: Occur when coders find a vulnerability in a smart contract and leverage that to siphon funds to their own address
- **Scams**: Utilize social engineering to deceive users and steal funds (e.g. a Ponzi Scheme)

Let's take a deeper look into each of these categories below:

<u>Malware</u>

Malware was responsible for over $3B of losses in 2021.

_____

Malware Cost Users $3.2B in 2021

Total value stolen and total number of thefts | 2015–2021
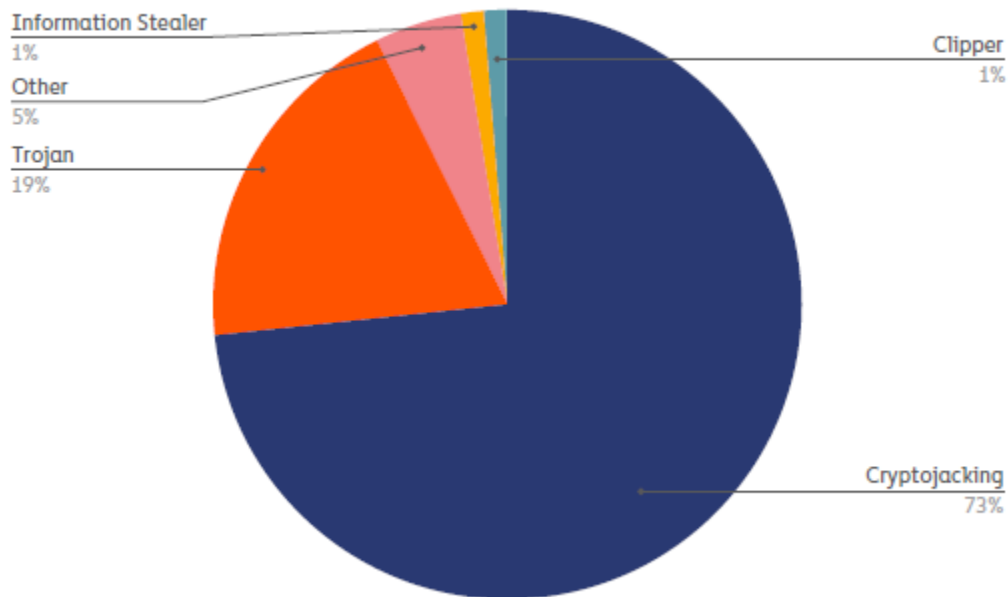
Source: Chainalysis 2022 Crypto Crime Report

The most popular methods used by hackers include:

- **Cryptojacking:** The unauthorized use of someone else's computer to mine cryptocurrency. Technically, cryptojackers are stealing computing power (and therefore electricity), but this can be given a numerical value.

- **Trojans:** Viruses that look like legitimate programs but instead infiltrate a user's computer to steal important data such as a person's private keys

- **Clippers:** Clipping is the process of inserting new text into a user's clipboard. Hackers use this to insert the address of their crypto wallets, so when a user goes to transfer funds it is redirected to the hacker (note: always triple check the address you're sending to!)

- **Info Stealers:** Collect saved files, autocomplete history and seed phrases from compromised computers.

Code Exploit

Like any piece of software, smart contracts with poorly written code have significant vulnerabilities. This is common across the cryptocurrency sphere and the DeFi, NFT, DAO, Smart Contract and Web3 spaces have all suffered exploits.

Projects lost hundreds of millions to hacks in 2021. Notable exploits include:

_____

<u>Notable Hacks in 2021</u>

The 10 Largest Cryptocurrency Thefts of 2021

Victim	Amount stolen (USD)	Service Type	Hack Type	Description
Poly Network	$613 million	DeFi platform	Code exploit	An attacker exploited cross-chain relay contracts to extract Poly Network funds from three different chains: Ethereum, BSC, and Polygon. The attacker ultimately returned the stolen funds. Read our complete case study.
BitMart	$200 million	Exchange	Security Breach	Attackers stole a private key that compromised two of BitMart's hot wallets.
BadgerDAO	$150 million	DeFi platform	Security Breach	Attackers used a compromised cloudflare API key to periodically inject malicious scripts into the Badger application. The scripts intercepted transactions and prompted users to allow a foreign address to operate on the ERC-20 tokens in their wallet. Once approved, the attacker siphoned funds from the user's wallets.
Undisclosed	$145 million	Private	Other — Embezzlement	Employee allegedly diverted funds to a personal account when the company attempted to transfer funds between financial accounts.

Source: Chainalysis 2022 Crypto Crime Report

This is not a new phenomenon and hacks have plagued the space since inception. Indeed, one of the first Bitcoin exchanges known as Mt. Gox – which handled 70% of all Bitcoin transactions at the time – was hacked in 2014 and 750K BTC were stolen (worth nearly $15 billion today – October 2nd, 2022).

In addition, the first DAO, known simply as "The DAO", was also the victim of an exploit. The project launched in 2016 and raised $150 million worth of Ether. Less than three months after launching, it was hacked, causing the project to lose $60 million.

The DAO hack caused controversy on many levels in the space. Notably, there was a debate on whether or not to reverse the transaction. Doing so would effectively return the funds, but also go against the spirit of decentralization and set a poor precedent.

Voters ultimately decided to reverse the attack, "forking" the Ethereum blockchain into:

- Ethereum: The version that restores the funds lost in the attack to their original addresses. This is the chain that most people use today

- Ethereum Classic: The original chain that preserves the hack. Classic is much less popular and trades at approximately 2% of the value of ETH

Although the funds were restored, the hacker did not lose out entirely, as he or she still retains possession of Ethereum Classic coins which are now worth over $100 million.

Scams

Outright scams were the largest source of cryptocurrency-based crime in 2021, costing users over $7.7B.

Scammers Stole $7.7B in 2021

Total yearly cryptocurrency value received by scammers | 2017–2021

Legend: ▮ Rug pulls ▮ Other scams
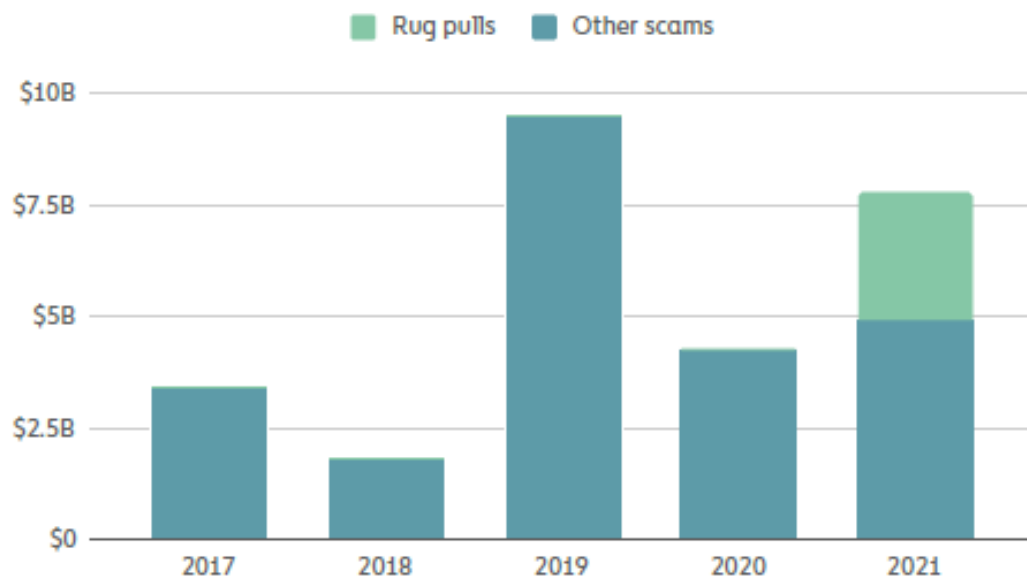
Source: Chainalysis 2022 Crypto Crime Report

While there are multiple types of scams in the crypto world (e.g. ponzi schemes, pump-and-dumps), a new form gaining notoriety is the "rug pull".

Rug pulls (aka "rugs") occur when a founder creates a project with the intent to abandon it and run off with the investor's funds. Critics argue that the hype around the space, lack of investor protections, ability for founders to remain anonymous and self-custody of funds provide an ideal breeding ground for these types of scams.

Indeed, rugs cost investors billions and accounted for 36% of the total crypto scams in 2021 (up from 1% in 2020). They have infected nearly every vertical including DAOs, DeFi, NFTs and cryptocurrencies.

Chapter 96: Lack of Legal and Regulatory Clarity

In most of the world, the crypto space still exists in a legal "grey area". The technology is still relatively new, and many governments haven't had time to catch up.

And while the space has its fans in the administration, it also has its share of detractors. For instance, SEC Chief Gary Gensler labeled the space as the "wild west" and Elizabeth Warren called DeFi "one of the shadiest parts of the crypto world".

