A free and open-source Bitcoin course by Area Bitcoin

Table of Contents - Bitcoin 4 All -

Inside Bitcoin: how does Bitcoin work?
(decentralization, blockchain and game theory)

---

6. Bitcoin and Game Theory

6.1 Aligning Incentives for Security
6.2 Why Cooperation Is More Profitable Than Attack
6.3 Solving the Byzantine Generals' Problem

---

7. Proof of Work and Blockchain

7.1 What Is Proof of Work?
7.2 The Role of the Blockchain (Timechain)
7.3 How Hashes Secure the Chain
7.4 Why Blockchain Alone Isn't the Revolution

---

8. Immutability and Verification

8.1 Hash Functions and Block Linking
8.2 Verifying Integrity and Preventing Tampering
8.3 Why Editing Past Records Is Practically Impossible

---

9. Forks and Upgrades

9.1 What Are Forks?
9.2 Soft Forks: Backward-Compatible Updates
9.3 Hard Forks: Creating New Currencies
9.4 Why Bitcoin Avoids Hard Forks

---

10. Final Reflections

10.1 Decentralization as the Key to Bitcoin's Survival
10.2 Why Bitcoin Is Unique and Resilient
10.3 What's Next: Deeper into Mining, Halvings, and Protocol Mechanics

Bitcoin 4 All - Full Text

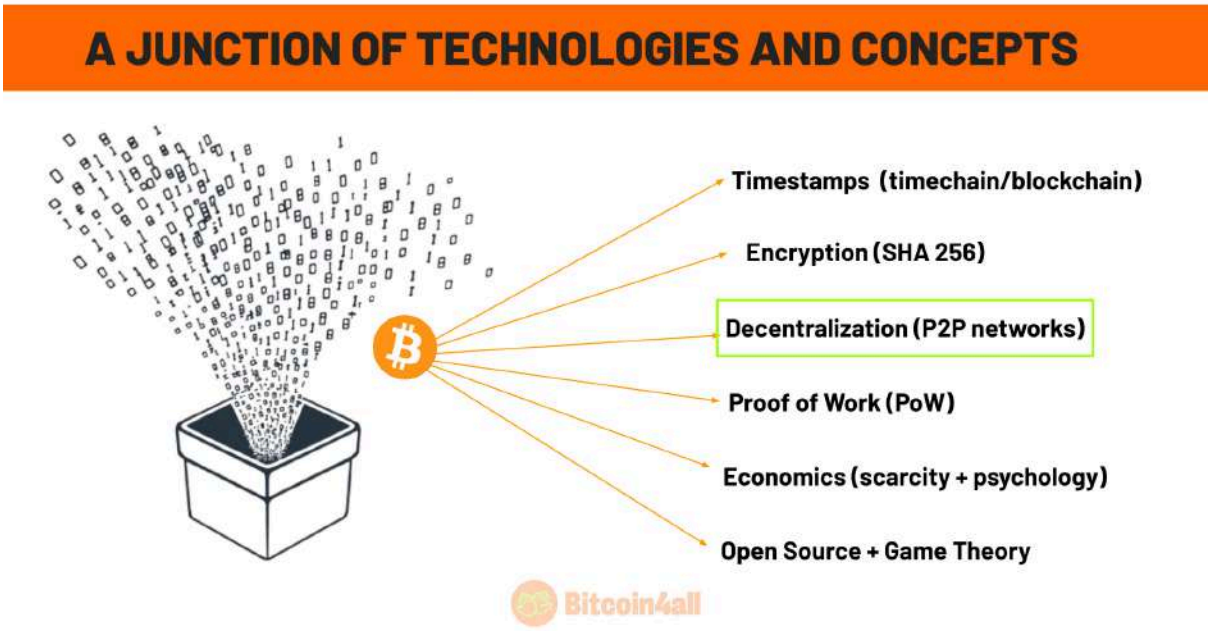
Bitcoin 4 All is a free and open source course created by Area Bitcoin. The goal is to help more people to understand Bitcoin and inspire anyone to be a multiplier of Bitcoin education.

