MONEY, BLOCKCHAIN, CRYPTO, NFT & DAO

PRIMER COMPILATION

COMPILED BY ANAHATA DAO

Contents

Introduction To The Exponential Age

We're about to go through the fastest period of technological adoption of recorded human history in the next 5-10 years, and nobody is prepared for it. Crypto is like a hyper-charged, new version of the internet!

Humans are simple creators, we think in linear terms, we can't understand exponentiality, it's just not something that suits our brains.

Let's focus on crypto thought, the internet between 1990 and 2000 experienced its fastest period of growth from low numbers to large numbers. That period the internet grew 60% per year, which was the fastest adoption of any technology in all recorded human history, much faster than the mobile phone that came before it. These are network businesses; we'll return to this important concept soon.

In contrast, crypto is growing at 113% a year and it currently has the same number of users as the internet had back in 1997. People keep saying the dotcom crashed and it was disastrous, well it wasn't because out of that came Facebook, Google, Amazon, you name it. It was the start; it wasn't the end. Crypto is growing at 113% a year which is nearly double the growth of the internet, the fastest adoption of all recorded history. That is exponential growth.

We are at about 114 million users as of 8/2021 of Crypto worldwide and if you lower the growth rate from 113% to 83% (to be slightly conservative, Crypto will hit 1 Billion users by 2024, that's just three years from now, it's hard to wrap our heads around this but that's how fast it's growing. It will basically get us to 3.5 billion users by about 2027.

What is causing this extraordinary adoption? The adoption is a network of money and all of finance, in fact it's a network of value that sits above the internet. It connects all of this digital world, in a way that the value is transferable, storable, ownerable and recordable. This is the world of everything, starting from Bitcoin. We have developed a new business model - network model.

Network business models started from mobile phone companies, then you have the network business models of Facebook, Google, Twitter, Reddit etc. who started using behavioral economics combined with data, creating a network of people that were incentivized to post more, share more, like more, do things more. Now, for us as users of these social networks, we got the benefit of finding our old school friends, keeping contact with your cousin and all those things you use it for, the shareholders got rich, we didn't. In fact, they took the economics from us, by monetizing our eyeballs and attention.

Then comes Bitcoin in 2008, and you've got something super powerful; a network where the users of the network have bitcoin, so the value of the network is bitcoin, so it becomes a network like no-other with all behavioral incentives aligned, where everybody is incentivized to grow the network. Bitcoin starts the whole process and everyone realizes that this business model works for almost everything and this gives rise to NFTs, DEFI, social tokens and so much that is going on. This is all happening at the same time; as AI, robotics, autonomous vehicles, EV technology, genetic sciences, distributed computing power, space "Wi-Fi" are all going mainstream exponentially at the same time, and they're all connected and driven by networks. Humanity has not dealt with this before, which has caused fear in some because their value system is changing.

Theory and Brief History of Money and Banking – Pre-Cryptocurrency Age

What is Money?

- The ultimate purpose of this section is to give the reader a solid grasp of how money works in today's world. We should first provide a general framework giving the basic theory or "economic logic" of money and banking.
- In short: Why do we have money in the first place? Where does it come from, and what determines its form (livestock, metal ingots, coins, paper notes, electronic ledger entries, etc.)? What qualities make for a good money?
- The Limits of Direct Exchange
    - In a world limited to barter, or what economists more precisely call direct exchange, there would still be private property and people would still benefit from voluntary trade. Because economic value is subjective—the "utility" of a good is in the eye (or mind) of the beholder—we can have win-win exchanges, in which both parties walk away correctly believing that they got the better end of the deal.
    - However, if society were limited to direct exchange—in which individuals only accept items in trade that they plan on using personally—then people would miss out on many advantageous transactions.
        - Let's consider a simplistic example. Suppose there are three individuals: a farmer, a butcher, and a cobbler. The farmer starts out with some eggs that he's just taken from his hens. He would like to trade his eggs in order to get his tattered shoes repaired. The problem, though, is that the cobbler doesn't want any eggs—but he would be willing to repair the shoes for bacon.
        - Unfortunately, the farmer doesn't currently have bacon. However, his neighbor the butcher does have bacon. Yet the butcher doesn't want to trade with the cobbler, because the butcher's shoes are just fine. What the butcher would really like are some eggs. Yet, the farmer himself doesn't like the taste of bacon, and would rather eat his own eggs.
        - In a world limited to direct exchange, these men are at an impasse, because no single transaction would benefit any pair of them. Yet all of them could improve their situation with a rearrangement of the goods.
    - The solution is to introduce indirect exchange, in which at least one person accepts an item in trade that he doesn't plan on using himself but holds merely to trade away again in the future. In our example, suppose that the farmer has an epiphany: Even though he personally dislikes its taste, he trades his eggs to the butcher to obtain the

bacon. Then he takes the bacon to the cobbler, who accepts it as payment for fixing his tattered shoes.

    - After these two trades, all three individuals are better off than they were originally. Remember, though, that the solution relied on the farmer accepting an item in trade—in this case the bacon—that he didn't plan on using himself. Economists call such a good a "medium of exchange". Just as air is a "medium" through which sound waves travel, the bacon served as a medium through which the farmer's ultimate exchange was effected—namely giving up his eggs in order to receive shoe-repair services.

- Media of Exchange and the Origin of Money
    - Individuals can often improve their position by trading away goods that are less marketable and accepting goods that are more marketable, even if they don't personally plan on using the items. This principle is all we need to explain the emergence of money.
    - As individuals in the community seek to trade away their less marketable (or less liquid) goods in exchange for more marketable (or more liquid) goods, a snowball process is set in motion: those goods that started out with a wide appeal based on their intrinsic qualities see a boost in their popularity simply because they are so popular.
    - Eventually, one or two commodities become so popular that just about everyone in the community would be willing to accept them in trade. At that point, money has been born.
    - A formal definition for money is that it's a universally accepted medium of exchange.
        - Founder of Austrian School of Economics Carl Menger's explanation showed how such a commodity could emerge from its peers merely through voluntary transactions and without any individual seeing the big picture or trying to "invent" money.
- The Qualities of a Good (Commodity) Money
    - Money that emerged in the process described would necessarily be commodity money, in which the monetary good itself is also a regular commodity. Historically, many types of commodities have served as money in various regions, including livestock, shells, tobacco, and of course the precious metals gold and silver.
    - What would make a community gravitate towards some commodities but not others? Besides having a wide marketability, an individual would want a medium of exchange to possess the following qualities: ease of transport, durability, divisibility, homogeneity, and convenient size and weight for the intended transactions.
        - Keep these qualities in mind as you learn about cryptocurrencies.

    - In our example, although bacon served as the medium of exchange, it would be ill-suited to serve this purpose generally, as bacon is perishable. Likewise, a shotgun might be very valuable in certain communities, but it's not divisible; you can't cut it in half to "make change." Diamonds might seem like a great candidate for a medium of exchange, but they aren't homogeneous: one giant diamond is more valuable than five smaller diamonds that (combined) weigh the same amount.
    - These types of considerations help explain why eventually gold and silver emerged as the market's commodity monies of choice.
        - These precious metals satisfied all of the criteria of what makes a convenient medium of exchange, and once the community generally agreed, they were money.
- Monetary Calculation
    - The emergence of money meant that a single commodity was on one side of every transaction. This greatly reduced the calculations required to navigate the marketplace. For example, consider a merchant whose business required him to closely follow twenty different goods. In a world of pure barter—where each good traded directly against every other good—in principle he would have to keep track of 190 separate barter "prices" (meaning the ratios at which one good traded for another). But if one of those twenty goods also serves as the monetary good—maybe it's silver—then the merchant only needs to keep track of nineteen different prices (all quoted in silver), because each of the other goods is always being bought and sold against silver.
    - Moving from a state of barter to a monetary economy allows for economic decisions to be appraised in terms of a standard unit. With the use of money, participants of an ecosystem can engage in accounting, where they can easily calculate whether they had a profitable year. Trying to compare revenues to expenses would be much more difficult in a pure barter system.
- The Function of Monetary Coins (and Tokens)
    - We have seen how a commodity money can emerge spontaneously from a prior state of barter, facilitating exchanges and profit/loss calculations. However, even though a community benefits tremendously from the existence of money, there would still be limitations if the money remained in its "raw" form. It would hamper trade if shopkeepers had to perform metallurgical tests on hunks of metal that customers presented for payment to verify that the hunks were indeed silver (or gold, etc.) of the claimed weight.

- The solution to this problem is to coin the raw hunks of metal into recognizable disks of a uniform size and purity (or "fineness"). We should emphasize that a full-bodied coin was not money because of the stamping process; the markings on the coin merely indicated to the community that the hunk of metal in question did indeed contain the specified weight in the underlying commodity that served as money.
- In addition to striking full-bodied coins, another possible solution is for reputable outlets to issue token coins, which represent redemption claims on the issuer for a specified amount of the actual money commodity. Note that to perform their function well, even token coins would need to be recognizable in the community and difficult to counterfeit.
    - For example, consider the plastic chips issued by casinos: A Las Vegas casino needs to have chips that are distinctive and "authentic"-looking, and which can't be easy for outsiders to replicate. Because such chips will be instantly redeemed by the casino, within its walls (and even perhaps in the surrounding neighborhood) they are "as good as money." But a gambler who travels back home wouldn't be able to buy groceries with chips issued from a Las Vegas casino.
- Just as the money itself can arise without the intervention of political authorities, so too can the non-public sector handle the operations of turning commodity money into coins.

The Function and Origin of Banks

- Even in a community with commodity money stamped into high-quality coins, there would still be limitations on commerce. For example, wealthy individuals would be nervous about holding vast sums of gold or silver in their homes where they would be vulnerable to theft, and it would be inconvenient to transport large amounts of coin or bullion for every transaction involving a significant purchase price.
- A bank solved these problems by providing a secure location where members of the community can store their excess supplies of money. (The other main function of banks is to serve as credit intermediaries, which act as a conduit between borrowers and savers.)
    - The goldsmith was a logical person to also act as banker, because his business already involved storing stockpiles of gold. It was easy enough for members of the community to deposit coins with the goldsmith in exchange for an official receipt indicating how much of the money commodity they (the depositors) had stored with him.
- It started with goldsmiths. As early bankers, they initially provided safekeeping services, making a profit from vault storage fees for gold and coins deposited with them.

People would redeem their "deposit receipts" whenever they needed gold or coins to purchase something, and physically take the gold or coins to the seller who, in turn, would deposit them for safekeeping, often with the same banker.

    - Everyone soon found that it was a lot easier simply to use the deposit receipts directly as a means of payment. These receipts, which became known as notes, were acceptable as money since whoever held them could go to the banker and exchange them for metallic money.

- Then, bankers discovered that they could make loans merely by giving their promises to pay, or bank notes, to borrowers. In this way, banks began to create money.
    - More notes could be issued than the gold and coin on hand because only a portion of the notes outstanding would be presented for payment at any one time. Enough metallic money had to be kept on hand, of course, to redeem whatever volume of notes was presented for payment.
- Once the banker (such as the goldsmith) realized that his deposit receipts ("notes") were treated by at least some members of the community as being "as good as money," he could lend out some of the coins that his customers had deposited with him, even though the customers still held paper receipts entitling them to immediate redemption.
    - The whole operation was viable so long as the banker always had enough coins on hand to satisfy whoever might show up to demand their deposits back.
- In the typical scenario, this is the type of deposit applicable to money; the people handing over coins to the goldsmith didn't care about receiving back those particular coins, they merely wanted to be assured of obtaining the same number of comparable coins when they redeemed their deposit receipts (i.e., banknotes).
- As a result of various court rulings, it is now standard to treat the deposit of money with a bank as a loan, so that the depositor becomes a creditor of the bank and the actual ownership of the money transfers to the banker, even for "demand deposits," which are payable upon notice.
    - Rightly or wrongly, it is this legal treatment that allowed the proverbial goldsmith to lend out some of the coins that his depositors had placed with him for safekeeping, and which allows modern banks to engage in **"fractional reserve banking."** To reiterate, it is this practice by which banks can create (and destroy) money.