<u>Elizabeth Warren Doesn't Like DeFi</u>

Although some things are definite – like the fact that profits gained from cryptocurrency trading is taxable in the US – there are still several open issues. While going through the entire gamut of these outstanding legal questions is well beyond the scope of this article, here are a few recurring themes:

- **Cryptocurrencies:** Although the US has deemed that Bitcoin is not a security, it has not passed the same judgement on every project (in fact Ripple, once one of the largest projects, is currently battling the SEC on that issue). In addition, many nations are struggling to deal with the tax implications of novel concepts such as airdrops

- **DeFi:** With the $40 billion collapse of the Terra stablecoin, DeFi is coming into sharp regulatory focus. Some of the questions regulators are trying to address are the legal treatment of decentralized exchanges, the enforcement and validity of smart contracts and potential regulations around stablecoins

- **NFTs:** Given the fact that the NFT market is only a few years old, it has been largely ignored by regulators. That said, there are several outstanding questions when it comes to the legal standing of non-fungible tokens, including: are they securities, what intellectual property rights are transferred in a sale and how do KYC and AML laws apply?

- **DAOs:** Given that DAOs have no physical location and don't register as corporations, they often exist in a legal state of limbo. This creates several potential risks – it's not clear whether DAO members have the same personal protection they would have in an LLC, there's no clear guidance on how a DAO pays taxes and it's not clear how DAOs can do business with traditional corporations

Unfortunately, these uncertainties haven't always stopped authorities from pursuing action against alleged offenders. While some of these cases are definitely warranted, such as the prosecution of an OpenSea employee for the insider trading of NFTs, others have been met with fierce resistance from the crypto community.

Perhaps the biggest example of this is the Netherlands' arrest of blockchain developer Alexey Pertsev, the creator of Tornado Cash. Tornado Cash is a "mixing" protocol designed to protect a user's privacy. Consumers can deposit cryptocurrencies in the platform, get an "IOU", and then redeem this IOU for a fresh set of tokens with different identification numbers.

While there are a dozen valid reasons for wanting privacy, Tornado Cash was unfortunately often used heavily by criminals and rogue regimes such as North Korea.

Despite this fact, most people in the crypto space agree that it's unfair to punish someone for creating a an open-source piece of code – that would be like jailing Tim Cook because drug dealers tend to use iPhones.

Given the unclear state of regulation in crypto, the Biden administration issued an executive order in March calling on regulators to explore the risks and benefits of the technology. Researchers will focus on potential measures to protect consumers and the financial system, mitigate illicit activity, advance US leadership in the technology and promote safe and equitable access.

While the results of this report could greatly impact centralized systems such as Coinbase or Tether, it's not clear how regulation would work for the broader ecosystem or if it's even possible in the long-run.

After all, blockchains are decentralized systems -- that is, they're run by thousands to tens of thousands of computers across the world – so there's generally no central point authorities can use to enforce rules or shut them down.

Part 9: Why Web3 Will Eat the World…

Chapter 97: What is Disruption?

The concept of "disruption" is overused and often misunderstood — many writers, consultants and researchers use the word to refer to any situation where a new player enters a market and starts to displace incumbents.

But the academic theory is much more nuanced — disruptive technology isn't necessarily "better" (in fact, it's almost always worse), it's just so fundamentally different from the status quo that it **can't be replicated by incumbents or competitors**. This gives it the ability to gain a foothold in an industry and, as technology improves, gradually eviscerate the market.

Disruptive Technologies Almost Always Initially Have Worse Performance
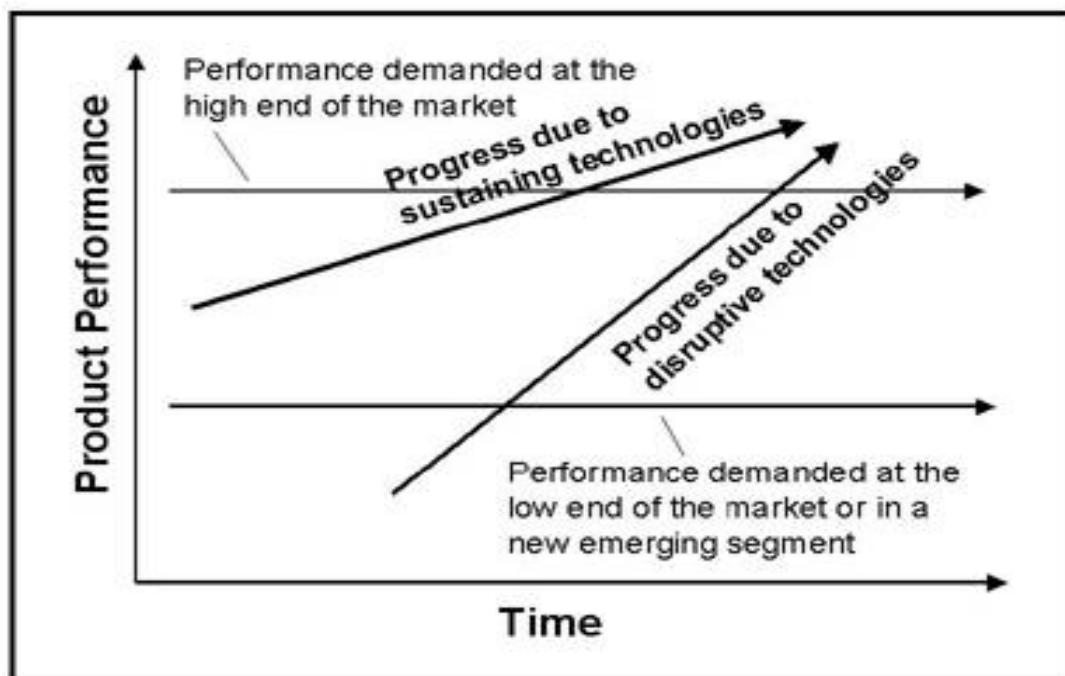
Source: Clayton Christensen

For a real-world example, we need to look no further than AT&T — one of the original disruptors.

In the late 1800s, Western Union dominated communications with a huge infrastructure of network cables and a massive consumer base. Although early telephones were largely inferior to the telegraph because their signals only traveled a few miles, the technology was much cheaper for short-distance communication and was therefore rapidly adopted by local businesses.

In a textbook case of disruption theory, Western Union couldn't react because serving these local businesses would be unprofitable. This gave AT&T the niche they needed — as telephone technology gradually improved they were able to continue to take share from Western Union, eventually rendering the incumbent all but obsolete.

Chapter 98: Birth of a Digital Nation

I believe that Web3 represents a classic case of disruptive innovation and has the potential to create digital entities that rival (or even replace) existing nation-states.

Like most disruptors, the space definitely has a ton of problems today – such as high fees, rampant fraud and theft and a relatively poor user experience.   But it also offers one advantage that traditional nation-states simply cannot match – true autonomy. A nation driven by Web3 could maximize personal freedom while minimizing the risk of bureaucracy, exploitation and corruption that often arises from centralized entities such as corporations, banks, governments and courts.

While the thought of Web3 forming something akin to a new nation may seem ridiculous at first glance, it's important to remember that nation-states – at least in the form we know them today – are themselves a relatively recent phenomenon, having existed for only ~200 years.

At their core, they are just *one* way of organizing people and coordinating their economic output. Prior to the nation-state, we had empires, tribes, feudal kingdoms, etc…. The nation-state ultimately prevailed as the dominant form of governance because people demanded (often by force) more individual sovereignty and personal freedom.

Digital Nations Could be the Next Logical Step in Governance

	Tribes (< 500)	Feudal Kingdoms (500 - 1500)	Empires (1500 – 1800)	Nation-States (1800s – Present)	Digital Nations (???)
Money	Barter	Gold	Commodity-Backed Currency	Fiat Currency	bitcoin — Cryptocurrency
Financial System	Temples	Moneylenders	Merchant Banks	CHASE — International Banks	AAVE — DeFi
Goods	Basic Commodities	Luxury Commodities	Manufactured Goods	salesforce — Digital Goods	BAYC — NFTs
Law	Chief	Feudal Lord	King or Emperor	President, Congress, High Court	ethereum — Smart Contract Platform
Economic Entities	Individuals	Guilds	Dutch East India Company — State Charted Corporation	Google — Limited Liability Company	UNISWAP Governance — DAO

So is it unrealistic to think that another paradigm shift is possible?   After all, we now have the technology to replicate most, if not all of the core features of a nation state. The internet allows for real-time global communication, a sense of shared culture and purpose and instant transactions, and Web3 gives us all the building blocks we need – a native currency, financial system, native goods and laws – for a fully functioning economy.

Perhaps more importantly, a decentralized state seems to offer several benefits over what we have now, including:

- **Fast and Efficient**: Web3 operates almost entirely via computer programs which automate the execution of all transactions. As such, there's no need for intermediaries such as bankers, regulators, lawyers, accountants, executives or government bureaucrats – making the system much faster and cheaper

- **Sovereign**: Web3 users have complete ownership and control of their assets, meaning no government, bank or corporation can seize them

- **Borderless:** Web3 has no borders. There are no citizenship requirements and anyone with an internet connection can join a digital nation and participate in markets that are open 24 hours a day, 7 days a week and 365 days a year

- **Transparent**: Every transaction in Web3 is broadcast to the public allowing for real-time monitoring and maximum transparency. In addition, protocols are built with open-source code allowing any user to audit them, greatly reducing the threat of corruption and serving as a safeguard against negligence

- **Permanence**: As a digital nation, Web3 is immune to traditional methods of coercion – it can't be bombed or occupied by an enemy army. And because it is hosted on thousands of devices across the world, it's very resistant to failures and almost impossible to shut down

Personally, I think it's very possible – if not inevitable – that we will see digital states within our lifetime.