About this eBook

Published by Area Bitcoin – 2025

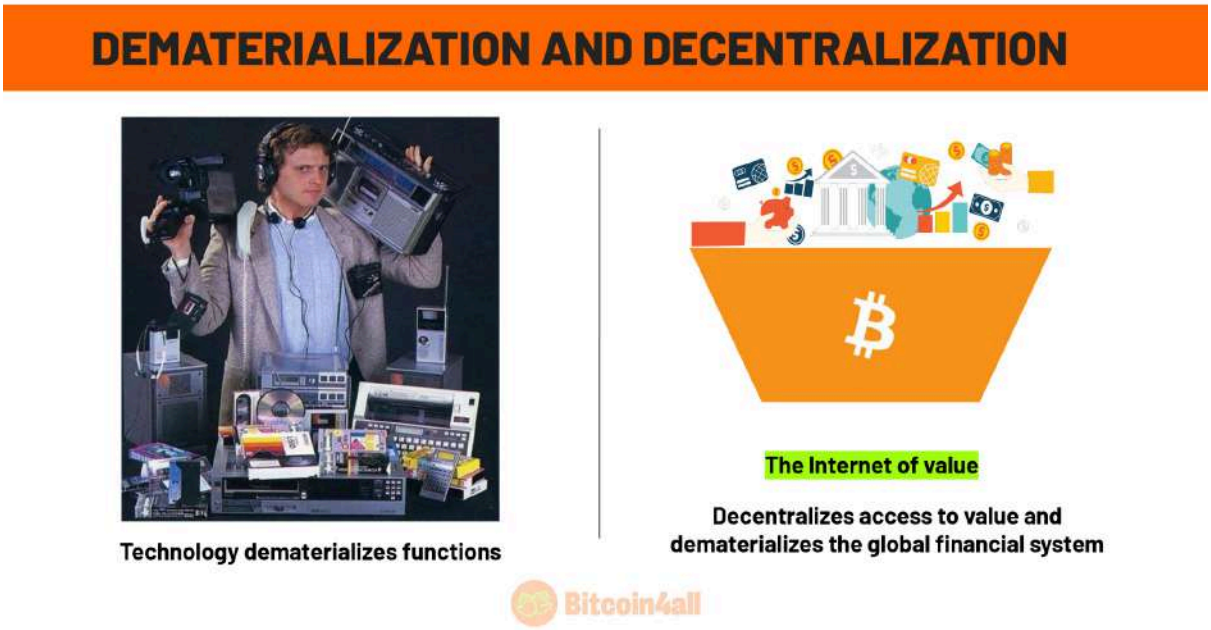
Inside Bitcoin: how does Bitcoin work?
(decentralization, blockchain and game theory)

In this lesson you'll dive into how Bitcoin works, learning about its characteristics, how the blockchain works, mining, halvings and fundamental technical concepts. Don't worry if you don't understand everything at first. Having to revise and rewatch a few times in order to consolidate your learning is absolutely normal. Over time, the concepts will fit together and make more and more sense.



(slide 90) - Bitcoin 4 All

As you noticed in lesson 1, Bitcoin is the combination of several technologies and concepts. Decentralization is what separates Bitcoin from any other invention in recent history.