Measures of money and how Commercial Banks "create" money

Various Measures of "How Much Money" Is in the Economy

- A standard definition of money is that it's a medium of exchange that is (nearly) universally accepted in trade among a given community of people. However, in practice there are different ways of applying this definition, because of the special economic nature of claims on money.
- In a town where everyone agrees that gold is the money, how should we treat a paper note issued by a reputable goldsmith that is an airtight and immediate redemption ticket entitling the bearer to a gold coin? If all of the merchants in town are just as willing to sell merchandise in exchange for these paper notes as they are for actual gold, then doesn't that render the notes issued by the goldsmith a "universally accepted medium of exchange"?
    - So if we're trying to count up "how much money" is held by the townsfolk, shouldn't we count the physical gold and the total number of paper notes issued by the reputable goldsmiths? These are the complications that give rise to different monetary aggregates (M0, M1, M2 and so on).
- M0: The narrowest definition of money, M0 refers to the actual physical items, such as $20 and other denominated bills and coins.
    - Monetary Base: The monetary base includes paper currency and coins, as well as commercial banks' (electronic) deposits at the Federal Reserve. Under current regulations, commercial banks in the US are required to keep some money "in reserve" in order to satisfy the demands of their customers who might show up to pull some cash out of their checking accounts. These "reserve requirements" can be satisfied by either literal paper currency in the banks' vaults, or by commercial banks' deposit balances with the Federal Reserve.
        - For example, suppose a particular bank had customers with total checking account balances of $1 billion. If the reserve requirement were 10 percent, then the bank would need to hold $100 million in reserves. It could satisfy this legal requirement if it held (say) $30 million in physical US currency in its own vaults on location and the Fed's own computer system said that the bank had $70 million in its own account with the Fed.
- Now that we have identified the narrowest, one could say "strictest" definition of money, let us proceed to see how even the commercial banks create money out of thin air, many times over.

How Commercial Banks "Create Money" under Fractional Reserves

- As far as we know, all of the world's monetary systems are based on *fiat* money; so there is nothing "backing up" the US dollar, Euro or any other fiat currency, in terms of its redeemability. The ability of the Federal Governments/Central Banks to create new money simply by printing up pieces of paper—or nowadays just through electronic activities that don't even involve physical currency—might lead some people to believe that it is *only* in a fiat money system that this type of money creation "out of thin air" is possible. However, *if they maintain less than 100 percent reserves on their checking accounts* (demand deposits), commercial banks also have the ability to create money through their lending decisions.
- To see how this works, let's first imagine a town where the banks *keep* 100 percent reserves. Suppose there are 100,000 gold coins held by the townsfolk. Out of concerns for safety and convenience, the people deposit (say) 80,000 of the gold coins with the bankers, for which they receive paper notes entitling them to their 80,000 coins.
    - Now suppose the banks do *not* practice fractional reserve banking, but instead maintain 100 percent reserves. That is to say, for every paper banknote held by someone in the town, there is an actual gold coin in a bank vault to "back it."
    - In this arrangement, notice that the public's decision to hold some of their money in the form of banknotes rather than physical gold coins does *not* affect the total amount of money in the town. The townsfolk still hold 20,000 of the gold coins in their direct physical possession, and they also have 80,000 banknotes entitling them to gold coins. So, if each person reports how many gold coins he or she effectively has, their answers will sum up to 100,000 gold coins, which is the same amount they would have reported before using the banks.
    - Incidentally, we should point out that 100 percent reserve banking is *possible*, whether or not one thinks that it is desirable. Banks can charge a fee for the warehousing of their customers' money, just as the owners of storage units manage to stay in business even though they don't rent out their clients' furniture. Furthermore, remember that we are here talking about *demand deposits* (think checking accounts), where the depositors believe they are entitled to obtain their money upon demand.
        - If instead a customer buys (say) a one-year bank certificate of deposit (CD), the bank can lend that money out to a borrower even while practicing 100 percent reserve banking, because the CD is not a promise for immediate redemption.
- But now suppose that the bankers don't maintain 100 percent reserves but instead practice fractional reserve banking, which is standard activity globally now. The bankers realize that the public has come to trust the redeemability of the banknotes, and that *most* of the 80,000 in gold coins in their vaults will just sit there.
    - Perhaps the bankers look at the history of transactions and conclude that so long as they always have enough gold coins in the vault to satisfy just 10 percent (say) of their total outstanding banknotes, they should be safe.

    - In other words, the bankers reason that it would be very unlikely that the public would show up at the same time to demand more than 10 percent of the total paper notes that they'd issued.
- In this case, the bankers see a great new way to earn income. Rather than "uselessly" keeping so many gold coins in their vaults, they *lend some of the coins out to new borrowers*. The borrowers then spend the money in the town, and the recipients in turn deposit the coins back into their own checking accounts at the banks. The process plays out until each gold coin sitting in a bank vault "backs up" *ten* paper banknotes held by people in the town.
    - In this new scenario, in which the banks only keep 10 percent reserves, what happens to the "total amount of money" in our town? If we calculate M0, the answer is still the same: there are 100,000 gold coins in the town, period. Issuing paper notes and making loans doesn't alter that fact.
    - However, if we use a broader aggregate such as M1, then the banks' actions *do* affect the total. Specifically, there are 20,000 gold coins still held by the public, plus *800,000* banknotes held by the public, each entitling the holder to a gold coin. In other words, the public's decision to keep 80,000 gold coins in the banks' vaults, combined with the bankers' decision to issue additional loans until the point at which they only held 10 percent reserves, caused M1 to grow from 100,000 gold coins to 820,000 gold coins.
- We have deliberately worked with an example of *commodity* money—in our example, gold—in order to isolate the role played by fractional reserve banking. Because the broader monetary aggregates (M1, M2, etc.) include not just the base money but also *very reliable and quick claims* on it, the actions of banks can expand or contract the total amount of money when measured in the broader sense of these aggregates.
    - In the modern United States, the base money is actual US dollars. But if someone has $100 in a checking account at a bank, she really thinks she *has* $100, even though her bank might only be holding (say) $10 in its vault (proportionate to each customer) to back her checking account balance.

Conclusion - Current Fiat Currency System

Today all government-issued currencies globally, but we'll take the United States as they have become the de facto "reserve" currency of the world for most of the 20th century; the US dollar itself— currently has *no* redemption option but is simply fiat money—the reserves held in bank vaults are green pieces of paper featuring US presidents. In addition, a commercial bank in the US can also satisfy its reserve requirements by having (electronic) balances on deposit with the Federal Reserve (Central Bank). Legally speaking, a commercial bank can itself hold a "checking account" with the central bank, and its deposit balance is "as good as" currency that the commercial bank holds in its own vaults.

For our purposes here, there are two crucial takeaway messages:

1. In the current fiat money system, the central bank creates new base money when it buys assets by writing checks on itself. These actions do not require a literal printing press, as they can be achieved through electronic operations.
2. When the central bank injects new base money into the system, it will often be deposited into commercial banks, where it will add to "reserves". Under fractional reserve banking, the new reserves give the commercial banks the ability to pyramid *new* money (as measured by M1, M2, etc.) on the system through the process of granting new loans.

Enter Bitcoin - "A Peer-to-Peer Electronic Cash System"

- What most enthusiasts don't know is how the trillion-dollar asset was first introduced to the world; through a PDF document. A pseudonym Satoshi Nakamoto published on October 31st of 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System", which was created as a solution against the Global Financial Crisis, providing a supply-capped monetary system that was fully decentralized and incorruptible, hence was the first ever cryptocurrency born.
- The significance - Bitcoin solved the issue of users spending the same asset more than once, known as double-spending. Built using blockchain technology, Bitcoin is run by numerous computers across the globe that collectively verify transactions and protect the network against hacking, due to the lack of a single point of failure.
    - Bitcoin was designed on the back of blockchain technology specifically to stop the fractional reserve banking that banks were and are still practicing.
- Bitcoin launched on its blockchain network in 2009. Since then, other people and companies have built numerous additional crypto assets — some of which position themselves as faster or more private assets.
- Other distributed and consensus technologies, most notably Ethereum Blockchain in 2014 and the Avalanche network in 2020 have also been created, giving developers a platform on which to build various additional assets, ecosystems and solutions, while connecting with all other blockchains in the greater ecosystem.

Bitcoin White Paper Summary

- Objective
    - The purpose of the Bitcoin network was to essentially eliminate the trust-based model of digital transactions by creating a digital representation of hard cash. Whether shopping for clothes online or using credit cards in stores, the payment standard until then was always done through financial institutions that approve and execute each transaction. By creating an electronic cash system, it eliminates the need for trust in third-party providers. The goal was accomplished by creating an asset - bitcoin, that allows peer-to-peer transactions that are immutable and encrypted through cryptography to protect users from fraud.
    - The whitepaper sought to fulfil the frameworks of what has been considered sound money throughout the ages. Bitcoin needed to function as a medium of exchange, unit of account and store of value. In creating a sound alternative to the existing monetary system, Satoshi Nakamoto also imbued the principles of durability, divisibility, portability, intrinsic value and scarcity.
- Transactions
    - For the system to work, what is now called the "Blockchain" was created. The transactions occur in a cooperative network that is kept active by sharing the transactional tasks with all computing systems that use it. When someone wants to transfer bitcoin to another user of the blockchain, the network verifies when the sender first received that amount (previous block) and confirms the amount they are now transferring to the receiver (future block). That way, the network asserts that the amount will no longer be in the sender's funds, with an irreversible transfer to the receiver, and so on.
- To ensure all transactions are verified, and there's no room for fraud, the Bitcoin network makes them public, allowing any user to access a record of transactions on the bitcoin blockchain. Each transaction is registered in what the whitepaper coined the word "timestamp" that displays where the amount existed previously and where it is heading, thus creating the chain of blocks.
- Solving double-spending
    - Double-spending surfaced once digital assets and currencies first became available, with the possibility of re-spending the same asset. After all, peer to peer (P2P) platforms existed more than a decade before bitcoin, where users could transfer files but still create duplicates in their computers through a simple copy and paste process.
    - How does bitcoin prevent that from happening?
        - For double-spending to be avoided, every transaction in the blockchain is verified by all existing nodes (computers), running programs that host and synchronize copies of the whole blockchain. Most computers available today can become a node, which helps the blockchain in validating transactions and

blocks. Since every transaction is publicly announced, verified by nodes and sender/receiver, the chance of double-spending is significantly reduced the more nodes the network has.

- Bitcoin mining – the incentive
    - Mining bitcoin simply means using one's computing system to process blockchain transactions. In return, miners are compensated in bitcoin as new transaction blocks are created and dictate how the network operates under a 51% majority system. The mining process is what the bitcoin creator(s) calls the incentive; a reason for people to keep a fully decentralized network up and running while making sure that it continues to grow in adoption. The Bitcoin whitepaper also mentions a predetermined number of coins to be mined, resulting in bitcoin's maximum supply of 21 million. Once all coins are mined, the incentive will continue in the form of transaction fees which oscillate freely and rely on the shifting hashrate of the network.
- Solving the Byzantine Fault
    - Byzantine Fault is the potential issue facing computers that participate in a shared system, where the framework might fail if the participants disagree on a strategy for the network. The Fault presumes that some members are corrupt, inefficient or non-democratic, noting that a single point of failure is enough to jeopardize the entire approach.
    - Bitcoin's blockchain solves the Byzantine Fault through its Proof-of-Work algorithm, allowing new strategies to be implemented only if 51% of the network agrees with the process. As the number of miners continues to grow, the chances of malevolent participants taking over the blockchain get increasingly unlikely. According to Business Insider, there are around one million miners currently active globally, which would take roughly 510,000 individuals to agree on intentionally jeopardizing the blockchain for the Byzantine Fault to be successful.
- Privacy
    - Privacy was one of the biggest concerns leading to the Bitcoin creation; the possibility of transacting funds in a secure network without compromising personal information to third parties.
    - While traditional banking systems limit user information in transactions, it still relies on the account owner trusting the institution to be able to access their data and to safeguard their privacy. In the Bitcoin network, all account owners are identified by their addresses; random sequences of 26-35 characters.
    - To send or receive assets, all a user needs is the blockchain address to interact with. The public can see all bitcoin transactions in the blockchain with ultimate transparency, but the chain only registers the addresses without linking the transaction to private information.

What is Blockchain?

- Like the name indicates, a blockchain is a chain of blocks that contains information, this technique was originally described in 1991 by a group of researchers and was originally intended to timestamp original documents, so it was not possible to back-date or to tamper with them, like a notary. However, it went mostly unused until it was adopted by Satoshi Nakamoto at the end of 2008 to create the digital currency bitcoin.
- A blockchain is a distributed ledger and in its purest form is completely open for anyone to view. Once the data has been recorded inside the blockchain, it becomes very difficult (nearly impossible in established blockchain networks) to change it.
- Each block contains the following;
    - Data
        - Data that is stored inside the block, depends on the type of blockchain. For example - The bitcoin blockchain stores the details of the transaction: such as sender, receiver and the amount transferred.
    - Hash
        - A block also has a hash, which can be compared to a fingerprint. It identifies a block and all of its contents, and it's always unique, just like a fingerprint.
        - Once a block is created, its hash (fingerprint) is being calculated. Changing something inside the block will cause the hash to change, in order words hashes are very useful when you want to detect changes made to the block.
            - If the fingerprint (hash) of the block changes, it is no longer the same block.
    - Hash of previous block
        - The third element is the hash of the previous block, which effectively creates a chain of blocks. It is this technique that makes the blockchain so secure.
            - Example - Each block has a hash and the hash of the previous block, so block nr. 3 points to block nr. 2, and nr 2 points to block nr. 1.
                - The 1st block is special because it cannot point to previous blocks, because it's the first one, hence called the Genesis Block.
            - Let's say you tamper with the 2nd block, this causes the hash of the block to change as well. In turn, that will make block 3 and all following blocks invalid, because they no longer store a valid hash of the previous block.
            - Changing a single block will make all following blocks invalid.
            - However, using hashes alone is not enough to prevent tampering, as computers are very fast nowadays (calculate 100,000's of hashes per

sec), where one can effectively tamper with a block and recalculate all the hashes of other blocks to make the blockchain valid again.