Chapter 99: What is the Economic Potential of a Digital Nation?

If digital nations do prove to be superior model of organization, it's not completely unrealistic to think that they may grow to rival existing, geographically-based ones in terms of economic value. After all, over 5 billion people use the internet and they are spending more and more of their time on it.

Furthermore, this encroachment of the digital world into the "real" one is not without precedent as:

- Digital entertainment makes up 72% of all entertainment revenue
- Online advertising makes up 2/3rds of total advertising
- Global eCommerce sales are approximately 20% of total retail sales and expected to grow to nearly 25% by 2025 (and in some countries, such as China, online sales make up almost half of all purchases)

Indeed, as Web3 matures, it too will likely begin to take share. While how much is still up for debate, the fact that the value of all crypto assets is less than 0.1% (1 / 1,000th) of the financial and physical asset market means that there's a lot of room to grow!

Crypto Assets Still Make Up a Very Small Percentage of Global Assets
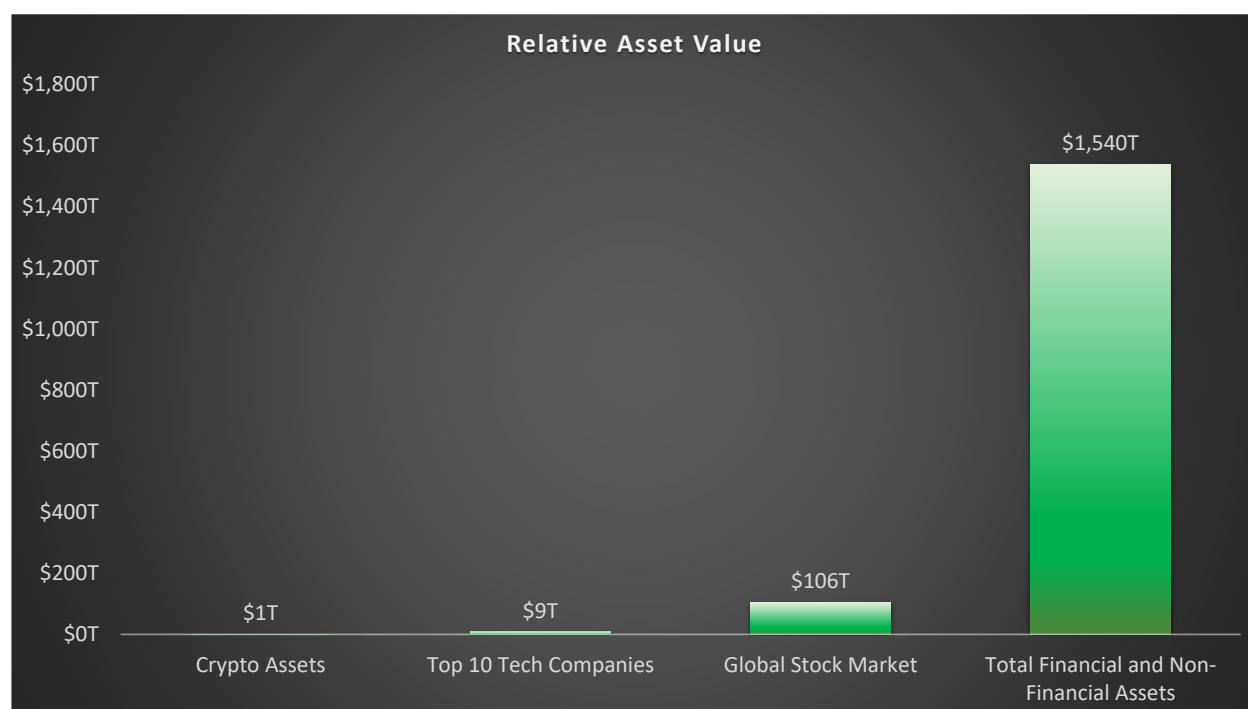
As such, Web3 could grow 10x from here (to $9T) and be roughly equivalent to the top 10 tech stocks…

…it could grow 100x from here (to $90T) and be roughly equivalent to the global stock market…

…and while I'd admit that 1,000x growth is a bit of a stretch ($900T) that would put it at roughly 60% of the world's total financial and physical asset market.

And keep in mind this analysis is for the "crypto space" as a whole. While cryptocurrencies themselves have appreciated significantly, and now account for roughly 1% of the global stock market value, verticals such as DeFi and NFTs are still relatively small, accounting for 0.005% and 0.004% of financial and real assets, respectively.

Wherever this thing ends up, it's important to watch as it has the potential to be both an existential threat to incumbent systems and a road to almost unlimited potential for investors.

Part 10: Web3 University

_____

Part 10 of this book is intended to provide a collection of the best articles, books, videos, podcasts, twitter accounts, reddits, news and research sources I've found covering Web3. So if you're interested in any particular resource, please don't hesitate to jump to that section.

Unfortunately, while there's a ton of great material below, I realize that most people don't have unlimited time to consume it all.

As such, I've created a special "Web3 University" section that attempts to organize all the material by rough order of priority, aligning it with the amount of time *you* have to learn. For instance, there are sections that can be finished in 1 hour, 1 week or 1 year.

The University consists of six levels:

1. White Belt: A basic overview of cryptocurrencies that can be consumed in **less than an hour**

2. Blue Belt: A short collection of articles and videos that can be **finished in a day**

3. Purple Belt: A more detailed collection of books, articles, videos and podcasts that will take **roughly a week to complete**

4. Brown Belt: A collection of the best books on the space as well as suggestions for how to stay on top of developing trends (including Twitter accounts to follow). This will take roughly **one month to finish**

5. Black Belt: Suggestions for five actions you can take if you want to really start to understand Web3 on a deeper level (e.g. canons, courses, whitepapers, practical experience, current trends). It would likely **take a year to finish** all of these steps

6. Red Belt: Suggestions for **lifelong study**

Like the progressing levels of a martial art, each section builds upon the previous one, striving to give you all the tools you need to become proficient in Web3.

_____

Appendix 1: White Belt (<1 Hour)

If for some reason you needed to learn as much about crypto as possible in an hour, then I'd recommend Linda Xie's An Intro to Crypto: Building Blocks It gives a direct and pithy overview, and it's actually only ~20 min long!

Linda Xie's Intro to Crypto is a Great Way to Learn about Cryptocurrencies and Web3

_____

Appendix 2: Blue Belt (1 Day)

If you want a little more background, but don't have much more than a day, check out the following resources.

What are Cryptocurrencies?
Crypto can be confusing and intimidating to newcomers. To get started, I recommend checking out the following two newbie-friendly resources:

- [Cryptopia: Bitcoin, And The Future of the Internet](#) on Amazon Prime provides a beginner-friendly and broad introduction to the space, and it takes about 90 minutes to watch
- While I don't agree with everything in Kevin Roose's [The Latecomer's Guide to Crypto](#), it nonetheless is a good guide for newbies (bonus points if you want to read ahead by clicking the links at the bottom for NFTs, web3, DAOs and DeFi)

Why are Cryptocurrencies Important?

In a word, "decentralization". Decentralization refers to the ability for crypto to exist outside of the purview of centralized third parties. This brings a host of benefits such as the potential to create a borderless currency that isn't controlled by governments, a financial system that isn't controlled by banks and a web that isn't controlled by Big Tech companies such as Facebook, Amazon, Apple and Google (also known as "Web3"). Nine articles to understand this better are:

- Fred Wilson's [AVC Blog](#) was one of the first to recognize the potential of a currency not controlled by governments or banks
- Chris Dixon's [Why I'm Interested in Bitcoin](#) and [Why Decentralization Matters](#)
- Kyle Samani dicusses the potential of open finance, Web3 and global, state-free money in Multicoin Capital's [Crypto Mega Thesis](#)
- Balaji Srinivasan notes how Bitcoin was already creating value in 2018 in his work [And What Has the Blockchain Ever Done for Us?](#)
- Packy McCormick discusses how cryptocurrencies are already creating value and will likely continue to do so in the future in Web 3 Use Cases [Part I](#) and [Part II](#)
- Nick Tomaino explains how cryptocurrencies could replace corporations in [The Slow Death of the Firm](#)
- Joel Monegro lays the groundwork for Web3 by discussing how crypto could return value to creators in [Fat Protocols](#)

How Does Crypto Work?

Cryptocurrencies rely on three distinct technologies – blockchains, digital key cryptography and consensus mining – to maintain decentralization. The following resources describe how this system works:

- Finematics explains why we need centralize parties to establish trust in the [Two Generals Problem](#)

_____

- Preethi Kasireddy explains the concept of trustlessness in <u>What do We Mean by "Blockchains are Trustless"?</u>
- Whiteboard Crypto breaks down each of these primitives in three articles: 1) <u>What is a Blockchain?</u> ,2) <u>Public and Private Keys (Asymmetric Encryption Animated)</u> and 3) <u>What is Proof of Work?</u>
- 3Blue1Brown ties it all together in <u>But How Does Bitcoin Actually Work?</u>

What are the Key Components of the Crypto Ecosystem?