(slide 91) - Bitcoin 4 All

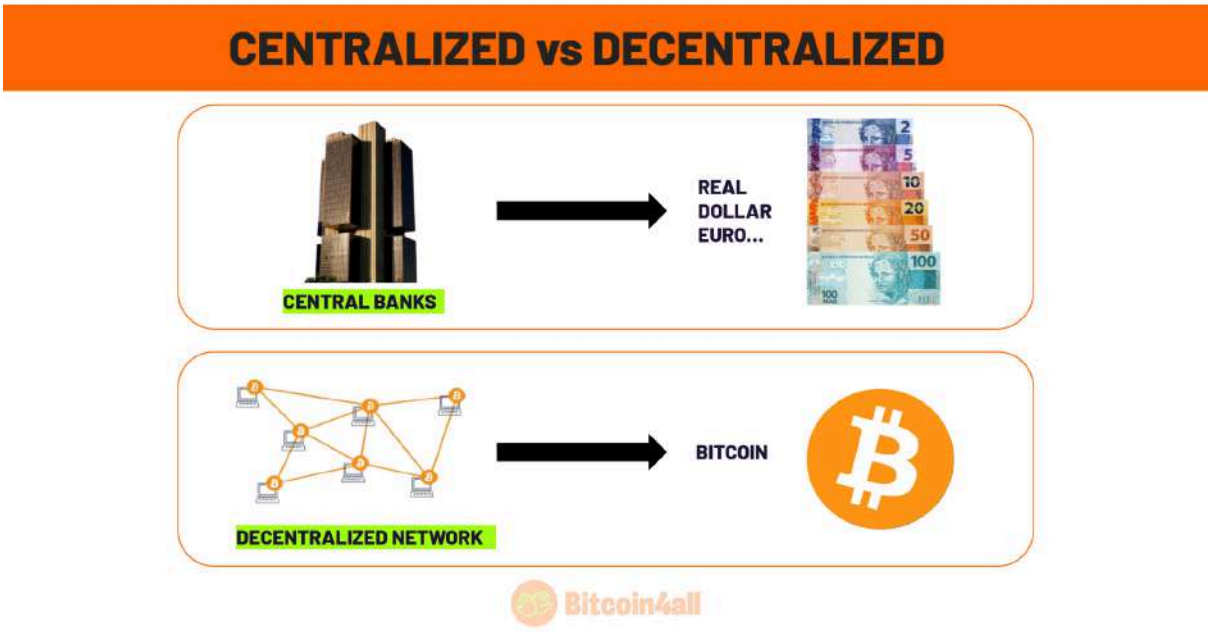
And what has been happening in recent decades is the action of two technological forces acting at the same time: decentralization and the dematerialization of things. Dematerialization began in the 1990s with computers and smartphones, which condensed and dematerialized various devices that we previously only knew in physical form. Radios, diaries, televisions, cameras, calculators, faxes -- all of this has been dematerialized and digitized in the palm of your hand, on your cell phone, in just 20 years. It became all in one.

Bitcoin continues this evolutionary and technological change, bringing both of these effects to the economy and to money. In other words, Bitcoin decentralizes access to value for anyone anywhere in the world without access restrictions and also dematerializes the banking financial system with vaults, ATMs and armored trucks. And if the internet has already decentralized information and changed the world, imagine what Bitcoin can do by decentralizing value and decision-making power. In addition to dematerializing central banks, commercial banks and the properties of sound money.

(slide 92) - Bitcoin 4 All

Bitcoin can only do this because it is decentralized. Without decentralization, Bitcoin would be a company. It is decentralization that sets Bitcoin apart from the rest and provides immutability. If there is no one making decisions for other people, it means that it is a network that is difficult to change. For any change to be made, almost all the participants need to agree with it. And that's not easy at all, whether in Bitcoin or in any system that involves thousands of human beings making decisions. Decentralization is what guarantees the immutability of properties and that Bitcoin's rules will follow suit. It brings confidence that no one could monopolize or corrupt Bitcoin authoritatively.