- To mitigate this, blockchains have what is called - Proof of Work (PoW). This is a mechanism that slows down the creation of new blocks, in bitcoins case it takes about 10 minutes to calculate the required POW and add a new block to the chain.
    - This mechanism makes it very hard to tamper with the blocks, because if you tamper with one block, you will need to recalculate the POW of all the previous blocks.
- The security of the blockchain comes from its creative use of hashing and the proof-of-work mechanism but there is one more essential way that blockchains can secure themselves, by being distributed instead of being a central entity.
    - Open-source blockchains use a peer-to-peer network and everyone is allowed to join.
    - When someone joins this network, they get the full copy of a blockchain to-date, with all of its transactions.
    - The node can use this to verify that everything is still in order.
        - What is a node?
            - When someone creates a new block, that block is sent to every computer (nodes) on the network. Each node then verifies the block, to make sure it hasn't been tampered with and if everything checks out, each node adds this block to their copy of the blockchain.
            - All the nodes in the network create what is called consensus, they agree about what blocks are valid and which aren't. Blocks that are tampered with will be rejected by others in the network.
- In order to successfully tamper with a blockchain, you'll need to tamper with all the blocks of the chain (hashing), re-do the proof-of-work for each block and take control of more than 51% of your peer-to-peer consensus network. Only then will your tampered block become accepted by everyone else, which is almost impossible to do.
    - In the case of the Avalanche network 80% or more need to be controlled to successfully pull out such an attack. Hence making it more resistant to the Nakamoto Consensus that is applied in Proof of Work for establishing consensus.
- The creation of blockchain technology can be used for a plethora of use-cases, most of which we are yet to figure out (look at the difference of Internet 2000 vs. 2021), the 1st and most obvious one is the example of Bitcoin – Electronic cash i.e. cryptocurrency was born.

Cryptography

- Cryptography gives us the security for these transactions to go through the distributed ecosystem by providing secure communication in the presence of malicious third-parties—known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used.
- Algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the ciphertext. An attacker should not be able to determine anything about a key given a large number of plaintext/ciphertext combinations which used the key.
- What problems does cryptography solve?
    - A secure system should provide several assurances such as confidentiality, integrity, and availability of data as well as authenticity and non-repudiation. When used correctly, crypto helps to provide these assurances. Cryptography can ensure the confidentiality and integrity of both data in transit as well as data at rest. It can also authenticate senders and recipients to one another and protect against repudiation.
        - Modern day software systems often have multiple endpoints, typically multiple clients, and one or more back-end servers. These client/server communications take place over networks that cannot be trusted. Communication occurs over open, public networks such as the Internet, or private networks which may be compromised by external attackers or malicious insiders.

What is a consensus mechanism?

An overly simplified analogy would be the classical consensus like a Monarchy, nakamoto consensus is sort of like a Republic, where miners are the officials that represent the will of the people, and Avalanche would be a Democracy without officials. The individual says what goes on, without any elected official, it is leaderless in nature.

Now we come to learn about how a decentralized peer-to-peer blockchain system with no authoritative figure makes decisions. The answer lies in the consensus mechanism. There are various consensus mechanisms but they all serve the same purpose; to ensure records are true and honest, the difference is the way the consensus is reached.

When it comes to blockchains which are, in essence, distributed databases, the network's nodes must reach an agreement on the network's current state. This agreement is achieved using consensus mechanisms. By consensus, we mean that a general agreement has been reached. Consider a group of five people going to the cinema. If three out of five agree on a film, a consensus is achieved — majority rules.

In regards to blockchain, reaching consensus means that at least 51% of the nodes on the network agree on the next global state of the network. Let's take a look at the following three consensus mechanisms:

Short History of Consensus – Classical consensus doesn't work well for a decentralized currency, all of the participating nodes have to know each other and with such a high communication cost, it doesn't scale very well. Leaders in the classical consensus are elected by an authority, rather than having a way to drop in and out of the system, it is a permissioned network.

In 2009 with the Bitcoin white paper, we have the Nakamoto consensus, which allowed Satoshi Nakamoto to create the first real decentralized cryptocurrency. It differs in that nodes don't have to know each other in the network, which allows greater scale. Can drop in and out at any moment, it is considered permissioneless network as anyone can come in, be a leader, or block producer, no central party decides to make them a leader, competition decides through mining.

In 2020 team Rocket created Avalanche Consensus. Avalanche is a new consensus protocol, that is different from the other two models. Instead of leaders being elected or earned through competition. Avalanche is leaderless by nature, every node on the network has a vote, there are no specially privileged nodes on running things, it is highly scalable and very fast.

Proof of Work (PoW)

- In the PoW system, transaction data is stored in blocks, validated by having people solve a complicated math problem attached to it. This is typically done by powerful computers and is known as "mining".
- Proof-of-work is the mechanism that allows the decentralized Ethereum network to come to consensus, or agree on things like account balances and the order of transactions. This prevents users from "double spending" their coins and ensures that the blockchain is tremendously difficult to attack or manipulate.
- Proof-of-work is the underlying algorithm that sets the difficulty and rules for the work miners do. Mining is the "work" itself. It's the act of adding valid blocks to the chain. This is important because the chain's length helps the network follow the correct Ethereum chain and understand Ethereum's current state. The more "work" done, the longer the chain, and the higher the block number, the more certain the network can be of the current state of things.
- A reward in the form of cryptocurrency is issued to the first miner who solves the problem. Let's break it down.
- Imagine a group of treasure hunters trying to open a chest with a complicated lock attached to it. Figuring out the correct combination is tedious, but the first person (or group) to do so, gets rewarded.

- Simply put, PoW is a race to figure out the right combination on a treasure chest.
- Cryptocurrencies like Bitcoin and Ethereum currently use the PoW mechanism.
    - Important note. Ethereum will be shifting to Proof of Stake as of 2022, the migration has already started.

Proof-of-work and security

- Miners are incentivized to do this work on the main blockhain such as Bitcoin and Ethereum (Ethereum is moving to Proof of Stake in 2022). There is little incentive for a subset of miners to start their own chain – it undermines the system. Blockchains rely on having a single state as a source of truth. And users will always choose the longest or "heaviest" chain.
- The objective of proof-of-work is to extend the chain. The longest chain is most believable as the valid one because it's had the most computational work done. Within a well-established PoW system like Bitcoin and Ethereum, it's nearly impossible to create new blocks that erase transactions, create fake ones, or maintain a second chain. That's because a malicious miner would need to always solve the block nonce faster than everyone else
- To consistently create malicious yet valid blocks, you'd need over 51% of the network mining power to beat everyone else. You would need a lot of computing power to be able to do this amount of "work". And the energy spent might even outweigh the gains you'd make in an attack

Proof of Work (PoW) and its Pros and Cons

- Pros of PoW
    - Proof-of-work is neutral. You don't need any cryptocurrency coins to get started and block rewards allow you to go from 0 to a positive balance. In contrast with proof-of-stake you need to start with a set balance of coin/s.
    - Proof-of-work is a tried and tested consensus mechanism that has kept Bitcoin and Ethereum secure and decentralized for many years.
    - Compared to proof-of-stake it's relatively easy to implement.
- Cons of PoW
    - Proof-of-work uses up so much energy that it's bad for the environment.
        - Reasonable estimates from the University of Cambridge place Bitcoin's current annual energy consumption at 130TWh, a continuous draw of 15 gigawatts of electricity. If Bitcoin were a country, its annual energy consumption would place it between the mid-sized countries of Ukraine and Argentina.
        - Ethereum reports that their proof-of-work protocol consumes 73.2 TWh annually, the energy equivalent of a medium-sized country like Austria.

        - As stated Ethereum will become Proof of Stake in 2022, migration process has started already.
    - If you want to mine, you need such specialized equipment that it's a big investment to start. Increasing difficulty leading to unprofitable mining hardware. Can be redirected to mine other coins though.
    - Due to the increasing computation needed, mining pools could potentially dominate the mining game, leading to centralization and security risks.
        - Governments like China are closing in on miners.

Proof of Stake (POS)

- Proof of stake is a type of consensus mechanism used by blockchain networks to achieve distributed consensus. It requires users to stake their ETH to become a validator in the network. Validators are responsible for the same thing as miners in proof-of-work: ordering transactions and creating new blocks so that all nodes can agree on the state of the network.
- Proof-of-stake (PoS) comes with a number of improvements to the proof-of-work system:
    - Better energy efficiency – you don't need to use lots of energy mining blocks.
    - Lower barriers to entry, reduced hardware requirements – you don't need elite hardware to stand a chance of creating new blocks.
    - Stronger immunity to centralization – proof-of-stake is expected lead to more nodes in the network, therefore strengthening the network.
    - Stronger support for shard chains – a key upgrade in scaling the Ethereum network. Sharding will be touched on, in this paper.
- In PoS, the creator of a new block is randomly chosen based on how much stake they commit to the network. Meaning to say the higher the stake placed, the higher the chance to be selected as a validator.
- Let’s apply this to the treasure chest scenario - picture a group of treasure hunters vying for a chest, the chest is rewarded based on a lottery system. To participate, each hunter has to buy lottery tickets, the more each hunter buys, the higher the chance of winning.
- A user's stake is also used as a way to incentivize good validator behavior. For example, a user can lose a portion of their stake for things like going offline (failing to validate) or their entire stake for deliberate collusion.

Proof of Stake (POS) and Security

- The threat of a 51% attack still exists in proof-of-stake, but it's even more risky for the attackers. To do so, you'd need to control 51% of the staked ETH. Not only is this a lot of money, but it would probably cause ETH's value to drop. There's very little incentive

to destroy the value of a currency you have a majority stake in. There are stronger incentives to keep the network secure and healthy.

- Stake slashing, ejections, and other penalties, coordinated by the beacon chain, will exist to prevent other acts of bad behavior. Validators will also be responsible for flagging these incidents.

Proof of Stake (PoS) and its Pros and Cons

PoS Pros

- Staking makes it easier for you to run a node. It doesn't require large investments in hardware or energy, and if you don't have enough coins to stake, you can join staking pools.
- Staking is more decentralized. It allows for increased participation, and more nodes doesn't mean increased % returns, like with mining.
- Staking allows for secure sharding. Shard chains allow Ethereum to create multiple blocks at the same time, increasing transaction throughput. Sharding the network in a proof-of-work system would simply lower the power needed to compromise a portion of the network.

What is sharding?

- Sharding is the process of splitting a database horizontally to spread the load – it's a common concept in computer science. In an Ethereum context, sharding will reduce network congestion and increase transactions per second by creating new chains, known as "shards".
- This is important for reasons other than scalability.
    - Everyone can run a node
        - Sharding is a good way to scale if you want to keep things decentralized as the alternative is to scale by increasing the size of the existing database. This would make Ethereum less accessible for network validators because they'd need powerful and expensive computers. With shard chains, validators only need to store/run data for the shard they're validating, not the entire network (like what happens today). This speeds things up and drastically reduces hardware requirements.
    - More network participation
        - Sharding will eventually let you run Ethereum on a personal laptop or phone. So more people should be able to participate, or run clients,

in a sharded Ethereum. This will increase security because the more decentralized the network, the smaller the attack surface area.
    - With lower hardware requirements, sharding will make it easier to run client solutions on your own, without relying on any intermediary services at all.

What is a transaction throughput?

- Transaction throughput is the rate at which valid transactions are committed by a blockchain in a defined time period. The throughput of a given blockchain is defined by the number of transactions per second (tps).
    - Bitcoin has 7 tps, Ethereum has 15 tps but expected to hit 100,000 tps with the Eth 2.0 upgrade.

PoS Cons

- Proof-of-stake is still in its infancy, and less battle-tested, compared to proof-of-work.

Proof of Work (PoW) compared to Proof of Stake (POS)

- At a high level, proof-of-stake has the same end goal as proof-of-work: to help the decentralized network reach consensus securely. But it has some differences in process and personnel:
- Proof-of-stake switches out the importance of computational power for staked coins.
- Proof-of-stake replaces miners with validators. Validators stake their coins to activate the ability to create new blocks.
- Validators don't compete to create blocks, instead they are chosen at random by an algorithm.
- Finality is clearer: at certain checkpoints, if 2/3 validators agree on the state of the block it is considered final. Validators must bet their entire stake on this, so if they try to collude down the line, they'll lose their entire stake.

Avalanche Consensus Mechanism

4 stages of the Avalanche Consensus Protocol

Slush – An avalanche network is made of large network of nodes, each one of these nodes has three states (neutral, true and false) which will be represented as uncolored (represented by yellow), blue and red. Each node starts off on the network as uncolored (yellow to see), until it is faced with a transaction or decision, where it will either vote red or blue. In this case blue, once a color is chosen, your node queries and a number of other random nodes on the network, if those queried notes do not yet have a color, they will adopt the color of your node. If the majority of nodes queried have the same color, your node takes no action.