Since its creation, crypto has evolved into a number of verticals. Let's dig a bit deeper into each of these:

- **Decentralized Money:** A cryptocurrency is a form of money that is created, distributed and owned directly by the public (as opposed to the government). There are three main types of "decentralized money" that you need to know: 1) **Bitcoin:** Bitcoin is the grandaddy of all cryptocurrencies, and you can learn more about it in the official <u>Bitcoin Whitepaper</u>, 2) **Ethereum:** After Bitcoin came Ethereum, a form of "programmable money". Linda Xie gives a great explanation in <u>A Beginner's Guide to Ethereum</u>, Fred Ehrsam talks about its disruptive potential in <u>Ethereum is the Forefront of Digital Currency</u> and David Hoffman argues that ETH is the perfect form of money in <u>Ether: The Triple Point Asset</u>,3) **Stablecoins**: Stablecoins are a very important form of decentralized money. You can learn more about them in <u>What is a Stablecoin?</u> by Whiteboard Crypto
- **Smart Contract Platforms:** Ethereum expanded on the technology of Bitcoin by turning it into a decentralized "world computer", known primarily as a smart contract platform (or "Layer-1"). Whiteboard Crypto gives a good overview of smart contracts in <u>What are Smart Contracts in Crypto?</u> And Finematics gives another good one in <u>Code is Law? Smart Contracts Explained</u>. Finally, Grayscale dives into to most important smart contract platforms in <u>Get Smart on Smart Contract Platforms</u> by Grayscale
- **DeFi:** DeFi, or Decentralized Finance, refers to a global, peer-to-peer network that is built to replace the traditional banking system. Finematics explains more in <u>What is DeFi?</u>
- **NFTs:** An NFT – or "non-fungible token"– is a certificate of ownership for a digital good that is recorded onto a blockchain. Whiteboard Crypto elaborates in <u>What is an NFT?</u>
- **DAOs:** DAOs are blockchain-based organizations that may replace the modern corporation. Packy McCormick highlights their potential impact in <u>The Dao of DAOs</u>
- **Metaverse:** The metaverse is an interconnected network of virtual worlds that will replace the web as the primary way in which we access information. Matthew Ball provides a nine-part overview in <u>The Metaverse Primer</u>
- **Web:** Web3 refers to an internet that is owned by the users instead of companies such as Google, Facebook, Amazon and Apple. Whiteboard Crypto explains more in <u>What is Web 3.0</u>

What Does the Future Hold for Crypto?

Ultimately, cryptocurrencies have the potential to grow massively and even create a new nations. A few more resources are below:

_____

- Cathie Wood explains how Ethereum and Bitcoin still have the potential to 100x in her Big Ideas 2022 Report (note: free download required, you can skip to the sections on Public Blockchains, Bitcoin, Ethereum & Defi and Web3)
- David Hoffman and Ryan Sean Adams describes how cryptocurrencies are forming new nations in A Bankless Nation Part I and Part II
- Tascha continues with the "nation-state" thesis in Public Blockchains Are the New National Economies of the Metaverse

_____

_____

Appendix 3: Purple Belt (1 Week)

This section provides even more articles and videos, as well as a few books and podcast episodes. It should take roughly a week to complete.

What is Web3? Web3 refers to an internet owned by users instead of Internet Giants such as Facebook, Apple, Amazon and Google. Below we have an article, book and podcast that you can peruse to get an overview.

- Article: Web3: in a Nutshell by Eshita Nandini
- Book: Token Economy by Shermin Voshmgir
- Podcast: Chris Dixon and Naval Ravikant — The Wonders of Web3 And Much More on The Tim Ferriss Show

Why is Web3 Important? Web3 is poised to fundamentally restructure our economy. The following resources detail how.

- Own the Internet by Packy McCormick
- The Quiet Master of Cryptocurrency — Nick Szabo on The Tim Ferriss Show
- Crypto Tokens: A Breakthrough in Open Network Design by Chris Dixon
- Crypto Tokens: A Breakthrough in Open Network Design by Chris Dixon
- The Ownership Economy 2022 by Li Jin
- Composability is the Most Powerful Creative Force in the Universe by Jon Radoff
- Understanding Web 3 — A User Controlled Internet by Emre Tekisalp
- Chain Reactions: How Creators, Web3, and the Metaverse Intersect by Rex Woodbury

How does Web3 Work? We've already covered some of the basics of how "blockchains" work, but let's take a deeper dive…

- Ethereum – The World Computer: The Ethereum Whitepaper by Vitalik Buterin, How does Ethereum work, anyway? By Preethi Kasireddy, Ethereum Will Be the Backbone of the New Internet by James
- Digital Ledgers: The Blockchain Economy: A beginner's guide to institutional cryptoeconomics by Chris Berg, Sinclair Davidson and Jason Potts
- The Byzantine General's Problem: Distributed Systems 2.2: The Byzantine generals problem by Martin Kleppmann
- Hash Functions: What is a Cryptographic Hashing Function? By Whiteboard Crypto
- Blockchains: WTF is The Blockchain? By Mohit Mamoria
- Digital Key Cryptography: A Beginner's Guide: Private and Public Key Cryptography Deciphered by Chris Coverdale
- Proof of Stake: What is Staking in Crypto? By Whiteboard Crypto
- Mining Pools: What is a Mining Pool in Crypto? By Whiteboard Crypto
- Smart Contracts: What are Smart Contracts in Crypto? By Whiteboard Crypto
- Gas: What is Ethereum Gas? By Whiteboard Crypto

_____

_____

What are Cryptocurrencies? Cryptocurrencies represent the potential to a "borderless" currency that doesn't rely on central banks

- Overview: The Moneyness of Bitcoin and Ethereum by Ryan Sean Adams
- Money: What is Money? by Investopedia
- Bitcoin: #8 Reasons Why Bitcoin is Better than Conventional Currency by Vishal Gupta
- Ether: The Triple Point Asset by David Hoffman
- Stablecoins: Designing a Price-Stable Cryptocurrency by Haseeb Qureshi

What is DeFi? DeFi, or Decentralized Finance, refers to a global, peer-to-peer network that is built to replace the traditional banking system

- Overview of DeFi: A Beginner's Guide to Decentralized Finance (DeFi) by Sid Coelho-Prabhu
- Stablecoins: Fiat-backed Stablecoins: What is Tether? By Whiteboard Crypto, Crypto-backed Stablecoins: What's MakerDAO and what's going on with it? Explained with pictures by Kerman Kohli, Algorithmic Stablecoins: 3 Stablecoin Algorithms Explained (Rebase, Empty Set Dollar, Basis Cash, Iron Finance) by Whiteboard Crypto
- Decentralized Exchanges: What is an Automated Market Maker? By Whiteboard Crypto, What is Uniswap? By Whiteboard Crypto
- Lending and Borrowing: DeFi Series #1 - Decentralized Cryptoasset Lending & Borrowing by Binance Research (Calvin & Etienne), What is Aave? By Whiteboard Crypto
- Insurance: Why insurance is needed for DeFi, and what it looks like by Shane Neagle
- Derivatives: Crypto Derivatives, Lending, and a touch of Stablecoin by Gary Basin
- Yield Farming: What is Yield Farming? By Whiteboard Crypto, What is Impermanent Loss? By Whiteboard Crypto, What is a Liquidity Pool? By Whiteboard Crypto
- Flash Loans: What is a Flash Loan? By Whiteboard Crypto
- Money Legos: The True Power of DeFi: Composability by Oxjim
- DeFi 2.0: DEFI 2.0 - A New Narrative? OlympusDAO, Tokemak Explained by Finematics, What is OlympusDAO? By Whiteboard Crypto
- DeFi Exploits: How (Not) To Get Rekt – DeFi Hacks Explained by Jakub, Bank Run in DeFi by Finematics

What are NFTs? For the first time in our history, NFTs allow us to truly own the content we post online. The following resources discuss this fascinating space in more detail:

- Overview of NFTs: The Non-Fungible Token Bible: Everything you need to know about NFTs by Devin Finzer
- Why are NFTs Important: The Bull Case for NFTs by Jake Burkhman & Andrew Steinwold, Signaling as a Service by Julian
- Art: Rise Of A New Disruptor: How NFTs Are Revolutionizing The Art And Entertainment Worlds by Michael Golomb
- PFPs: 10 things to know about CryptoPunks, the original NFTs by Christie's, How Four NFT Novices Created a Billion-Dollar Ecosystem of Cartoon Apes by Samantha Hissong
- Sports: What is NBA Top Shot? Explaining the Blockchain NBA highlight collectables by Kyle Irving
- Virtual Worlds: Are We in the Metaverse Yet? By John Herrman and Kellen Browning

_____

_____

- Gaming: [How Gamers are Making a Living: A Case Study on Axie Infinity](#) by Benjamin Hor
- Utility: [Not just for kitties, punks, and top shots: NFTs will change everything we know about subscriptions, membership, licensing](#) by Matt Galligan
- Intellectual Property: [NFTs Reshape Brand Marketing In The Creator Economy](#) by Avi Dan
- Music: [Here's what NFTs are — and what they could do for the music industry, artists and fans](#) by Mikel Jollett, lead singer, Airborne Toxic Event, and author, "Hollywood Park"
- Financialization of NFTs: [Road to Financialization of NFTs](#) by Ishanee Nagpurkar