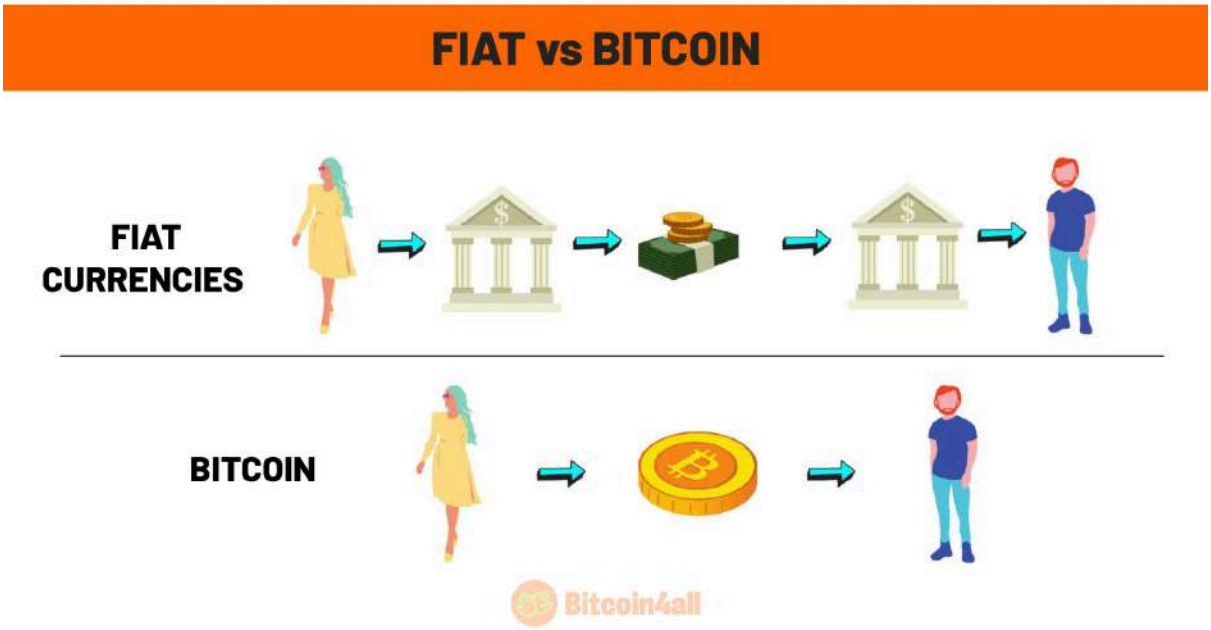
Bitcoin is decentralized because it is a peer-to-peer network. It's made up of computers that connect to each other and follow rules that everyone agrees on. There is no central server coordinating or storing the data (such as the case of centralized networks). It also means that there is no single point of failure. If any computer connected to the network goes down, is destroyed or attacked, the network survives and continues to function because there are thousands of others fulfilling the same function independently.



(slide 93) - Bitcoin 4 All

In practice, this means that there are no intermediaries in Bitcoin. Each person can connect to the network without depending on anyone else, without having to ask permission and without the possibility of being prevented by third parties. This is the opposite of fiat money, which is centralized and makes you depend on numerous entities -- the Minister of the Economy, the head of the Central Bank, payment institutions, banks and so on to access the system.

Central banks determine monetary policies and you don't have the option of not following the rules, you are forced to follow them. Commercial banks, on the other hand, provide access to the system. To participate you need to ask their permission. If you don't meet the requirements, you may not be allowed to create a bank account or they may even close your current one.



(slide 94) - Bitcoin 4 All

Another big difference is when it comes to making transactions.

Currently, when you make a digital transaction, you have to ask your bank to send an amount to someone else's bank. Then, that person's bank deposits the amount in the corresponding account. In a transaction between two people using the fiat banking system, there is at least one intermediary -- a bank -- between two people. If these two people have accounts with different banks, then there will be two banks intermediating the transaction.

Bitcoin is like making a physical money transaction, just like when you buy a product and hand over the notes directly to the other person. With Bitcoin, the value is sent directly to someone else's wallet without necessarily going through some kind of fiat intermediary or bank. Unless you want it to do so: if you choose to trade through exchanges, for example. But it's a choice, not a mandatory route. This completely changes the way the financial system works, because today the fiat system depends on these intermediaries to transfer money online.