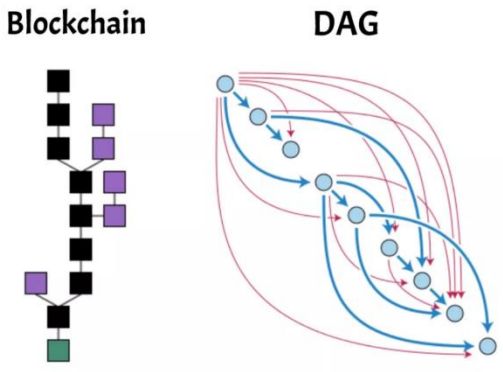
If the majority of nodes are of a different color, your node will flip to that color. Multiple rounds of querying will occur with different random nodes, until the majority of the network is all on the same color. Even in the worst case scenario, let's say a 50/50 network split. After enough rounds of querying are completed, the pseudo randomness of the querying process will ensure that one side will clearly emerge and consensus is reached. This is the general idea behind the Avalanche Consensus and everything builds off of this.

Snowflake – 2nd part of Avalanche is snowflake, which is when the network starts to gain a very short memory, each node has a counter, for every slush query that returns the same color, the counter turns up by 1, every time the node flips its color, the counter resets. When the counter reaches a high enough number, it will lock in at this number and no longer flip with slush queries, which create a sort of ending period to the slush cycle.

The snowflake's memory is extremely short, only lasting until the node locks in or flips to another color. Nodes begin to have a persisting memory in the third part, snowball.

Snowball – Builds upon snowflake by adding a state of confidence. This confidence counter holds a longer memory than snowflake, changing colors based on its confidence of past queries, rather than simply based of the consecutive color results of each node. This all leads to part four, Avalanche.

Avalanche – Where everything ties together and becomes permanent. The confirmed transactions are appended to a data structure, in a DAG.



The avalanche network follows proof of stake pretty closely but it does have a few unique differences first off the avalanche model uses a form of sub-sampled voting this means that there's a large group of people who volunteer to participate in the network and get randomly asked to check things. To put it in their own words small random subsets of validators are asked whether they think the transactions would be accepted or rejected.

One of the benefits of this is that contrary to proof of work and proof of stake mechanisms, it doesn't matter how many nodes there are how many people there are in the system consensus will be reached within a certain desired time frame. Also due to some technicalities this consensus model is actually much more difficult to attack;

- Unlike bitcoin where you would need 51 % of all the computers to attack the network, or;
- Ethereum 2.0 where you would need 51 % of all the staked tokens to attack the network.
- With avalanche you would need to control up to 80 percent of the network to perform an attack.

The avalanche network model allows for up to 4 500 (Visa processes 1 700) transactions per second, per subnet and has a finality clock of less than three seconds.

- You can technically create as many subnets as you want.
- Compare this to bitcoin with seven transactions a second in an hour-long finality and even Ethereum pales to compare with 15 transactions a second and a 10-minute finality, but the Eth 2.0 merge should drastically change that also, which is great for the overall blockchain ecosystem, family of blockchains, co-existing, interoperable with one another, whenever so chosen.

Let's explain how the avalanche consensus model works, Avalanche has one primary network, that network has actually three built-in blockchains with it, that's right avalanche just isn't one blockchain, it is at least three.

- The first blockchain in the network is called the x-chain - this is the part specifically for creation, management and transaction of tokens on the network.
    - Now the engineers would tell us in technicality, that this is actually based on a DAG which is a unique form of a consensus model, unlike a blockchain.
- Then we come to the the c-chain, specifically for smart contracts, it is actually an exact copy of the Ethereum Virtual Machine, so that way you can instantly copy and paste and start using ethereum dapps on the avalanche network, allowing developers to move their projects over.
- Next we have the p-chain or the platform chain and it is specifically, for management of the subnets, it also coordinates all the validator nodes and the staking mechanism.

Subnets - each subnet is a new network in the avalanche ecosystem, this system is scalable in so many ways.

- Each subnet can have multiple blockchains just like the primary avalanche network secondly each blockchain in a subnet can have its own consensus model, additionally each blockchain can have its own VM or virtual machine, you can copy the ethereum virtual machine just like the primary chain has.
- Subnets can be permissionless or permissioned, this means that they can either be public or private blockchains. Now you might start to understand the purpose of this if you are a government and you want the full power of a blockchain without developing the groundwork, you can just add a subnet in avalanche's ecosystem.
- Maybe you're a government or maybe you're a business or an organization or some other protocol needing to use these very powerful tools without wanting to actually invest in something new.
- In avalanche you can even change the rules for each blockchain in your network you can make it so that it is compliant across many different geographic or political requirements.
    - For example, you could say every validator in your subnet needs to have a license or maybe they need to fill out certain information, avalanche is built to be able to create and follow rules like that.
- Important note to add is that to validate your own subnet you are also contributing to the validation of the entire network via the primary three chains.

Ethereum – General Purpose Blockchain

Decentralized Technologies - Thanks to the power of modern communication, we have the ability to create technologies that are decentralized, removing middle-men and allowing users to interact with each other directly, through a global network.

Decentralized Applications have become more and more important in the last 10 years, which have the benefits of massively reducing costs, barriers to entry, removing single points of failure, preventing censorship and ensuring transparency and trust between all the parties involved in an interaction.

- Bit torrent (2003) - A file sharing network is arguably the first decentralized application to have been created. Bit torrent allows anyone to share any kind of file with anyone else in the world, allowing people to distribute content quickly and easily, even if they do not have the resources to pay for their own website or server.
- Bitcoin (2008/2009) - Satoshi Nakamoto came up with the idea of a blockchain - distributed database. Used it to build the world's first decentralized currency, Bitcoin.
- Decentralized currencies like bitcoin allow people to send money instantly anywhere around the world, with no regard for national borders and negligible fees.
- Ethereum (2014) - Ethereum is a platform that is specifically designed for people to build these types of decentralized applications (dApps for short). The ethereum client (ether browser) includes a built-in peer-to-peer network for sending messages and a generalized blockchain, with a built-in programming language.

- Allowing people to use the blockchain for any kind of decentralized application (dApps) that one wants to create. Ethereum can be used to build financial applications that are fully trustworthy and transparent, because they run on the blockchain;
    - Online cryptographically secured systems for managing your properties and contracts
    - Social networking and messaging systems that allow users to maintain control of their own data.
    - Systems for trading under-utilized computational resources like CPU time and hard drive space.
    - Online voting and distributed governance.
    - Most exciting applications of Ethereum have not been thought of yet, as with all new platforms for innovation, like the protocols that underline the internet itself, it is not always easy to predict what they are going to be used for.
        - Gmail, Facebook, Twitter, Instagram and the modern internet as a whole are all the result of early developments in the world wide web in javascript, the programming language of the world wide web from the 1990's.
    - Similarly, by providing a universal, programmable blockchain and packaging it up into a client that anyone can use. The Ethereum project will do the same for finance, peer-to-peer commerce, distributed governance and human collaboration as a whole.
        - The question is - what will you build on top of Ethereum?

More in-depth look at Ethereum

- Ethereum is an open-source platform to build and distribute next generation decentralized applications, which means there are no middle men, but rather users will interact with social systems, financial systems, gaming interfaces, all in peer-to-peer fashion.
- Because the Ethereum network is distributed on hundreds of thousands of computers around the globe, this all takes place on a censorship proof foundation.
- Easy for developers to build these applications, leveraging tools that developers are already familiar with, to build the business logic.
    - Ethereum projects goal is to open up the floodgates of decentralized application (dApp) development.
- Why Ethereum?
    - Most of the services we use today have one thing in common; they're centralized. For example, you trust your bank to be independently audited and to be honest.
    - Same is true with Facebook when you upload a picture of your kids, when you upload your document on DropBox or even when you go to share your personal medical information to your medical provider.
    - As a developer you need to submit your application to an App Store and risk having it removed for the most far-fetched of reasons.

- History has proven time and time again that this model implemented in various services in our lives, is flawed but necessary as so called trustless operations have thus far been unprofitable and too complex to implement.
- Everything that is centralized makes it easy to attack, because it offers a single point of failure, like the firewall of a website.
- Applications built on Ethereum do not require their users to trust the developers with their personal information or funds. On Ethereum, your personal information, funds and content are yours.

Use Cases

- Ethereum is an application-programming platform, so what can be built on Ethereum is only limited by the creativity of the developers. However, we can identify three types of immediate use cases;
    - Individual Currencies & Tokens
        - Imagine that you are an artist and you want to support yourself by issuing a brand new currency or token. If you want to support such an artist instead, you purchase their currency, technically investing in their personal IP (intellectual property).
        - As those millions of currencies, tokens are traded on decentralized exchanges, these currencies and tokens become a representation of your values, not just a means of exchange.
        - Ethereum makes it straightforward to issue your own tokens of values, so you can reward your users for actions that they take even outside of the network.
        - Imagine how the relationship between consumers and retailers would change, if instead of issuing royalty points, retailers would issue crypto tokens of value that can be then exchanged for goods and services in decentralized markets, or even other tokens of value.
    - Another interesting application - For example today on Facebook, if you help identify an artist who suddenly becomes successful, by pressing the like button, that value goes to the Facebook Advertisers, not the content producers nor you the one who liked (rewarded) the artist.
        - However, on Ethereum, both the content creator and the early adopter will be rewarded for identifying that artist. It is a brand new revenue model that has never been seen before and could totally revolutionize the way we think about revenue on the internet today.
    - Another type of application envisioned to be very successful on Ethereum - are applications that currently require a middleman.
        - Users are tired of paying fees to companies such as Ebay, Kickstarter or Airbnb.

        - On the peer-to-peer network the existence of a middleman is limited to bringing true value-add such as insurance for example. Rather than just putting two people in-contact with each other.
        - For a decentralized kickstarter, instead of receiving a pre-ordered product that becomes obsolete or just a t-shirt. Instead users can be rewarded with tokens of value into the startups that they invest in.
    - Financial applications
        - Credit System that relies on reputation, rather than physical assets. In case of default, one would be banished. This has proven a successful concept in the developing world, where microfinance companies have experienced very low default rate and it is not new, but it never scaled past a small group of individuals.
        - Ethereum makes it possible to scale reputation to millions of individuals, forcing disruption not just in the developing world, but also much closer to home.
        - This wouldn't be limited to credit, as on Ethereum any user can issue and trade stocks, bonds, derivatives and even contracts for differences (COD).
    - Most impactful Ethereum applications have most likely not been invented yet, just like it took four years for social networks to appear on the web and a couple more years to see them diversify, and see novel applications such as micro blogging.

How does it work?

- At the core of Ethereum, you're going to find blockchain technology. If you look at centralized applications, you'll find that they achieve trust by being closed; firewalls and security teams that you have to trust and trust that they do their job well.
- With blockchain, trust will be reached over an open network. Bitcoin is a currency that was the first and currently the best known blockchain technology.
- Ethereum makes this technology applicable to just about anything else, anything that can be mathematically represented, can be modeled, secured and traded. Just like in bitcoin, where you do not need to trust a bank or a central authority to keep your funds safe. On Ethereum your personal information, identity and funds stay under your control at all times.
- On Ethereum, developers will write business logic into what we call contracts.
- Contracts are programs that follow a series of steps, every time they receive a message called a transaction. Contracts can store data, send and receive transactions and even interact with other contracts, independently of any control.
- Contracts are maintained by the network and they are written in a programming language that will be instantly familiar to any developer.

- Because the interfaces to the contracts that live on the Ethereum network are also decentralized, as an application-developer you will need zero infrastructure to deploy and distribute your applications.
- Your application will also be impervious to denial of service (DOS) attacks.
    - A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.
    - Buffer overflow attacks – is the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle.

The Future?

- A future application of Ethereum are DAO's (Decentralized Autonomous Organizations). A DAO consists of one or more contracts and could be funded by one or more like-minded individuals.
- A DAO operates completely transparently and independently, without any human intervention, including its original creators.
- A DAO will stay on the network for as long as it covers its survival cost and provides a useful service to its user base (customer, member, holder).
    - We will discuss more about DAO later.
- Think of Ethereum as a programmable, distributed network. The fact that Ethereum is by its very design - both fraud and tamper-resistant, means that it offers a new range of solutions to everyday problems that are currently solved at a great expense.
    - Voting machines
    - Domain name registration
    - Registration of legal documents
    - Medical software
    - Transfer of goods and services
    - Smart properties and contracts between individuals
    - Reputation systems
    - Financial Derivatives
- All those applications can be built on the network, where users control their funds and their personal information at all times.
- Ultimately, Ethereum is not here to undermine or to strengthen any existing system - it's a third way, beyond voice vs. exit.
- While there are of course challenges ahead of such an ambitious project, Ethereum has the largest number of brightest minds, developers working on it globally, estimated at 2,400 developers (Electric Capital Developer Report 2020), in addition to having assembled world renowned experts to help build Ethereum - including;

    - Neal Koblitz - Co-Creator of the elliptic curve cryptography used in bitcoin
        - Elliptic Curve Cryptography (ECC) is one of the most powerful but least understood types of cryptography in wide use today.
    - Ralph C. Merkle - One of the inventors of public key cryptography, the inventor of cryptographic hashing, and more recently a researcher and speaker on cryonics.