What are DAOs? A DAO is a blockchain-based organization that may replace the modern corporation. Unlike a traditional corporation, no single person or group owns or controls a DAO. Below are several resources that can help you understand this groundbreaking concept better:

- Why are DAOs Important? [DAOs: Social networks that can rewire the world](#) by Justin Mart & Connor Dempsey
- DAO Landscape: [DAO Landscape](#) by Coopahtroopa
- Investment DAOs: [What Is BitDAO and BIT Token?](#) By Bybit Learn
- Charity DAOs: [Philanthropy DAOs — The future of giving?](#) By Yonca Braeckman
- Collector DAOs: [ConstitutionDAO Hits $30M in Ethereum Raised, One Day Before Sotheby's Auction](#) by Kate Irwin
- Media DAOs: [Will DAOs revolutionize media or just create a playground for the rich?](#) By Leigh Cuen
- Service DAOs: [Service DAOs - Landscape, Challenges, and Solutions](#) by Terry Chung
- Social DAOs: [This Social Club Runs on Crypto Tokens and Vibes](#) by Erin Woo and Kevin Roose
- DAO Tooling: [Organization Legos: The State of DAO Tooling](#) by Nichanan Kesonpat
- How to DAO: [How to launch a DAO](#) by Lucas Campbell, [What Is It Like to Join a DAO?](#) By Aragon, [The Life of a Protocol Politician](#) by Coopahtroopah
- Legal Considerations: [A Legal Framework for Decentralized Autonomous Organization by David Kerr (Principal, Cowrie LLC) and Miles Jennings](#) (General Counsel, Crypto, Andreessen Horowitz), [The LAO: A For-Profit, Limited Liability Autonomous Organization](#) by The LAO

What are Smart Contract Platforms? Smart Contract Platforms are "world computers" that serve as the operational layer of Web3. Below are several resources that describe this phenomenon in more detail:

Smart Contract Platform Landscape:

- [The Smart Contract Platform Sector Explained](#) by Jodie Gunzberg
- [Layer-1 Platforms: A Framework for Comparison](#) by The Block Research
- [Mental Models for L1 and L1](#) by Patrick McCorry

Scalability:

- [Blockchains don't scale. Not today at least. But there's hope](#) by Preethi Kasireddy
- [Modular vs Monolithic Blockchains](#) by Ryan Sean Adams and David Hoffman
- [The DCS Triangle](#) by Trent McConaghy

_____

_____

- Blockchain Layer 1s Vs Layer 2 – Key Differences by Georgia Weston
- Proof of Work vs. Proof of Stake: Ethereum's Recent Price Surge Shows Why the Difference Matters by Miranda Marquit
- What is Sharding in Crypto? By Whiteboard Crypto
- What are Rollups in Crypto? By Whiteboard Crypto
- What are Sidechains in Crypto? By Whiteboard Crypto

Layer 1s:

- Ethereum 2.0 Upgrades Explained - Sharding, Beacon Chain, Proof of Stake by Whiteboard Crypto
- Solana: Solana Summer by Packy McCormick
- Terra: Terra: To the Moon and Back by Packy McCormick
- Avalanche: What Is Avalanche? A Look at the Popular 'Ethereum-Killer' Blockchain by Ekin Genç

Layer 2s:

- Layer 2 Scaling Solutions Explained by Whiteboard Crypto
- A beginner's guide on blockchain layer-2 scaling solutions by Cointelegraph
- Optimism by Packy McCormick
- Zero Knowledge by Pack McCormick
- Understanding Zero-knowledge proofs through illustrated examples by OxSage
- The Essential Guide to Arbitrum by Ben Give

What is the Metaverse? The metaverse is an interconnected network of virtual worlds that will replace the web as the primary way in which we access information. Read below to learn more:

- Overview of the Metaverse: Metaverse: A guide to the Next-Gen internet by Credit Suisse , The Metaverse: Web 3.0 Virtual Cloud Economies by Grayscale
- Why is the Metaverse Important? The Value Chain of the Open Metaverse by Packy McCormick
- Virtual Worlds: Riffs by Raph: How Virtual Worlds Work - Part 1 by Raph Koster
- Otherside: Otherside: Everything to Know About the New BAYC NFT Project by Langston Thomas
- Decentraland: Decentraland: Metaverse Land Boom Fueling MANA Token Growth by Grayscale
- Sandbox: What is The Sandbox by The Sandbox
- Virtual Economies: The Virtual Economy by L-Atelier
- Identity: Stay for Who You Can Be: Avatars in the Metaverse by Rex Woodbury

What is Web3s Infrastructure? The infrastructure of Web3 will differ from what we are used to today. Below are several resources detailing the core components of this new world:

- Overview of Web3 Infrastructure: The Architecture of a Web 3.0 application by Preethi Kasireddy, A simple guide to the web3 developer stack by Jonathan King, Connor Dempsey, & Hoolie Tejwani

_____

_____

- Decentralized Internet: Will Helium finally make IoT a reality? By Preethi Kasireddy
- Wallets & Identity: An Overview of the Crypto Wallet Landscape by Richard Chen, Your crypto wallet is the key to your Web3 identity by Michael Calce, Mapping the Web3 Identity Landscape by dommy.eth
- Providers: What is Infura? By Tim Copeland, Pocket Networks Investment Thesis by Dermot O'Riordan and Lior Messika
- Decentralized Storage: Web3 Storage — Massive Growth and Capital Gains with Arweave, Filecoin and Stratos by Huobi Research, An Introduction to Filecoin by Grayscale, Investing in the Permaweb by Kyle Samani
- Querying: Our investment in The Graph by Kyle Samani
- Oracles: What is the Blockchain Oracle Problem? by Chainlink, Blockchain Oracles Explained by Vallery Mou, An Introduction to Chainlink by Grayscale
- Shared Compute: Rendering the Metaverse by Kyle Samani
- Bridges: Blockchain Bridges: Building Networks of Cryptonetworks by Dmitriy Berenzon

What are Tokenomics?

If you want to make money investing in crypto, you need to understand tokenomics – the economic characteristics of crypto based economies. The best resources covering this topic are:

- Tokenomics 101, 102, 103 and 104 by Nat Eliason
- Tokenomics Blueprint by Longhash
- Tokenomics Deep Dive by Binance

What are the Challenges Faced by Web3? Like any disruptive technology, Web3 has its problems. The below articles discuss these in more detail:

- High Fees: Yes, Ethereum has a Gas Problem by Mike Fay
- Volatility: What Skeptics Get Wrong About Crypto's Volatility by Omid Malekan
- Environmental Concerns: Is Bitcoin Inherently Bad For The Environment? By Joshua Rhodes, FACT CHECK: Is Bitcoin mining environmentally unfriendly? By Coinbase, Bitcoin mining isn't nearly as bad for the environment as it used to be, new data shows by MacKenzie Sigalos
- Interoperability: The Interoperability Trilemma by Arjun Bhuptani, Blockchains Have a 'Bridge' Problem, and Hackers Know It by Lily Hay Newman
- MEV: Miner Extractable Value: the good, the bad & the ugly by Panther Team
- User Experience: I think there is a User Experience problem in Web3 by Mentie Omotejowho
- Crime: The Chainalysis 2022 Crypto Crime Report by Chainalysis

What are the Criticisms of Web3? Web 3 is not without its critics. Read some of the more popular detractors (as well as a few rebuttals) below:

- My first impressions of web3 by Moxie Marlinspike (Rebuttal: Vitalik Buterin via Reddit)
- Web3 by Scott Galloway (Rebuttal: The Web3 Debate by Packy McCormick)

_____

_____

- Line Goes Up – The Problem with NFTs by Folding Ideas (Rebuttals: Discussing the "Line Goes Up" NFT criticism video by Loopify and The line is not a line – the real problem with NFTs by The Defiant)

What are Pundits Predicting for Web3? There is no shortage of Web3 coverage by analysts and VCs. Read some of the more popular reports below:

- Introducing the 2022 State of Crypto Report by a16z Crypto (by Daren Matsuoka, Eddy Lazzarin, Chris Dixon and Robert Hackett)
- Crypto Thesis for 2022 by Messari

_____

_____

Appendix 4:   Brown Belt (1 Month)

Once you've consumed all of the resources in the "Purple Belt" section, it's time to deepen and broaden your understanding of key concepts, as well as start paying attention to developing trends in the space. You can do so by following the below roadmap:

1. **Deepen Your Understanding of Key Concepts:** While books on the crypto space are often dated the moment they are released, I still find them extremely helpful in gaining a deeper understanding of important concepts. My list of favorites (in rough order of preference) is below:

   - Token Economy by Shermin Voshmgir
   - The Internet of Money by Andreas M. Antonopoulos
   - How to DeFi: Basic by CoinGecko
   - How to DeFi: Advanced by CoinGecko
   - How to NFT by CoinGecko
   - The Sovereign Individual by James Dale Davidson and William Rees-Mogg
   - The Bitcoin Standard: The Decentralized Alternative to Central Banking by Saifedean Ammous
   - The Metaverse by Matthew Ball
   - Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World The Age of Cryptocurrency by Don Tapscott
   - Economics in One Lesson by Henry Hazlitt
   - The Network State by Balaji S. Srinivasan
   - Cryptoassets by Chris Burniske and Jack Tatar
   - A History of Money by Glyn Davies
   - Mastering Bitcoin by Andreas M. Antonopoulos
   - Creature from Jekyll Island by G. Edward Griffin
   - How to Bitcoin by CoinGecko
   - Digital Gold by Nathaniel Popper
   - Bitcoin Billionaires by Ben Mezrich
   - Proof of Stake by Vitalik Buterin
   - The Infinite Machine: How an Army of Crypto-hackers Is Building the Next Internet with Ethereum by Camila Russo
   - The Cryptopians by Laura Shin
   - Debt the First 5000 Years by David Graeber
   - Money: The Unauthorized Biography by Felix Martin
   - Bitcoin: The Future of Money? by Dominic Frisby
   - Bitcoin and Cryptocurrency Technologies by Arvind Narayanan et al

_____

2. **Broaden Your Understanding of the Space:** We've covered many of the high-level concepts in crypto above, but to the extent that you don't understand something, now is the time to fill the gap. As such, I would recommend reviewing the YouTube Channels of both Whiteboard Crypto and Finematics and watching any video on 1) a topic that you're unfamiliar with or 2) don't understand well. These videos are generally 10 – 20 minutes max and they break things down well.