It was through cryptography, timestamps, peer-to-peer networks and a robust consensus mechanism that Satoshi Nakamoto managed to digitize the financial system as a whole, without the need for governments or banks.

(slide 95) - Bitcoin 4 All

The Bitcoin network is made up of the code, the miners and the nodes. The code is a set of rules in the form of computer codes and cryptography that guide the participants to coordinate with each other. It determines how records will be made and how the Bitcoin network should work. The code is public and anyone can suggest modifications, audit it for bugs and even copy it. It is this code that is hard to modify and monopolize. It is run by thousands of participants: in order to modify it in a valid way, practically the entire network would have to agree to run a modified version.

You can check out Bitcoin's github, where developers discuss updates and where you can also contribute if you wish. I'll leave the link to Bitcoin's [Github](https://github.com/bitcoin/bitcoin) here under the lesson. The code works through software and the most widely used is Bitcoin Core, an implementation of the original version created by Satoshi Nakamoto.

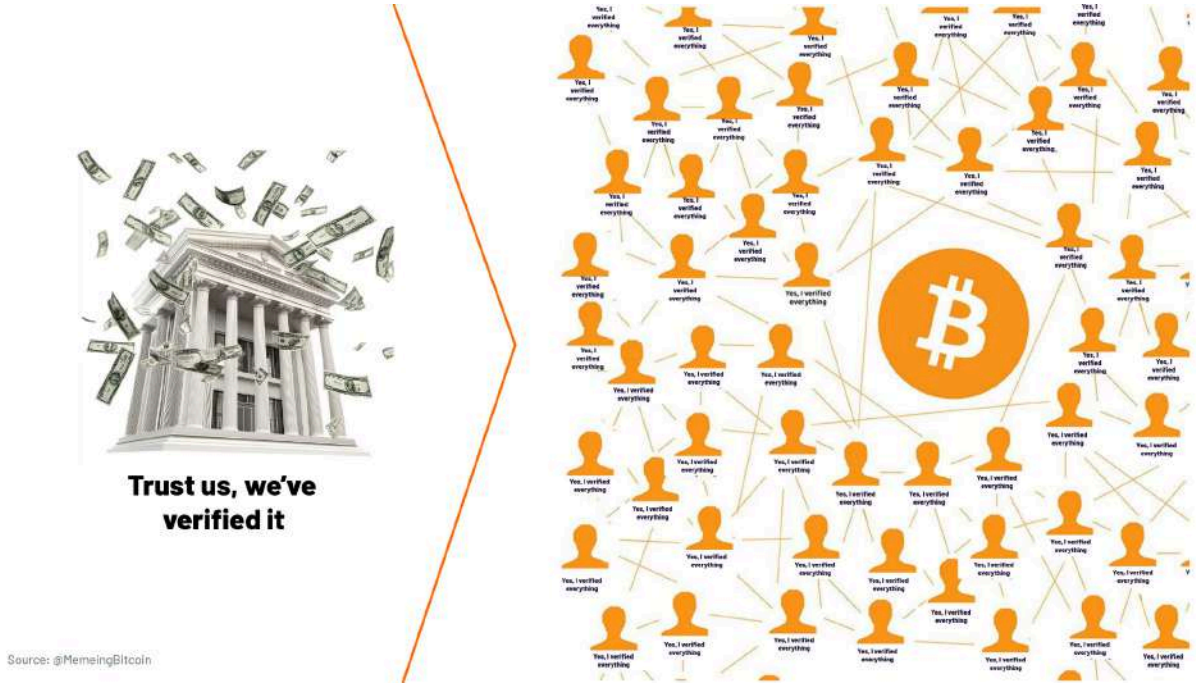
Miners, on the other hand, are the participants who propose the blocks, insert the transactions and defend the network from attacks through computing power. They are the first to receive bitcoin from the network with each mined block.