What is the Ethereum Virtual Machine (EVM)

- The Ethereum Virtual Machine is designed to be the infrastructure for smart contracts based on Ethereum. The major focus of this project is related to avoiding and preventing denial of service (DOS) attacks, which have become a concern in the crypto world.
- The EVM's physical instantiation (or representation) can't be described in the same way that one might point to a cloud or an ocean wave, but it does exist as one single entity maintained by thousands of connected computers running an Ethereum client.
- The Ethereum protocol itself exists solely for the purpose of keeping the continuous, uninterrupted, and immutable operation of this special state machine; It's the environment in which all Ethereum accounts and smart contracts live.

From Ledger to State Machine

- The analogy of a 'distributed ledger' is often used to describe blockchains like Bitcoin, which enable a decentralized currency using fundamental tools of cryptography. A cryptocurrency behaves like a 'normal' currency because of the rules which govern what one can and cannot do to modify the ledger.
    - For example, a Bitcoin address cannot spend more Bitcoin than it has previously received. These rules underpin all transactions on Bitcoin and many other blockchains.
- While Ethereum has its own native cryptocurrency (Ether) that follows almost exactly the same intuitive rules, it also enables a much more powerful function: smart contracts. For this more complex feature, a more sophisticated analogy is required. Instead of a distributed ledger, Ethereum is a distributed state machine.
- More specifically the EVM ensures programs have no access to each other's state. Making sure communication is created without anyone being able to disturb. The EVM is also designed for delivering security and executing untrusted code by the computers in the networks.

Blockchain and Turing Completeness

- The Ethereum Virtual Machine is considered a “quasi” - Turing complete machine.
    - Turing Complete - Refers to a machine that, given enough time and memory along with the necessary instructions, can solve any computational problem, no matter how complex.
    - Turing Machine - Before modern-day computers, Alan Turing hypothesized that there would one day be a machine that could solve any problem. This machine became known as the Turing Machine.
    - While some applications of blockchain technology are Turing Complete, others are Turing Incomplete. This varies according to the scripting technology implemented. For example, the scripting language used in Bitcoin is intentionally designed as Turing Incomplete because it serves its purpose and increased complexity would potentially introduce problems.
        - By keeping it simple, the developers can predict with high accuracy how it is going to react in the finite number of situations in which it is used.
    - Ethereum, on the other hand, is built as a “quasi” Turing Complete blockchain. This is important because it needs to understand the agreements which make up smart contracts. By being Turing Complete, Ethereum has the capability to understand and implement any future agreement, even those that have not been thought of yet. In other words, Ethereum’s Turing Completeness means that it is able to use its code base to perform virtually any task, as long as it has the correct instructions, enough time and processing power.
    - The EVM is a quasi–Turing-complete state machine; "quasi" because all execution processes are limited to a finite number of computational steps by the amount of gas available for any given smart contract execution. As such, the halting problem is "solved" (all program executions will halt) and the situation where execution might (accidentally or maliciously) run forever, thus bringing the Ethereum platform to halt in its entirety, is avoided.
        - In order to execute a transaction, the sender has to set the gas limit and gas price attached to the transaction, otherwise the transaction will be counted as invalid and will claim that you’ve run out of gas.

Smart Contract – Code is Law

- The term "smart contract" was first used by Nick Szabo (Computer scientist, law scholar & cryptographer) in 1997, long before bitcoin was created.
    - In simple terms, he wanted to use a distributed ledger to store contracts.
- A Digital Vending Machine Metaphor
    - Perhaps the best metaphor for a smart contract is a vending machine, as described by Nick Szabo. With the right inputs, a certain output is guaranteed.
    - To get a snack from a vending machine:
        - Money + snack selection = snack dispensed
            - This logic is programmed into the vending machine.
        - A smart contract, like a vending machine, has logic programmed into it.
            - Like how a vending machine removes the need for a vendor employee, smart contracts can replace intermediaries in many industries.
- Smart contracts are just like contracts in the real world, the only difference is that they are completely digital. In fact, a smart contract is actually a tiny computer program that is stored inside of a blockchain.
    - Let's take a look at an example of how smart contracts work - you're probably familiar with kickstarter (a large fundraising platform).
        - Product teams can go to kickstarter
        - Create a project
        - Set a funding goal
        - And start collecting money from others who believe in the idea.
    - Kickstarter is essentially a third-party that sits in between the product-teams and its supporters. This means that both of them need to trust Kickstarter to handle their money appropriately.
    - If the project gets successfully funded, the project team expects kickstarter to give them the funds, on the other hand supporters want their money to go to the project, if it has been funded or to get a refund, if it hasn't reached its funding goals.
    - Both the product-team and its supporters have to trust Kickstarter to keep on its promise as the middle-man.
- We can easily build a similar system with smart contracts that doesn't require a third-party like Kickstarter. We can program a smart contract, so that it holds all the received funds, until a certain goal is reached.
    - The supporters of the project can now transfer the money to the smart contract.
    - If the project gets fully funded, the smart contract automatically releases the money to the creator of the project.

    - If the project fails to meet those goals, then the money automatically goes back to each supporter.
- Because smart contracts are stored inside a blockchain, everything is completely distributed. No one is in control of the money with this technique, but how can you trust a smart contract?
- Smart contracts are stored on the blockchain, they are inherently immutable and distributed:
    - Immutable – means that once a smart contract is created, it can never be changed again, so no one can go behind your back and tamper with the code of the contract.
    - Distributed - means that the output of your contract is validated by everyone on the network, so a single person cannot force the contract to release the funds, because other people on the network will spot this attempt and mark it as invalid. Tampering with smart contracts becomes almost impossible.
- Smart contracts can be applied to many different things, not just for crowdfunding. Banks for example can use it to issue loans and offer automatic payments. Insurance companies could use it to process claims. Delivery companies could use it for payment on delivery.
- Right now there are only a handful of blockchains who support smart contracts, but by far the biggest and most well established ones are Ethereum and Avalanche which uses the Ethereum Virtual Machine in its c-chain, was specifically created and designed to support smart contracts.
- A "smart contract" is simply a program that runs on a blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on a blockchain.
- Smart contracts are a type of Ethereum account. This means they have a balance and they can send transactions over the network. However, they're not controlled by a user, instead they are deployed to the network and run as programmed.
- User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible.

Code is Law

- In Code is Law, technologies are used to enforce rules. In that case, do we need lawyers or maybe we can live in a fully automated world, where code dictates what we can and cannot do. With the current development in smart contracts, this futuristic scenario may be closer than we think.
- The aim of smart contracts is to remove the human factor from decision making, as human factor often proves the most error prone and unreliable element of the standard traditional contracts.

- Let's compare a hypothetical smart contract to its equivalent a traditional contract;
  - If Alice sends x number of tokens A and Bob sends the same number of tokens B, the tokens will be swapped. Alice will receive Bob's token and Bob will receive Alice's tokens.
  - In a traditional contract, one way of achieving this without Alice or Bob having to trust each other, would be to create an escrow contract with the third-party.
    - The third-party would collect tokens A from Alice, wait for the same number of tokens B from Bob and send Alice and Bob their respective swapped tokens.
    - This approach is not deterministic and shows a few problems such as trusting intermediaries, as there is no guarantee that the third-party will not run-away with the tokens after receiving funds from Alice and Bob. have to rely on the reputation of the intermediaries and potential insurance.
    - If something goes wrong, it may have different outputs (results) depending on multiple factors, including the jurisdiction where a potential case would be settled in.
  - On the other hand, the smart contract would work in a fully automated and deterministic way. Ensuring that both parties receive funds when they meet the initial criteria of depositing coins.
    - Smart contracts can also hold funds within themselves, which is not possible to achieve in the traditional world.
  - Speed - depending on the intermediary, Alice and Bob may have to wait days or weeks to settle the transition of tokens, also weekends would be either limited or closed, so the use of an intermediary imposes time-bound limitations. Such concerns are removed with smart contracts and the contract can be fulfilled seconds after the initial criteria are met.
  - Cost - traditional contracts are expensive, not only because of the need for profit by the intermediaries, there is also a large risk of hidden costs; arbitration and enforcement if there are any problems with the contract.
  - Reusability - The same smart contract that is responsible for swapping Alice's and Bob's tokens could be used by anyone else, who wants to swap tokens. In the traditional world, they would all have to sign separate contracts and pay their respective fees to the intermediary.
  - Fraud - Yet another hidden cost, this time for the intermediary, who would have to ensure that both tokens are legitimate, before initializing the swap. Fraud is very common in traditional finance and most companies have large teams, working exclusively on preventing fraud. With smart contracts, the tokens can be verified on the blockchain and with digital signatures it's clearly seen if both parties are eligible to spend their tokens.

Permissionless

- Anyone can write a smart contract and deploy it to the network. You just need to learn how to code in a smart contract language, and have enough ETH to deploy your contract. Deploying a smart contract is technically a transaction, so you need to pay your Gas in the same way that you need to pay gas for a simple ETH transfer. Gas costs for contract deployment are far higher, however.
- Ethereum has developer-friendly languages for writing smart contracts:
    - Solidity
    - Vyper

Composability

- Smart contracts are public on Ethereum and can be thought of as open APIs. You don't need to write your own smart contract to become a dapp developer, you just need to know how to interact with them.
- For example, you can use the existing smart contracts of Uniswap, a decentralized exchange, to handle all the token swap logic in your app – you don't need to start from scratch.
    - That means you can call other smart contracts in your own smart contract to greatly extend what's possible. Contracts can even deploy other contracts.

Decentralized Application (dApp)

- Our phone has a bunch of different applications; Facebook, Instagram, Gmail and Youtube are all basically applications that run code that was created by the company, so that you would interact with their company.
- A decentralized application (dApp) is very similar in how it works, but instead of reporting back to Facebook or TikTok servers, this app reports back to the blockchain, you're simply interacting with the blockchain through the application.
- A decentralized application (dApp) is an application built on a decentralized network that combines a smart contract and a front-end user interface. On Ethereum, smart contracts are accessible and transparent – like open APIs – so your dApp can even include a smart contract that someone else has written.
- A dApp has its backend code running on a decentralized peer-to-peer network. Contrast this with an app where the backend code is running on centralized servers.
    - Smart contracts - are a dApp's backend for lack of a better term.

    - Once smart contracts are deployed on the network you can't change them. dApps can be decentralized because they are controlled by the logic written into the contract, not an individual or company. This also means you need to design your contracts very carefully and test them thoroughly.
- A dapp can have front-end code and user interfaces written in any language (just like an app) to make calls to its backend. Furthermore, its front-end can get hosted on decentralized storage service.
    - Decentralized - dapps operate on Ethereum, an open public decentralized platform where no one person or group has control.
    - Deterministic - dapps perform the same function irrespective of the environment in which they get executed.
    - Turing complete - dapps can perform any action given the required resources.
    - Isolated - dapps are executed in a virtual environment known as Ethereum Virtual Machine so that if the smart contract has a bug, it won't hamper the normal functioning of the blockchain network.
- Benefits of dApp development
    - Zero downtime – Once the smart contract is deployed and on the blockchain, the network as a whole will always be able to serve clients looking to interact with the contract. Malicious actors, therefore, cannot launch denial-of-service attacks targeted towards individual dApps.
    - Privacy – You don't need to provide real-world identity to deploy or interact with a dApp.
    - Resistance to censorship – No single entity on the network can block users from submitting transactions, deploying dApps, or reading data from the blockchain.
        - Really important for financial applications, this way nobody can control your money. As historically governments have acted tyrannically and irresponsibly have taken control over their citizens' money.
        - There have also been cases where Facebook or Twitter have actually banned or censored certain people based on their opinions. A decentralized application (dApp) will not allow this, unless it's written in its code which is publicly seen.
    - Complete data integrity – Data stored on the blockchain is immutable and indisputable, thanks to cryptographic primitives. Malicious actors cannot forge transactions or other data that has already been made public.
    - Trustless computation/verifiable behavior – smart contracts can be analyzed and are guaranteed to execute in predictable ways, without the need to trust a central authority. This is not true in traditional models; for example, when we use online banking systems, we must trust that financial institutions will not misuse our financial data, tamper with records, or get hacked.