    (Note: if you're more of a podcast person you can also do the same on Bankless or Unchained)

3. **Stay Updated on Current Developments**: Like with learning any topic in business or technology, it's always helpful to stay on top of the news. As such, you can find a couple of my favorite news and research sources here. But what's infinitely more helpful, in my opinion, is to follow the top accounts on "crypto twitter". Many of these accounts provide breaking news and very thoughtful commentary (although you often have to take a contrarian mindset and do your own research, as everyone is wrong from time to time and many accounts are, unfortunately, paid to hype projects). A list of my favorite twitter accounts can be found in Appendix 7.

_____

Appendix 5:   Black Belt (1 Year)

Web3 has become a very complicated space. Over the last several years it has split into several verticals – such as cryptocurrencies, DeFi, NFTs, DAOs, smart contract platforms and the metaverse – and, as of July 2022 there are over 20,000 cryptocurrencies in circulation and thousands of NFT projects.

As such, truly starting to get your arms around the space will likely take at least a year. If you're up for it – and you've read all of the White, Blue, Purple and Brown Belt sections above – I would recommend the following:

1. **Study Reading Lists and Canons:** There is no shortage of curated reading lists (often called "canons") on crypto. Some of these resources can each contain dozens to hundreds of dense articles and, as such, **could take weeks or months to finish**. While getting through a canon can be a ton of effort, in my opinion it's well worth it if you want to truly start to learn. Some of my favorites include:

   - a16z's Crypto Canon
   - Bankless's Getting Started Guide
   - a16z's NFT Canon
   - a16z's DAO Canon
   - a16z's Zero Knowledge Canon
   - Gabby Goldberg's Web3 Reading List
   - Richard Chen's Crypto Reading List
   - Jon Radoff's Metaverse Canon
   - Packy McCormick's Tokenomics Reading List
   - Rabbit Hole's Governance Library
   - CoinGecko's How to DeFi Basic and Advanced Books have a great bibliography with a ton of good DeFi reads
   - Coinbase Learn
   - Binance Academy

2. **Take a Few Courses:** For those that excel in an academic environment, there are several free or relatively cheap courses available. A list of popular courses is included in Appendix 11.

3. **Read Whitepapers**: In my experience as a VC, after you have a solid understanding of the "top-down" dynamics of a space, one of the best ways to master it is through a "bottoms-up" approach, by learning about of its key players, companies and projects. As such, I'd recommend reading as many whitepapers – the official documentation about what a project does and how it works – as you can. I'd recommend starting with projects you are interested in, but if you need a little nudge then research the dozens of protocols that I mention in my articles. Most projects whitepapers can be found on their website or through a simple Google search.

_____

_____

4. **Gain Practical Experience:** The absolute best way to understand Web3 is to experience it first-hand. Make a loan on Aave, a trade on Uniswap, buy a few NFTs, join a DAO, try out the metaverse, use a bridge, etc…

   • If you are unsure where to start, check out Rabbithole, a website that pays you in crypto for performing simple Web-3 related tasks (such as buying an NFT, taking out a loan on Aave or voting in a DAO)

   • Join a DAO and participate!

   • Get a job in Web3

5. **Keep Up with the News:** As discussed, crypto moves very fast, so it's important to keep on top of trends by reading the news, following key Twitter and Reddit accounts and even paying for research. I've listed my favorite Twitter accounts and subreddits in Appendix 7 and Appendix 8.

6. **Free Sources**: Some of the absolute best sources to keep on top of crypto news are free. You can find a list of these accounts in Appendix 10.

7. **Paid Sources**: While expensive, paid sources can be worth it in that they provide deep analysis on projects, verticals and trends (in fact, many of my favorite articles come from paid sources, but I tried not to include them in earlier sections because I wanted to keep the focus on free resources as much as possible). My favorite paid sources include: Messari, The Block and Delphi Digital

_____

_____

Appendix 6:   Red Belt (Lifetime)

While it's possible to get very solid understanding of Web3 and crypto in a year, truly "mastering" the subject will take a lifetime. There's simply too much going on in the space, and the technology is too disruptive, to require anything less.

If you do want to dedicate your life to the study of Web3, however, I'd recommend taking the following steps:

1. **Broaden Your Horizons:** One of the reasons that crypto is so hard to understand is that it's interdisciplinary and requires understanding of politics, economics, computer science and cryptography. If you are weak in any of these areas, then it will be difficult to understand what's truly going on (in fact, most skeptics I've met tend to be experts in one field but neophytes in the other). Dhruv Bansal explains this perfectly in [Why It's Hard to "Get" Bitcoin: The Blockchain Spectrum](#) and recommends studying the following subjects:

Understanding Crypto Requires as Mastery of Multiple Disciplines
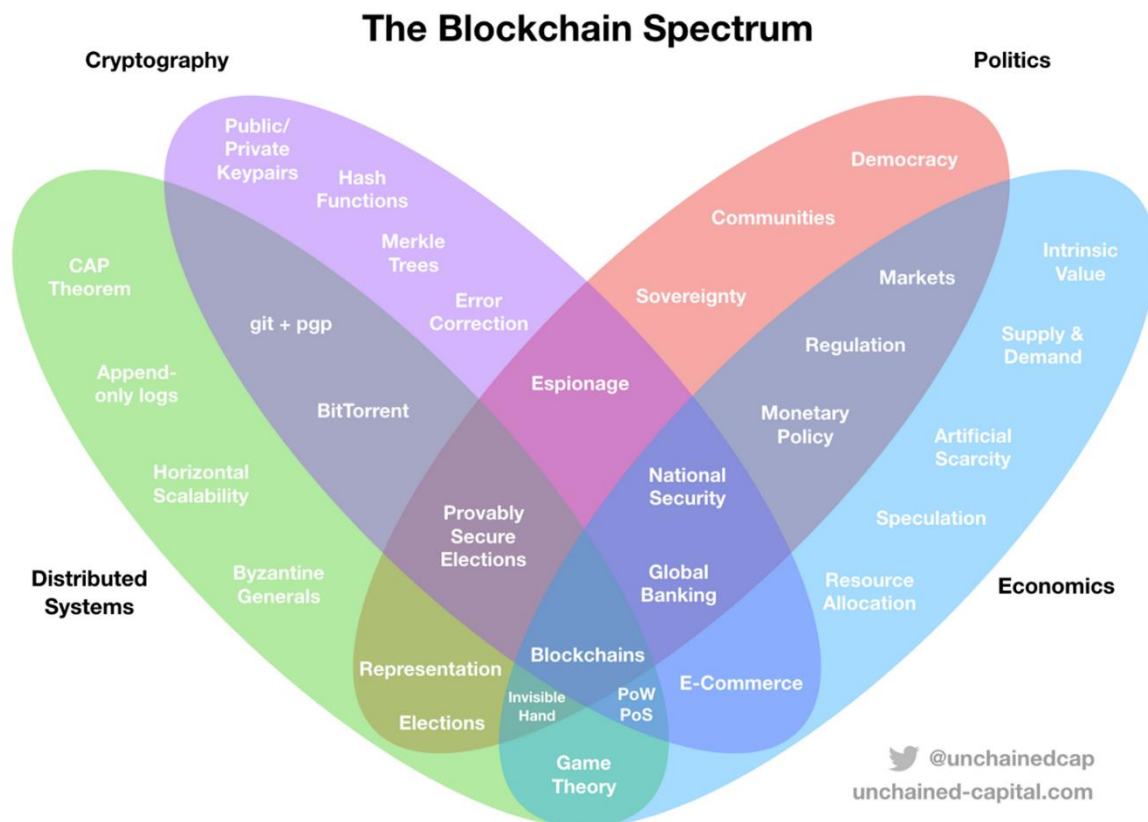
Source: [Unchained](#)

_____

_____

2. **Learn to Code in Solidity (or Rust, Move, etc…):** I've spent most of my career on the "qualitative" side of business, learning strategy, marketing, sales, operations, finance, legal, etc… While that helped me understand crypto reasonably well, I didn't really break through until I spent a year learning to code. Becoming a programmer (especially in Solidity) is extremely helpful as it gives you a very clear understanding of how the web truly works today and why crypto is so much better (and of course, learning to code also gives you a much deeper understanding of how decentralized applications function). If you'd like to learn more, I'd recommend the following resources:

- Learn Web3 DAO
- Cryptozombies

3. **Invest!:** One of the best ways to improve your understanding of Web3 is to "put your money where your mouth is". While I'm not giving specific investment advice, I am saying that investing helps sharpen your knowledge – it forces you to think analytically about a protocol and what problem it's solving, dive deep into the technical architecture and tokenomics and gain a thorough understanding of the founders and community. Some of the best lessons, in fact, come from the losses – as they'll give you a sense of what works in Web3 and what doesn't. If you want to become a better investor, I'd suggest that you do the following:

- Pay attention to sources such as Twitter and Reddit to get a feel for developing trends and projects
- Read whitepapers and do your own independent analysis (again, it's very important to never take the word of any "expert" – no matter how knowledgeable they seem I can pretty much guarantee you that they are wrong as often as they are right)
- Go to conferences, network with other investors and join crypto investing groups
- If you can afford it, subscribe to paid research sources. Some of my favorite include Messari, The Block and Delphi Digital
- Follow a project on Twitter, join its Reddit and Discord groups, participate in its DAO (if applicable) and even meet the founders if possible

Last, and perhaps most important, if you want to master the space I'd recommend making it your career. Volunteer for a DAO, get a full-time gig at a Web3 project or, even better, found your own!

_____

_____

Appendix 7: Twitter

Below is a list of my 50 favorite follows on Crypto Twitter (ranked by subscribers, not necessarily in order of preference):

Name	URL	Followers
Vitalk Buterin	https://twitter.com/VitalikButerin	4.2M+
Naval	https://twitter.com/naval	1.8M+
Chris Dixon	https://twitter.com/cdixon	876K+
Andreas Antonopoulos	https://twitter.com/aantonop	746K+
Cobie	https://twitter.com/cobie	734K+
Balaji Srinivasan	https://twitter.com/balajis	680K+
Lyn Alden	https://twitter.com/LynAldenContact	506K+
Punk 6529	https://twitter.com/Punk6529	396K+
Nic Carter	https://twitter.com/nic__carter	347K+
Farokh	https://twitter.com/farokh	316K+
ZachXBT	https://twitter.com/zachxbt	287K+
Ryan Selkis	https://twitter.com/twobitidiot	275K+
Cozomo De' Medici	https://twitter.com/CozomoMedici	268K+
Route 2 Fi	https://twitter.com/Route2FI	262K+
Chris Burniske	https://twitter.com/cburniske	238K+
Ari Paul	https://twitter.com/AriDavidPaul	221K+
Laura Shin	https://twitter.com/laurashin	217K+
The Defi Edge	https://twitter.com/thedefiedge	209K+
Ryan Sean Adams	https://twitter.com/RyanSAdams	202K+
Larry Cermak	https://twitter.com/lawmaster	188K+
Tascha	https://twitter.com/TaschaLabs	174K+
Packy Mccormick	https://twitter.com/packyM	167K+
Coopatroopah	https://twitter.com/Cooopahtroopa	162K+
David Hoffman	https://twitter.com/TrustlessState	161K+
Linda Xie	https://twitter.com/ljxie	154K+
Frank Chaparro	https://twitter.com/fintechfrank	150K+

_____

Cantino.Eth	https://twitter.com/chriscantino	136K+
Mike Dudas	https://twitter.com/mdudas	123K+
Nader Dabit	https://twitter.com/dabit3	120K+
Preethi Kasireddy	https://twitter.com/iam_preethi	112K+
Jack Niewold	https://twitter.com/JackNiewold	110K+
Matthew Ball	https://twitter.com/ballmatthew	107K+
Matt Huang	https://twitter.com/matthuang	104K+
Misha	https://twitter.com/mishadavinci	94K+
Cami Russo	https://twitter.com/CamiRusso	88K+
Cathy Hackl	https://twitter.com/CathyHackl	69K+
Katherine Wu	https://twitter.com/katherineykwu	68K+
Ryan Watkins	https://twitter.com/RyanWatkins_	67K+
Humble Defi Farmer	https://twitter.com/PaikCapital	64K+
Jessie Walden	https://twitter.com/jessewldn	51K+
Rex Woodbury	https://twitter.com/riabhutoria	32K+
Kinjal Shah	https://twitter.com/_kinjalbshah	31K+
Daniel Cheung	https://twitter.com/highcoinviction	28K+
Eshita	https://twitter.com/eshita	21K+
Bobby Bananas	https://twitter.com/BobbyBananasNFT	18K+
Jason Hitchcock	https://twitter.com/JasonHitchcock	18K+
Tory Green	https://twitter.com/mtorygreen	16K+
Paul Veradittakit	https://twitter.com/veradittakit	15K+
Jon Radoff	https://twitter.com/jradoff	12K+
Lisa Jy Tan	https://twitter.com/lisajytan	8K+

Appendix 8:   Reddit

While I personally prefer Twitter for breaking news and trends, Reddit communities can also be a powerful source of alpha if you know where to look. When you're deeper along in your crypto journey and looking into specific projects, I highly recommend joining their reddit pages.

If you're looking for more general industry discussion, here are a few popular subreddits:

Subreddit	Members	Description
r/CryptoCurrency	5.3M	General forum for cryptocurrency news, discussion and analysis
r/Bitcoin	4.5M	Official subreddit of Bitcoin
r/Ethereum	1.4M	Official subreddit of Ethereum
r/BitcoinBeginners	1.1M	Subreddit for newcomers to ask Bitcoin related questions
r/CryptoMarkets	1.0M	Forum to discuss cryptocurrency trading, especially technical analysis
r/Cryptotechnology	674K	Subreddit dedicated to highly technical discussions of blockchain technology
r/Satoshistreetbets	631K	Modeled after the famous Wall Street Bets, Satoshi Street Bets is a subreddit for crypto trading
r/NFT	497K	Subreddit to discuss NFT trends, projects and news
r/CryptoCurrencies	375K	General news and discussion source for crypto
r/Altcoin	220K	Forum to discuss all coins other than BTC
r/Opensea	162K	Subreddit for NFT marketplace Opensea

r/Defi	103K	Forum to discuss project ideas, articles, events, questions, support and other topics related to DeFi
r/Ethdev	96K	Forum for Ethereum developers to discuss technical topics
r/Crypto_General	71K	General discussion related to the crypto space
r/Metaverse	38K	Subreddit for discussion of metaverse - related topics
r/Web3	23K	Discussion of trends and projects related to Web3
r/Dao	6K	Discussion of architectural principles of DAO creation

_____

Appendix 9: Podcasts

While I'm not a huge podcast fan, I do listen from time to time as hearing directly from thought leaders can provide a unique and valuable perspective.

I know that others are die hard podcast fans, so wanted to list a few of the more popular crypto-focused resources below

Podcast	Episodes	Score	Ratings	Description
Coindesk Podcast	1,254	4.8	574	General cryptocurrency news and trends
The Token Metrics Podcast	1,246	4.0	88	News, analysis and investment strategies from the Token Metrics team
The Bad Crypto Podcast	709	4.6	999	General discussion on the cryptocurrency space
Decrypt Daily	677	4.7	241	Breaking news and general crypto updates
Crypto 101	489	4.3	703	General cryptocurrency discussion
Epicenter	488	4.7	181	Provides in-depth discussions about the technical, economic and social implications of crypto
Bankless	476	4.8	809	Podcast discussing the crypto space with a focus on DeFi
Unchained	403	4.6	1,100	Laura Shin's deep dive into the crypto markets
Unconfirmed	169	4.7	268	Another Laura Shin podcast, Unconfirmed provides a much quicker overview of the top crypto news and trends
Flippening	117	4.9	232	Podcast for crypto investors
Moon or Bust	102	5.0	4	Focus on altcoins and DeFi (hasn't been updated since Jul 29th 2022)
GM NFTs on Rug Radio	75	5.0	1	NFT-focused podcast

_____

_____

Appendix 10: News and Research

While I think that the best way to keep on top of breaking trends in the crypto space is through Twitter and Reddit, there are some "traditional" news sources that do an excellent job of covering developing trends.

I'm particularly fond of sites such as The Block and Messari that provide in-depth, Wall Street quality research (albeit at a fairly hefty sum).