The third type of network participant are the nodes. Nodes are ordinary computers that check that the miners are following the consensus determined by the code. Nodes are powerful agents of decentralization. After all, it's from nodes that anyone can have a copy of the Bitcoin blockchain on their own computer, decide which version of the code to run and also be part of the Bitcoin network with the autonomy to send their own transactions without depending on anyone else. Even if miners get together to attack Bitcoin, the nodes are the ones that have the power to prevent this attack from being effective. This even happened in the so-called Blocksize Wars which took place in 2016.

(slide 96) - Bitcoin 4 All

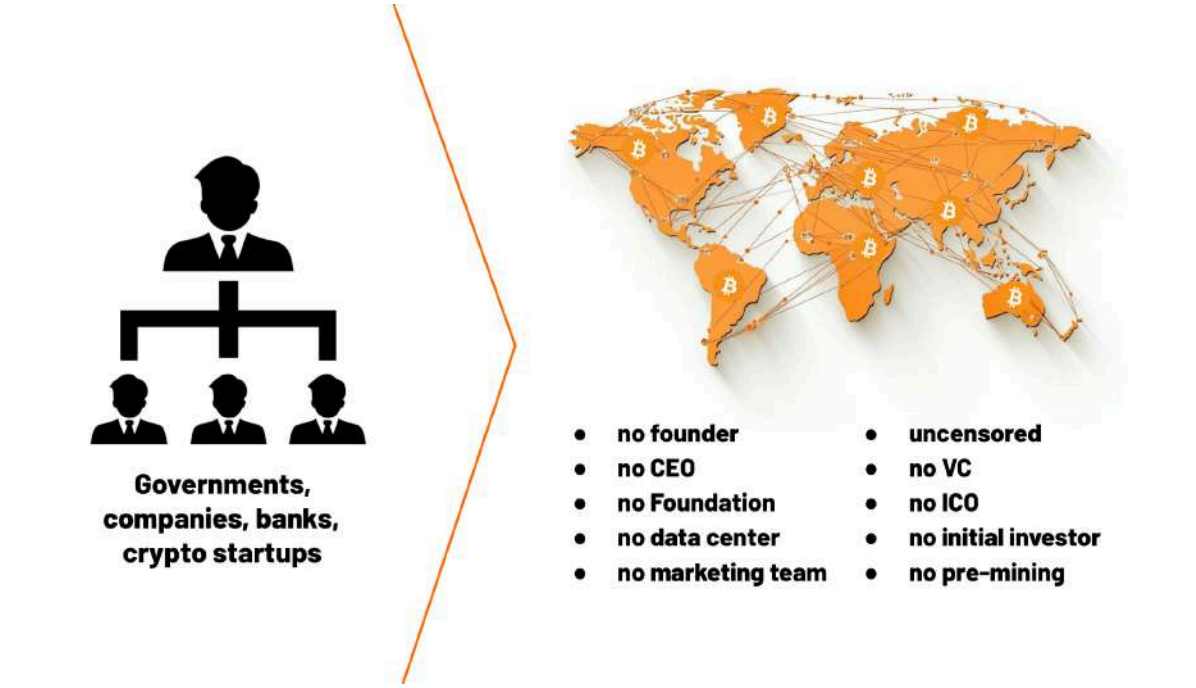
According to the website Bitnodes, there are more than 65,000 Bitcoin nodes operating globally. Most of them -- 65% -- do not have an exact location identified. These thousands of nodes on ordinary computers connected to each other are the ones that make the Bitcoin network the strongest, most resilient and accessible computer system for anyone anywhere in the world to verify. Anyone can run a node and the cost is low. You can even run a node on an old computer you have at home.

The nodes verify the blocks all the time. This is why the Bitcoin network's accounting is a closed loop, because the nodes constantly verify blocks, transactions and that the number of coins circulating is correct. It's a distributed system of records, where the accounts always match up, which is also rather powerful and unique.