- Drawbacks of dApp Development
    - Maintenance – dApps can be harder to maintain because the code and data published to the blockchain are harder to modify. It's hard for developers to make updates to their dApps (or the underlying data stored by a dApp) once they are deployed - even if bugs or security risks are identified in an old version, which is why legitimate protocols go through an auditing process to ensure everything checks out on the code side.
    - Network congestion – When one dApp uses too many computational resources, the entire network gets backed up. Currently, the network can only process about 10-15 transactions per second; if transactions are being sent in faster than this, the pool of unconfirmed transactions can quickly balloon.
        - The ETH 2.0 upgrade – previously called Serenity is meant to address this issue and more. More on this later.
    - Centralization – User-friendly and developer-friendly solutions built on top of the base layer of Ethereum might end up looking like centralized services anyways. For example, such services may store keys or other sensitive information server-side, serve a front-end using a centralized server, or run important business logic on a centralized server before writing to the blockchain. Centralization eliminates many (if not all) of the advantages of blockchain over the traditional model.
        - Important not to be fooled by keywords such as blockchain, smart contract, dApp but to truly see if the service has maintained its integrity as a distributed protocol or reverted back to a traditional model with a new set of bells and whistles.

Decentralized Finance (DeFi)

- Decentralized finance, or DeFi, is a system by which financial products become available on a public decentralized blockchain network. That makes them open to anyone to use, rather than going through middlemen like banks or brokerages. Unlike a bank or brokerage account, a government-issued ID, Social Security number, or proof of address are not necessary to use DeFi. More specifically, DeFi refers to a system by which software written on blockchains makes it possible for buyers, sellers, lenders, and borrowers to interact peer to peer or with a strictly software-based middleman rather than a company or institution facilitating a transaction.
- DeFi is an abbreviation of decentralized finance, a term for products and services built as open-source financial software on top of blockchain technology that can be pieced together like money legos via shared infrastructure.

- Accordingly, decentralized finance is exciting because it's leading to a constant influx of novel opportunities that can financially empower users across the globe in unprecedented ways. DeFi is thus creating an alternative financial system that's open to everyone and that minimizes one's need to trust and rely on central authorities.
- Technologies like the internet, cryptography, and blockchain give us the tools to collectively build and control a financial system for the users, by the users. DeFi is the culmination of these tools and the efforts of global communities of early builders and users, all collectively committed to pushing beyond the limits mainstream finance.
- End of 2017 was when MakerDAO, which is widely agreed to be the first true DeFi DApp, launched on Ethereum. The decentralized finance ecosystem has blossomed across a variety of teeming sectors. Blossomed, because the total value locked (TVL) in DeFi — akin to assets under management (AUM) — has reached as high as +$101 Billion as of October 2021.
- Essentially DeFi is the way to give financial freedom back to the people. Innovation is rapid, in some ways similar to what Wall Street was doing with financial derivatives 30 years ago, but DeFi is doing all of this in a transparent way and inclusive, where anyone with an internet connection and a crypto wallet can join.
- Previously the way one would make money in the financial markets, such as Wall Street - by being not transparent, by not passing information, making the spreads (between buy and sell prices) as everything was hidden. In complete contrast, DeFi blockchains are all public record by definition.
- DeFi is like smart money legos - With each new project, product, or service launched on Ethereum, you have one more money lego in your collection. And by piecing together existing components of DeFi, you can combine, modify, or create powerful new finance tools out of these money legos.
- The emergence of DeFi is the first major blow to traditional financial institutions, such as banks and investment firms. As some countries will eventually either release their own digital currency, centralized digital currency, becoming a purely communist nation or adopting one of the decentralized blockchains such as Ethereum or even Bitcoin as the backbone for a monetary system. Banks will simply disappear as neither the consumers nor the governments would need them anymore.
    - Decentralized - Bitcoin became legal tender in El Salvador in 2021.
    - Centralized - China has introduced their own Digital Currency Electronic Payment (DCEP) in 2021.
        - Nigeria is looking to pilot their own digital currency, as well.

What can you do with DeFi?

- Borrowing / Lending
    - One of the most popular use cases of DeFi is borrowing and lending crypto. In particular, lending is an extremely popular way to earn passive income in DeFi. And while you may think lending to a stranger sounds risky, most loans made in DeFi are secured via smart contracts with more collateral than borrowed value. This reduces the risk for lenders.
        - Notable DeFi borrowing and lending protocols include Aave, Compound, and Liquity.
- DEXes (Decentralized Exchanges)
    - Decentralized exchanges, or DEXes for short, are protocols that allow users to buy, sell, or trade cryptocurrencies or any tokens. Because they run on the Ethereum blockchain, these exchanges operate without a central authority. Instead, the smart contracts enforce the rules, execute trades, and securely handle funds when necessary.
        - Ethereum example is UniSwap.
        - Avalanche Network example is Pangolin.
    - Moreover, unlike a centralized exchange there's often no need to deposit your funds before making your swap.
- Derivatives
    - In mainstream finance, a derivative is a financial contract between two or more parties, the value of which is determined by the performance of a specific asset. On Ethereum, an endless variety of derivatives can be created and secured via smart contracts without the need for intermediaries.
- Assets
    - Tokenized assets and asset management is a quickly growing sector of DeFi. Existing financial assets deployed to the blockchain as tokens fit nicely into DeFi protocols, extending their utility.
    - Additionally, asset management protocols allow investors to put their money in the hands of smart contracts or fund managers to manage their portfolio. Other asset management protocols, such as Set Protocol, employ automated strategies such as periodic rebalancing following technical indicators and beyond.
    - DeFi leads to the creation of new asset or sub-asset classes.
- Decentralization may vary
    - "Decentralization" in DeFi refers to whether tokens and DApps can run totally independently and without administrative interference from anyone via smart contracts. There are varying degrees of decentralization when it comes to DeFi services.

Token Economics

Blockchain technology is said to have a transformative effects on the very foundations of how our economies function. This new form of distributed economy may be called token economics, also termed crypto economics. Economic forces are everywhere, they shape and structure our everyday lives in how we organize people, resources and technology to create an exchange of value within society, during the modern era those forces came to be channeled and structured within a particular set of centralized bureaucratic institutions, based around the nation-state and the enterprise but today the proliferation of the information networks is once again unleashing those economic forces.

A new economic system that is being built on top of these previously disconnected building blocks, one that is truly global that reflects the underlying logic of services an economic model that is for the first time in harmony with its underlying technology of information.

These emerging token networks now offer the potential for unleashing a massive wave of creativity and innovation as vast flows of financial capital and supply chain information start flowing along these newly built channels. Trillions of dollars of securities are now about to migrate on the blockchain networks; equities, bonds, venture capital, not to mention the world's currencies with trillions of dollars said to migrate to this global cloud computing infrastructure of the blockchain in the coming years, the stakes are high as financial and economic sovereignty appears to be slipping out of the fingers of nation-states.

Token economics is an opportunity to revisit the foundations of economic organization and from that to reconstruct a new form of economy that is very different from the industrial model that we know so well, it is an exercise that is of critical importance to the development of a sustainable model to economic developments in the age of information, globalization and billions of people wishing to join a formal economic system that is already showing major signs of stress. This is no longer about politics, policies or protesting the technology is reaching maturity, we now really stand at a point where we can literally design economic systems from the ground.

What is so powerful about this revolution, is that it does not require large-scale political coordination, indeed it actually bypasses it altogether, instead employing a highly modular and granular transition. This new economic paradigm holds out the potential to build new forms of economic organization, networks that go beyond pure economic utility and GDP to incorporate all relevant parameters and value sources to capture, define and deliver what people really value. A distribution economy could be more open and thus inclusive in harnessing the efforts of the many instead of the few.

Existing large platform, organizations such as Google, Facebook (Meta) etc. that have arisen with the developments of the Internet's are still centralized around the platform providers, creating many current issues around; security, data privacy, control, alignment of incentives, concentration of

wealth and power. Blockchains latest designed protocols that provide the same capacities for people to collaborate within large peer networks but this time without the need for the centralized entity.

Through the use of tokens, the network is converted into a token market, with the market mechanism used to coordinate it in a decentralized fashion. By removing the centralized components, this works to align the incentives of members better and to turn businesses into something more like communities or ecosystems. By removing the centralized components that is controlling the overall network and operating it for profits, the individuals in the network become more aligned with the whole, this alignment between the individuals in the whole network is realized through the token, because as the value of the whole organization increases, this increase in the value of the platform does not get sucked up by management and shareholders but in fact gets distributed across the network itself by accruing to all of those that hold the token.

This is how and why in a token economy, the description of the industrial age that was primarily designed to create a profit for its owners is greatly reduced and replaced by these token networks which are more like public utilities as profit does not get taken out by shareholders but instead is continuously reinvested and redistributed to the users of the network through the utility token that they must hold to use the network.

The blockchain is a new modality for organizing society and economy, as such it is often referred to as an institutional technology. This isn't a story about how the economy grows because of this new technology, it's a story about how we can create new economies in ways that we could never create new economies. It used to be that you have to have governments, a nation-state, a money system and laws, legislation and all of those things and there's 193 economies in the world or however many nations there are. We are about to enter a world, where the number of economies in the world may well be measured in the billions, not the small hundreds and these things will be largely built on technologies like the blockchain. Once one sees that this a governance technology, an institutional technological that is revolutionary, which has been largely missed.

Blockchains are distributed systems with extreme network effects, they're designed to push outwards - the more people and organizations they bring into common systems of coordination, the stronger they become. As blockchain becomes this globally distributed cloud computer that it promises to be, it will become extremely easy to build, secure automated services on top of this and amass micro payments in a frictionless fashion, those services will be borderless as they're running on a globally distributed computer.

Likewise, it's important to note, that they will not be limited to the traditional offerings of the private sector but will also now include public services. For the first time in centuries, nation-states will find that they're having to compete with global token networks when it comes the provisioning of public services. It will be very difficult for individual organizations to compete with these global public utility networks that support whole ecosystems of users, particularly those that managed to

align incentives in more productive ways and are able to harness the productive capacities of the many instead of the few along more dimensions of both intrinsic and extrinsic motives, similar to the rise of Google and Facebook these token networks will be very formidable actors in the global economy and that will happen just as fast, if not faster this time.

We are seeing the astronomical rise of a new model for the funding of technology companies called initial coin offerings (ICO), in 2017 the amount of money raised by startups via ICOs surpassed early-stage venture capital funding for Internet companies. Within the space of just a few months, ICOs went from almost nowhere to today where new blockchain projects are able to attract hundreds of millions of dollars and billions by offering tokens directly, for anyone in the world with an internet connection to purchase.

This illustrates one of the important aspects to notes which is that these networks are very autonomous a network can fund its own initial developments through ICO but not only this, it can then fund its own future growth through simply increasing the number of tokens and giving those to members who present initiatives projects or other forms of work that will be beneficial to the future success of the ecosystem, the network inflates its own tokens gives those new tokens to projects that will increase its future service delivery and thus will work to deflate the token in the future when more people demand that added future service.

We need to understand that we're dealing with the actual invention of something extraordinary new and very powerful and that is the ability to build economic "games" that actually are organizations and which are controlled by a community who are vested in the "game".

Token economies can be understood as a new way of coordinating human activity in a decentralized fashion, this being done through peer exchanges within market networks. It is common to compare the invention of the blockchain technology with the Internet, in this respect it is often said that the blockchain is Internet 2.0. The Internet has been a powerful tool that has revolutionized the way we interact but if anything this comparison under-sells the significance of the blockchain.

We can think of token economies as a way for people to mimic the social dynamics found in certain highly social creatures like bees, ants and termites as a way to promote and ideally achieve effective collective organization. By recording individual actions on a distributed database the blockchain makes it possible for people to coordinate themselves indirectly and collaborate on a global scale without any centralized authority or hierarchical structure.

This is something quite new in human civilization, as until very recently the basic premise has been that order and organization are achieved by centralized authority. Token economics turns these centralized institutions of the Industrial Age into distributed token markets, the critical change that is coming about, is that we are now able to design token systems that work to incentivize people's behavior towards coordinated outcomes without that coordination being imposed by some centralized Authority.

One of the interesting properties of token economics is that it provides a new way to fund and incentivize these newly formed distributed networks, to create markets, communities where there wasn't such a market or community before.

Tokens (Coins)

- A token is a quantified unit of value; tokens can be generic or fungible;
    - Generic such as social capital tokens, natural capital tokens, cultural tokens, community tokens or;
    - Fungible which is traditional currency, i.e. cryptocurrency.
- The capacity to differentiate between different forms of value is made possible by the programmability of token units. Because tokens are digital, they are also programmable which enables one to specify certain rules for that token and have these rules executed, when it is exchanged thus enabling certain constraints or possibilities in its usage.
    - One can specify that a certain token is only spendable under certain terms or specify how it can be converted. For example, one could program the tokens so it could not be exchanged for diamonds, that are mined at a particular location in the world, known for its use of slave labor. In this way, the token is not just a unit of utility but also expresses social values.
    - Likewise, one could create a health care allowance in euros/dollars, that could only be used to pay for health care at certified parties. These measures automatically lead to a considerable decrease in bureaucracy.
- This programmable token system works to shift our economies from a single-value model to a multi-value model. They create different types of value and economies but still retain the possibility of exchange between them.
- Tokens define whatever is of value within that organization and the market system is used as a disturbed coordination mechanism for managing and growing that resource.
- Let's take a use case – Data Storage Centers, Amazon and Microsoft have the largest data storage centers, however there is a large source of untapped storage which is everyone's personal computer storage, so FileCoin came to utilize this untapped source of storage in a distributed fashion, therefore creating a distributed token economy.
    - Tokens such as Filecoin's can be exchanged for other currencies or members can hold on to their tokens, whose value may appreciate as the networks grow over time.
    - This illustrates a very interesting aspect of tokens, anyone who uses the system is also an investor in the system. Thus tokens merge investment capital and liquid exchange capital in new ways.
- In the traditional capitalist model, we have a divide between owners of capital and workers, a divide between investment capital and liquid exchanged currencies.