Below are some of the more popular news sites in crypto:

Site	Monthly Visitors (1)	Description
CoinDesk	10.5M	The largest general cryptocurrency news site
Cointelegraph	9.3M	Provides breaking news in the crypto space
Decrypt	4.0M	General crypto focused news and analysis
The Block	2.5M	Provides enterprise-grade, in-depth research (akin to The Information for crypto)
Messari	1.6M	Detailed, Wall Street-grade research on cryptocurrency projects
The Defiant	0.4M	DeFi, Ethereum and Web3 news
NFT Now	0.4M	Provides research and news on the NFT space
Bankless	0.3M	Web3 news with a focus on DeFi
Delphi Digital	0.1M	Research on cryptocurrency projects and verticals
NFT Lately	NA	Newsletter focusing on the latest NFT news
Unchained	NA	Laura Shin interviews the top players in crypto and provides in-depth analysis

(1) Source: Similarweb

_____

Appendix 11: Courses

Course	Provider	Description
Bitcoin and Cryptocurrencies	Berkeley	Developer-focused course teaching the fundamentals of Bitcoin, Ethereum, the basics of smart contract platforms and the building of decentralized applications. Course is 6 weeks at roughly 3-5 hours per week
Bitcoin and Cryptocurrency Technologies	Princeton University	One of the earliest and most popular introductory courses taught by Arvind Narayanan. Takes roughly 23 hours to complete
Bitcoin and Fintech	The University of Hong Kong	Introductory course on the implications of blockchains on Fintech. Course lasts six weeks and requires 3-4 hours per week
Blockchain Analystics Course	Metrics DAO	Course teacher users how to gather and analyze on-chain data
Blockchain and Money	MIT	Introduction to Cryptocurrencies taught by Gary Gensler (Chairperson of the SEC)
Blockchain Specialization	Coursera	Intermediate level course from Coursera, requiring approximately 17 hours to complete
Cryptocurrency Class 2022	Patrick McCorry	Highly technical 8-week class from Patrick McCorry, an engineer at Infura
Cryptocurrency Engineering and Design	MIT	Technical overview of cryptocurrencies from MIT
Decentralized Finance	Berkeley	12-week deep dive on DeFi from UC Berkeley
Introduction to Cryptocurrencies and Blockchain by Udemy	Udemy	Relatively short (2 hours of video) introductory course on Udemy
Introduction to NFTs and the Metaverse	University of Nicosia	Overview of NFTs and the Metaverse taught by Punk6529 with several prominent guests (such as Fred Wilson, Chris Dixon and Yat Siu). This is a relatively new course that will span 12 weeks
Token Engeinering Fundamentals	Token Engineering Academy	100-hour course focused on tokenomics, governance and the technical design of tokens

_____

Appendix 12:   Data Sources

While it's important to stay on top of the news, follow key twitter and reddit accounts and learn as much as you can by consuming books, articles, videos and podcasts, if you really want to get ahead you need to do your own diligence.

One of the great things about the crypto space is that virtually all the data you need is publicly available on-chain and accessible 24/7.   You can see how many users a project has, how much they are transacting, what the top wallets are doing, who's trying to squeeze projects through MEV, etc… This allows you to monitor the space in real-time, perform your own analysis and develop your own insights.

While the ideal way to do this will always be directly through the block explorers of each project, that's not always practical and, as such, many investors and researchers use data aggregation tools.

In the following section, I provide a list of the most popular tools, categorized by:

- General Market Information: Sites that provide high-level market information such as prices, volume, marketcap, etc…
- Industry Information: Sites that provide detailed industry analysis, such as NFT sales, TVL locked in DeFi, virtual land sales, etc…
- On-Chain: Sites that provide detailed on-chain analytics, ranging from # of addresses, address growth, transaction volume, fees, MEV tracking, etc…
- Block Explorers: Block explorers for the Layer 1s
- Social: Provide tools for sentiment analysis such as Reddit subscribers, social dominance, etc…
- Technical: Provides information on developer activity, security vulnerabilities, decentralization, etc…
- Tokenomics: Sources that relevant information on upcoming ICOs, token unlocking schedules, wallet tracking, etc…

I've highlighted the resources I personally use most frequently in green.

Keep reading to learn more…

_____

_____

General Market Information

Site	Description
CoinDance	Bitcoin statistics
CoinGecko	Cryptocurrency prices, charts and market caps
CoinMarketCap	Provider of high-level stats such a price, volume, market cap, etc…
Cryptorank	General market information for cryptocurrencies
MDX_ALGO	General market analytics
Messari	Provides a variety of metrics for hundreds of tokens as well as best-in-class research

_____

_____

Industry Information

Site	Specialty	Description
APY Vision	DeFi	Allows users to find the most profitable liquidity pools and track performance
Coindix	DeFi	Monitors 10K+ vaults on 63 protocols across 27 chains
DeFi Llama	DeFi	Go-to source for TVL information
DeFi Pulse	DeFi	Ranking of top projects by TVL
Laevitas	DeFi	Derivatives tracking
Parsec	DeFi / NFT	Professional grade DeFi and NFT analytics
Dapp Radar	Decentralized Applications	Provides overviews of the top decentralized applications by chain
DAO Masters	DAO	Detailed overview of the top daos and top dao tools
DeepDAO	DAO	Provides overall DAO statistics as well as organization-specific information such as treasury size, members, etc…
Tally	DAO Governance	Tracks active governance proposals across a variety of DAOs
L2beat	Layer 2	Provides market share of the top L2 protocols
Metacat	Metaverse	Virtual real estate information
WeMeta	Metaverse	Provides detailed information virtual worlds and digital land sales
Cryptoslam	NFT	Extremely detailed analysis of the NFT market activity by chain and project
Flips Finance	NFT	Tracks important NFT data
NFTGo	NFT	All-in-one NFT analytics platform
NFT Nerds	NFT	Analytics for the NFT market
Nonfungible	NFT	NFT market stats and rankings
Web3 Index	Web 3 Infrastructure	Tracks demand-side metrics (e.g. fees) for a variety of infrastructure projects

_____

_____

On-Chain

Site	Description
Coin98 Analytics	Provides a variety of reports across different veriticals (DeFi, Web3, Smart Contract Platforms) in very easily digestible graphical formats
Coinmetrics	Provides a variety of detailed metrics (e.g. address growth, fees) for projects such as BTC, ETH and LINK
Dune Analytics	Contains user-generated metrics gained from on-chain data
EigenPhi	MEV tracker and analysis tool
Footprint Analytics	Tracks on-chain data across 17 chains and 80K+ NFt projects
Glassnode	Provides detailed on-chain data and analysis
Nansen.ai	Enterprise-level analytics
Santiment	Enterprise-level analytics across a variety of categories (including sentiment analysis)
The Block	Provides a variety of metrics for hundreds of tokens as well as best-in-class research
TokenTerminal	Tracks several on-chain metrics across a variety of projects (including revenue)
ZeroMEV	Tracks MEV

_____

_____

Block Explorers

Site	Description
Avalanche	Block explorer for Avalanche
BSC	Block explorer for BSC
Cardano	Block explorer for Cardano
Cosmos	Block explorer for Cosmos
Ethereum	Block explorer for Ethereum
Near	Block explorer for Near
Polkadot	Block explorer for Polkadot
Polygon	Block explorer for Polygon
Solana	Block explorer for Solana
Tron	Block explorer for Tron

_____

_____

Social

Site	Description
LunarCrush	Analyzes social trends and provides sentiment analysis
Subredditstats	Provides historical reddit subscriber figures

_____

_____

Technical

Site	Description
CryptoMiso	Ranks projects based on developer activity
DeFi Safety	Provides detailed technical audits and provides scores for several top projects
Nakaflow	Provides nakamoto coefficients for several projects

_____

Tokenomics

Site	Description
EtherDrops Bot	Bot that tracks specific wallets and sends notifications via telegram
ICO Drops	Provides a calendar of upcoming ICOs
Token Unlocks	Tracks token unlocking schedules

Other

Site	Description
Chainalysis	Provides detailed data on trends in crypto "crime" including hacks, rug pulls, etc…

About the Author

_____

My Journey Down the Web3 Rabbithole...

I'm an operationally-focused VC. This means that in addition to investing, I also spend much of my time helping our investments grow by taking on interim COO, CFO and even CRO roles. If you're interested in the full details of my professional background, you can check them out on LinkedIn (but you will probably find more value by following me on Twitter 😊).

In 2015 I was working with one of these companies – an early blockchain startup – and the founder started to teach me about crypto. At that point in my life, I had barely heard of Bitcoin, had no idea how a blockchain functioned and – despite having a background in economics – did not truly understand how the global financial system worked.

But the CEO said something that stuck with me:

"Blockchains are how everyone thinks the internet works but actually doesn't".

That opened my eyes and I started to see the world as it really was. I saw how central governments manipulated the money supply, how banks could restrict and even seize our assets, how corporations abused their power and how "Big Tech" dictated the terms of our digital lives and got rich off of our data.

Despite living in a "capitalist democracy", I realized that we really weren't all that free.

But I was shown that blockchains offered a better way – that they were more than just a new form of "money" or the "next iteration of the internet". They were a tool that could drastically re-engineer human society. An invention that comes along once in a millennium – like writing or the printing press – that could give us true freedom and autonomy.

Once this passion was ignited, there was no stopping it.

Over the next several years I spent almost all of my time learning as much as I could about crypto. I invested in projects, met people in the space, learned how to code so I could build my own blockchains and decentralized apps and – most importantly – consumed every book, article, video and podcast I could find on the subject.

Unfortunately, while there is a ton of great material out there, I found that most of the time it was pretty scattered and disorganized. You can find individual canons on DeFi, DAOs, NFTs, cryptocurrenices, etc… but nothing that ties it all together.

This is unfortunate because each of these seemingly separate crypto "verticals" combine to form something way more powerful than the parts.

They're creating the first truly sovereign digital economies, and perhaps the first digital nations. Online states that can survive outside of the purview of governments, banks and Big Tech because they have their own money, financial system, goods and laws.

And that's why I wanted to create this book – it's my humble attempt to summarize what I've learned by putting it in writing, and also to share the best resources I've found on Web3.