- The shares of a company are not the same thing as what people get paid with for working in that enterprise and use for everyday exchanges in the market. This creates the notorious divide within the industrial economy, between the capitalists that make money off their investments and the workers that have to stay, selling their labor for money without ownership.
- Tokens represent both the inherent value of the community, which is its capital investment and they are also units of exchange, within that ecosystem.
- Investors become users and users become investors, interests are aligned with all.

Non-Fungible Token (NFT)

Non-Fungible Token means that something cannot be exchanged for another item, because it is unique; for instance, one piece of art is not equal to another, both have unique properties.

Fungible items on the other hand can be exchanged for one another; for instance, one dollar or bitcoin is always equal to another.

- NFTs are tokens (essentially smart contracts) that live on the blockchain that represent ownership of unique items. This is helpful, because tracking who owns a digital file is tricky, because it can be copied and distributed effortlessly, so how can one prove as being the original owner, when everyone has an identical copy of the file.
- NFTs solve the mentioned problem. Imagine that you have made a piece of digital art, essentially a JPEG on your computer. You can create or "mint" an NFT out of this. The NFT that represents your art will contain information about it, such as;
    - A unique fingerprint (hash) of the file
    - Token name
    - Token symbol
- This created token (NFT) will be stored on the blockchain and now you as the artist become the owner and you can sell that token by creating a transaction on the blockchain.
    - Also, NFTs have a feature that you can enable that will pay you a percentage every time the NFT is sold or changes hands, making sure that if your work gets popular and grows in value, you'll see some of that benefit, in the form of royalties.
- The blockchain makes sure that this information can never be tampered with and allows you to track the current ownee and for how much has been sold in the past.
- It's important to note that the art work itself is not stored within the NFT or the blockchain, but rather only its attributes such as;
    - Unique fingerprint (hash)
    - Token name & symbol
    - Link to file on IPFS (optionally) – we will get to IPFS later.

- Aside from digital art work, NFTs can be used to sell concert tickets, domain names, in-game items, real-estate and basically anything that is unique or limited) and needs proof of ownership.
    - For example - The Founder of Twitter sold his first tweet as an NFT and while anyone can see that tweet on his profile, now only one person can own it, that person paid over 1630 Ethereum coins (2.9 million USD at the time of purchase.)
    - You can even make an NFT out of a video which can be purchased and the buyer becomes the owner of the video, even though it is free to watch for everyone.
    - Worth is determined by what people are willing to pay for it - prices are determined by demand and supply. Be mindful that a highly priced NFT might be worthless, if nobody is willing to buy it.
- Sports, Celebrity, Collectors craze
    - Marvel, NBA, Star Wars, Producers, Artists, Celebrities, Billionaires and Media Moguls like Mark Cuban, Kevin O'Leary, Gary Vaynerchuk and the list of those who are deeply invested and praise the immense potential of Blockchain, Ethereum, NFTs, Cryptocurrency realm keep growing, as more people become aware and understand the revolution happening through technology.

Key takeaways

- Possibilities for Collaboration: Brands can work alongside influencers to create exclusive NFTs for their customers. It works in the same way as any brand/influencer collaboration, but with a higher and more exciting innovation touch.
- Ownership: NFTs are like having an ownership log, similar to taking a book out from the library. When an influencer has had ownership of an NFT, the hype is already driven. Influencer and Brand NFT collaboration is the digital equivalent of auctioning off a piece of clothing or item belonging to a person of influence.
- Brand/Influencer collaboration breeds awareness: Like influencers who promote products on their social media, they could use their popularity to influence people to invest in NFTs.

ENS - Ethereum Name Service

When the internet first started out websites were accessed through IP addresses, a long string of numbers that were not very user friendly. To improve the use case of the world wide web, developers designed DNS, which allowed users to use names instead of random, hard to remember numbers. Thankfully, now you can find your favorite crypto services at Oobit.com instead of 104.26.10.222.

- In Ethereum's parallel aim to make crypto as easy to use as possible, the network introduced ENS so that users can bypass long complex codes to access the eth addresses that they need.
    - For example, a regular Ethereum address looks like this: 0x89205A3A3b2A69De6Dbf7f01ED13B2108B2c43e7, and the majority of crypto wallets work with such. Unsurprisingly, such addresses are easy to misspell and hard to memorize.
    - At its core, Ethereum Name Service is a distributed domain name provider linking information to a human-readable name in a secure and decentralized manner. Built on Ethereum and available to all of its products, users can now send ETH and ERC tokens to name.eth instead of the previous alphanumeric codes.
- Main features of ENS
    - Your own web3 username
        - No more sandboxed (isolated) usernames. Own your username, store an avatar and other profile data, and use it across services.
    - One name for all of your addresses
        - No more copying and pasting long addresses. Use your ENS name to store all of your addresses and receive any cryptocurrency, token, or NFT.
    - Decentralized Websites
        - Launch censorship-resistant decentralized websites with ENS. Upload your website to IPFS and access it with your ENS name.
            - The InterPlanetary File System (IPFS) is a protocol and peer-to-peer network for storing and sharing data in a distributed file system.
                - A peer-to-peer hypermedia protocol designed to preserve and grow humanity's knowledge by making the web upgradeable, resilient, and more open.
                    - More on IPFS later.
    - Use Traditional Domains
        - The native name suffix for ENS is .ETH, which has the full security benefits of being blockchain-native.

        - You can also use ENS with DNS names you already own. ENS supports most DNS names, including:
            - .com, .org, .io, .app, .xyz and .art
    - Growing Ecosystem
        - Crypto wallets, dApps and browsers
            - Examples such as Coinbase, Uniswap and Brave

InterPlanetary File System (IPFS)

Today the internet is such an important tool in our everyday life, we use it to consume media, to communicate with our friends and colleagues, to learn, handle our finances and much more.

- The web as we know it has a major problem, the information on it is centralized, it's all stored on big server farms, which are usually controlled by a few companies. Have you ever wondered what would happen if sites like YouTube and Wikipedia went offline.
- Centralization has another problem, which is censorship. Because content is hosted on just a few servers, it's easy for governments to block access to them - in 2017 Turkey ordered internet providers to block access to Wikipedia, because the administration called it a "threat to national security".
- We have gotten used to this centralized model, partly also because of our high expectations for the web - we want pages, images and videos to load instantly and we want them in high quality.
    - Centralizing servers allows companies to have complete control over how fast it can deliver all of this content.
    - Another reason we have been using this model, is that there hasn't been a good, fast alternative.
- That's all changing, meet the InterPlanetary File System (IPFS). That's a fancy name and they have ambitious goals as well - they want to make the web a completely distributed network, by running it on-top a peer-to-peer network, that runs very similar to how bit torrent works.
- Before we can look at how IPFS plans on accomplishing its goals, first let us understand how we access content on the web right now;
    - Let's say you want to download a photo from the internet, when you do that, you tell the computer exactly where to find the photo (ip address or domain name), which is called "location based addressing". You tell the computer where to get the information but if that location isn't accessible, in other words the server is down, you won't get that photo.

        - However, there is a high chance that someone else has downloaded that picture before and still has a copy of it, but yet your computer won't be able to grab a copy from that person.
    - To fix this, IPFS goes from "~~location~~ ***content*** based addressing", so instead of saying *where* to find the resource, you just say *what* it is that you want.
        - How does this work? Every file has a unique hash (comparable to a fingerprint), when you want to download a certain file, you just ask the network, who has the file with this hash and someone on the IPFS network will provide it to you.
            - Because you use a hash function to request the file, you can verify what you have received - you check if the hash matches with what you have received.
                - Security is built-in.
            - Another feature of using hashes to address content is deduplication - when multiple people publish the same file on IPFS, it will only be created once and that makes the network very efficient.
    - Let's take a look at how IPFS stores files and makes them accessible to others - Files are stored inside IPFS objects and these objects can store up to 256kb worth of data. They can also contain links to other IPFS objects.
        - A simple "Hello World" text file can be in a single IPFS object, but what about files that are larger than 256kb like an image or a video for instance? Those are split up into multiple IPFS objects that are all 256kb in size and afterwards the system will create an empty IPFS object that links to all the other pieces of the file.
    - IPFS data architecture is very simple, but yet it can be very powerful. This architecture allows us to really use it as a file system.
    - Additionally, because IPFS uses content based addressing, once something is added, it cannot be changed anymore. It is an immutable data store, much like a blockchain.
    - How do we change stuff on it?
        - Versioning - IPFS supports versioning of your files. Let's say you're working on an important document that you want to share with everyone over IPFS.
        - When you do that, IPFS will create a new *Commit* object for you. This object is really basic, it just tells IPFS which commit went before it and it links to the IPFS object of your file.
        - Let's imagine that after a while, you want to update this file, well you just add your updated file to IPFS, and the software will create a new *commit* object for your file. This new commit object will be linked to your previous commit, and this process can be repeated endlessly.

        - IPFS will make sure that your file plus its entire history is accessible to other notes on the network.
    - While this all sounds great, nothing is perfect. The biggest challenge with IPFS is keeping files available.
        - Every node on the network keeps a hash of the files that it has downloaded and helps to share them if other people need them, but if a specific file is hosted by a low number of nodes and the nodes go offline, then the files become unavailable and no one can grab a copy of it until they are back online.
            - FileCoin has stepped up with two possible solutions for this challenge;
                - Incentivize nodes to make them available
                - Proactively distribute files.
            - FileCoin is created by the same team of people that created IPFS. It is essentially a blockchain built on-top of IPFS, that wants to create a decentralized market for storage.
                - If you have free space on your hard drive, you can rent it out to others and make money from it in the process.
            - FileCoin creates strong incentives for nodes to keep the files online for as long as possible, otherwise they won't get reported.
                - The system also makes sure that files are replicated on many notes, so that they cannot become unavailable.
    - Applications of IPFS - In 2017 the Turkish government decided to block access to Wikipedia and the people behind IPFS responded by taking the Turkish Wikipedia and putting a copy of it on IPFS and because IPFS is distributed and there is no central service, the government can't block it.
    - Another application is DTube, which is basically a site like YouTube, but entirely distributed and hosted on IPFS.
        - Anyone can publish videos and help to support the network.
    - You may have wondered why is IPFS called the Interplanetary File System? Is it suited to run across multiple planets?
        - Let's assume that we have a base on Mars. Communicating from Mars to Earth is quite difficult. Depending on the position of the two planets, a signal can take 4-24 minutes to travel between them.

        - Let's take the best case scenario - you're on Mars, you open your laptop, and you request a copy of the Wikipedia page of planet Earth, because you had forgotten what it is like there.
            - The request to Wikipedia takes 4 minutes to travel to earth and when it arrives there, it is sent over the internet to the Wikipedia servers, who responds in just a few milliseconds. That response however needs to travel another 4 minutes back to Mars, so this can take anything from 8 minutes to 48 minutes to reach you on Mars.
        - With IPFS it is possible to cache large parts of the internet on Mars, so if someone has already requested a page that you want to download, it can come straight from a node on Mars, making that page load just as fast as it would on Earth.
        - In summary, IPFS could be used to distribute parts of the internet across multiple planets.
    - IPFS is an extremely ambitious project that can lead to a truly decentralized internet.

Ethereum 2.0 Vision

The Ethereum protocol that launched in 2015 has had incredible success. But the Ethereum community always expected that a few key upgrades would be necessary to unlock Ethereum's full potential.

- High demand is driving up transaction fees that make Ethereum expensive for the average user. The disk space needed to run an Ethereum client is growing at a fast rate. And the underlying proof-of-work consensus algorithm that keeps Ethereum secure and decentralized has a big environmental impact.
- Now that the technology is ready, these upgrades will re-architect Ethereum to make it more scalable, secure, and sustainable – to make life better for existing users and entice new ones. All while preserving Ethereum's core value of decentralization.
    - This means there's no on-switch for Eth2. Improvements will ship incrementally over time.
- Overview of Ethereum 2.0 (ETH 2.0)
    - A set of interconnected upgrades to the Ethereum network, that aims at making Ethereum more scalable, more secure and sustainable. These changes are being worked on by multiple developer teams, each team focusing on building a specific part of the whole upgrade.
- Scalability - The current Ethereum network supports only 15 transactions per second (tps), this becomes a limiting factor when it comes to on-boarding millions of new users and launching many more dApps.

        - ETH 2.0 aims to support 1000s of transactions per second (above 100,000 has been mentioned by Vitalik Buterin the main founder of Ethereum.
            - In contrast, major credit card company Visa is clocked at 1,700 transactions per second (while they officially claim 24,000 tps).
        - Important note is that the increase in transactions per second should not come at the cost of increasing the size of the node/s in the network.
    - Security - Security of a decentralized network is always one of the top priorities. ETH 2.0 aims at increasing the security of the network against all forms of attack; including a 51% attack, where someone can force through fraudulent changes, by controlling the majority of the network.
    - Sustainability - The well-known proof-of-work based consensus model used by the current Ethereum network requires a lot of computing power and energy (electricity).
        - ETH 2.0 aims to make Ethereum better for the environment, by replacing energy intensive proof-of-work with proof-of-stake.
        - Interestingly all of these goals have been essentially always in the Ethereum Roadmap and were discussed even when the network was officially launched.

Ethereum 2.0 is one of the most anticipated releases in the entire blockchain space, this is a new and improved version of Ethereum that we have been very hearing about for a long time, it's going to get the masses ready and able to adopt the blockchain and distributed technologies revolution.

Decentralized Autonomous Organization (DAO)

Next generation of internet technologies, built on the blockchain is an - Institutional Technology. At the heart of social organizations and all forms of institutions is the question of how we work together, by exchanging value within a trusted environment.

The blockchain is technology that enables automated trust and the automated frictionless value-exchange. This capacity to automate the basic workings of social institutions, coupled with increased inter-connectivity, means that we increasingly have the technological means to create massive organizations that are truly distributed and automated, something we have never seen before.

A potential that is only limited by one's imagination - this potential of the blockchain to revolutionize human social institutions is most clearly demonstrated in what are called - Decentralized Autonomous Organization (DAO), that give us a glimpse into the future. These can also be called Distributed Autonomous Organization.

Although truly autonomous decentralized organizations are something new, they can also be seen as just one more step in a millennia old process of institutional evolution - a process in which we have gone from organizations based fully upon the specific characteristics of their leaders within hierarchical structure to the modern bureaucratic organization to today's platform economy.

- Platform economy - where we have moved into semi-distributed organizations, where businesses operate platforms where the rules are executed by computer code automatically.
- In our current platform economy, which has been built on web 2.0 technologies over the past decade, organizations are a hybrid of distributed automated platforms and centralized business organizations managed by people.
    - Platforms such as YouTube, AliBaba, WeChat, UpWork or Uber represent a combination of both - a centralized digital platform operated by a private business and distributed user-generated systems built on the platform by hundreds of millions of users.
- However, things are changing fast at present, and the web 2.0 that created these platforms is giving way to a new era in web technology, with the rise of the blockchain.
- Blockchain technology offers the possibility to dis-intermediate these platforms by creating fully distributed systems of organization, without need for a centralized organization supporting the platform.
- With the blockchain, we now have the technology to create truly distributed organizations at a global scale, something that we didn't have previously.
- Decentralized Autonomous Organization (also called DAO) is an organization that is run by rules, that are created by its members, through a consensus process and written to a set of contracts that are run by a computer code.
- On a more technical level, a DAO is an organization that is managed in rules and coded in smart contracts, which are run on the blockchain.
- DAOs are online platform communities, with their resources organized according to rules agreed on in advance and set out in its code.
- DAOs are an open-source software, capable of modification through member consensus.
- DAOs are essentially a set of complex smart contracts that combine to form a set of rules that manage the operations of a group of members and their resources.
- Distributed organizations are based on a few core principles to their design, which are ultimately trying to support a self-sustaining system of organization, through local feedback loops.
- Instead of having formal management structures monitoring and coordinating the organization from a central point, decentralized organizations work through signaling systems, which are distributed feedback loops as means for aligning the individual with the group.

- Distributed organizations tackle a problem by creating an infrastructure of cooperation, done through the local interactions between members and signaling systems, which are designed to create self-organizing systems.
    - A good example for such a signaling system would be feedback a buyer leaves for a seller on ebay, thus creating a signal to others about the seller's trustworthiness via only a peer-to-peer interaction.
- At the heart of these distributed organizations is the idea that groups are about value as measured by some form of a token.
    - With distributed ledgers, we can create markets out of tokens that represent whatever value system the organization is based around. It is this value - token system and market mechanism that are at the heart of the organization. They regulate the system and define any one person's position within the group.
    - The corresponding value and reputation that they have received through their interaction with other members, define their status within the community. All of this is encoded as tokens on the blockchain.
- Distributed organizations try to draw upon the intelligence of many people, by drawing upon their specific local knowledge. They try to avoid situations where people can become over-influenced or persuaded by any highly influential member.
- Such distributed organizations try to harness a diversity of perspectives from all the members, embodying the process of evolution in their design, similar to the evolutionary process that is built into the market economy.
- Distributed organizations work through a process whereby members create a stock of new ideas, decisions or initiatives and then members essentially invest their tokens into those that they believe most viable and receive rewards if the initiative is beneficial to the organization. Thus mimicking the process of evolution, where new varieties are created and selection is performed, based upon their contribution to the whole organization.
- Distributed Autonomous Organizations are very much in their infancy, although many promising projects have sprung up and the sky's the limit for what is ahead of us, as we learn and adopt these technologies.
    - Anahata DAO, Backfeed, Colony and more.
- Although such systems may be considered experiential in nature, their potential is not to be under-estimated and they will grow as the underlying technology develops and our understanding of distributed self-organizing systems matures.
- The blockchain and new distributed models of governance can play a major role in providing the trust infrastructure, the platforms and off-the-shelf organizational solutions to massive social systems, the type that would be required to develop functioning, thriving global institutions.
    - Notable project - Aragon (where you can create your own DAO and tokenomics),

The four pillars of a decentralized society

- As we can go back in the history of mankind, we find that most societies have lived together in small, decentralized network communities of about 30-70 people. Everybody knew everybody and it was hard to get away with doing bad things.
- Then about 10,000 years ago something happened that changed the course of history - the invention of agriculture, which allowed people to produce food at a scale they hadn't been able to before. It allowed not just a few people, but thousands and even millions of people living together in large societies.
- But humans are believed to have a human memory limit, known as Dunbar's number, where we can only remember about 150 persons well. So in these large societies, we could no longer remember everyone that we interacted with, there was a rise of anonymity, which led to threatening the social order.
- This created an opportunity for strong men to arrive, to restore social order. These men instituted social systems that were top-down, centralized, command and control. This kept the social order, but with great power came great abuse, so the people who lived in these centralized societies suffered great abuses and paid a big price.
- People put up with these abuses for 10,000 years, because it seemed that this was the only way to organize society on a large scale.
- Another change happened about 500 years ago, which started turning the tide of human history back to the decentralized society that we've lived in for thousands and possibly millions of years.
- When you look at the whole span of social evolution, the span of 10,000 years of centralized society, which is really all that we remember is actually just a blip in time, a short transition phase that takes us from decentralized society of our past (which was on a small scale) to a decentralized society of our future, which allows millions and billions of people to live together in a decentralized way.
- People-based trust systems don't scale beyond Dunbar's number, so what allowed us to bridge and transcend Dunbar's number is the emergence of Technology-based trust systems, which scale virtually without limit and centralization.
    - First of these technologies was the printing press about 500 years ago. The printing press has no memory limit and the economics of printing allowed ordinary people everywhere to cheaply record and communicate ideas across the world, free from the restrictions of the centralized state and church (religions).
        - Communicating these ideas freely, without censorship inspired the first democracy movements.
        - People started challenging the state, the church and developed their own ideas of how they could do things.

- But the printing press was only the first of a long series of technologies - most recent of which are the internet and bitcoin, collectively these technologies could be termed "the technology of trust" - A new era in human social evolution.

- Four pillars of "Technology of Trust"
  - Decentralized communications - before we can do anything, we need to communicate what we want to do.
    - Two essential components in the modern world;
      - The Internet - The internet and peer-to-peer decentralized technologies such as Bit torrent are now enabling people to communicate without censorship, so centralized power structures can no longer control the flow of information.
      - Cryptography
        - The internet by itself is not enough, because without cryptography, the centralized structures can use surveillance and censorship of what we communicate and this impacts our freedom of speech and thought.
      - For freedom of speech, thought and action we need a privacy-enabled communication system, so the internet plus cryptography gives us that.
  - Decentralized Law - first we communicate what we want to do, then we come into an agreement how we are going to operate
    - Three essential components of a decentralized legal system;
      - Choice of Law - means that we can choose the law that applies to our agreements and interactions; something available or make up our own law.
      - Choice of Judicator - who hears and resolves our disputes.
      - Choice of Enforcer - we can choose who enforces our contracts and legal judgements.
    - It may surprise you to hear, that these seemingly radical ideas are not untested theories, these ideas date prehistory, these were the cornerstones of the legal system of our past.
    - It is only in the past 10,000 years of increasingly centralized societies and legal systems, that we have gradually forgotten these building blocks. Therefore, today it's almost impossible for us to imagine how we can have a legal system that is decentralized as described.
    - It's time to bring back these ideas and to re-introduce them into the modern world, so that we can really operate a decentralized society.
      - Researchers have developed a complete legal framework for a decentralized society that operates on these principles.

            - In fact, these principles and legal systems are already being implemented in businesses and so called "startup cities", following the examples of HongKong and Singapore, there are now entrepreneurs building so-called "startup cities" in developing countries, autonomous regions of developing countries that desperately need it.
            - These "startup cities" are built with these advanced legal systems, that allow people to create society, jobs and generate wealth on a scale that hasn't been possible in today's world. These are very exciting developments.
    - Decentralized Production - allows to by-pass the censorship of centralized systems
        - Two essential elements;
            - Decentralized materials production - includes technologies such as 3D printing, where anyone in the world can download a design from the internet and print their own products at home.
                - This bypasses the restriction that seeks to control the flow of goods across national boundaries.
            - Decentralized energy production - we are starting to produce our own energy cheaply at home, at virtually unlimited qualities.
        - Together these will move us from the days of the Pharaoh, where one person controlled an army of thousands of slaves, today we've got Apple having factories in China with tens of thousands of workers.
        - This will move us to much smaller systems, where people can produce their own goods and services at home, without censorship.
    - Decentralized Finance - essential components are currency and contracting systems
        - The invention of Bitcoin is one of the most important breakthroughs in human history. For the first time, we have a decentralized currency that cannot be censored, it cannot be controlled by any entity, by any government.
        - The invention of Bitcoin has sparked the emergence of a whole new digital finance industry, that is forming an ecosystem that will develop digital products and services.
        - The most important of these is decentralized contracting systems. For the first time, these contracting systems offer a complete, universal transaction platform, so on a single integrated platform, you can do literally any kind of financial and legal transaction.
        - These two technologies of decentralized currency and decentralized contracting platforms give power to ordinary people.
            - Today's financial system is highly centralized, a few people pull the levers of power and we are at their mercy - a stark example is Cyprus,

where people thought they had money saved up for 30-40 years and suddenly they heard that the government was going to confiscate 40% of their assets and there was nothing they could do about it.

- But with these technologies you have the power back in your own hands.

- These are the four pillars of a decentralized society and there is a logical order to them - we communicate about what we want to do, then we agree the terms of our cooperation, then produce what we agree to cooperate on and finally we trade/consume the goods and services we have produced.
- Together these technologies form what is termed "The Technology of Trust", which enable ordinary people to communicate, to come to legal agreements, to build products and services and to trade without inference from 3rd parties.
- The world of the future - imagine a Masai tribe warrior on the plains of Africa, who has no access to the banks and infrastructure that we take for granted in the developed world. He is cut off from the global economy, no bank account, no lawyer, no financial services, all of which severely limits his ability to generate wealth, but he has a mobile phone and now using that mobile phone, he can start with an idea and within hours or soon minutes, with a few clicks he can incorporate a legal entity, connect to a global transaction platform that allows him to safely and securely transact and cooperate with anyone in the world, including people that he's never met nor can he trust them, yet the integrity of the transactions is guaranteed by the technology, a truly trustless system that will dramatically improve people's standard of living.
- The combined force of these technologies will force the old, centralized coercive monopolists to change - they will either become service providers that service us or they will cease to exist.
- A radical transformation has begun in our financial systems, communications system, production systems and more importantly government and legal systems, all of which will lead to an explosion of prosperity and abundance.
- A new vision for a new future - A decentralized network society, where people once again have the power in their own hands to live the lives of their choosing in peace, freedom and prosperity.
- Join us in creating the New Earth.

First Follower: Leadership Lessons from a Dancing Guy

This short 3-minute talks at the TED Conference yesterday and got a standing ovation! They call it "How to Start a Movement")

First Follower: Leadership Lessons from Dancing Guy - video of transcript above

https://youtu.be/fW8amMCVAJQ

Welcome to the Anahata DAO family www.anahatadao.org