(slide 97) - Bitcoin 4 All

Central banks don't allow you to look at their internal accounts or give your opinion directly at meetings. The accounting of a central bank is private and done behind closed doors. The population depends on the data provided by the Central Bank and cannot independently verify or have a direct say in monetary policies. The people don't even choose who will chair the Central Bank! In Bitcoin, anyone can audit the network and suggest improvements, because it is freely accessible.



(slide 98) - Bitcoin 4 All

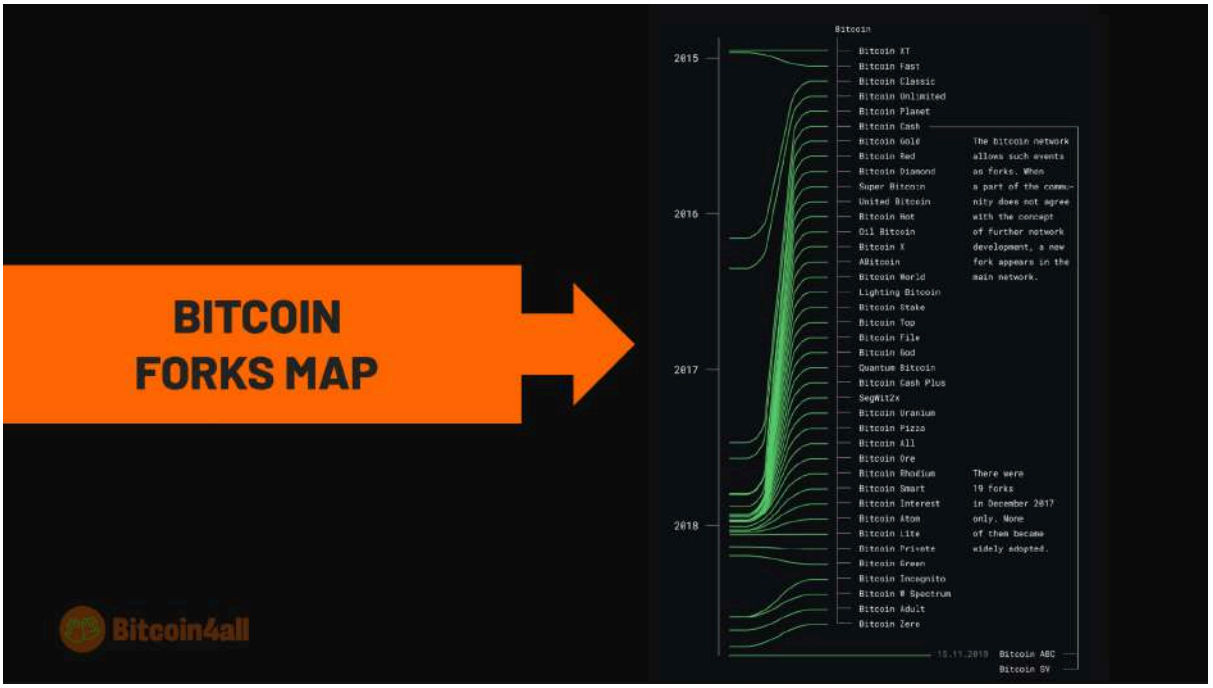
Centralized structures are hierarchical, like a company: there's a CEO, someone making decisions about the next steps, there's a marketing team and a research development team.

They all work through this hierarchy of power. Companies compete with each other to win the market. Cryptocurrencies are like companies and compete with each other for market share by selling utility, just like companies do.

Bitcoin, on the other hand, is horizontal and collaborative. It simply exists and allows anyone to enjoy and participate in the network. There's no one determining where the protocol goes and what the next update will be. It is the collective of users, nodes and miners who define which versions of the protocol will run so that they are in agreement with each other. That's why Bitcoin has no competitor, nothing works like it. Bitcoin embraces adversarial thinking and uses these individual incentives to strengthen the whole.

That's why Bitcoin is so resilient. You can't censor or prevent people from accessing it, even if they disagree with each other, unlike banks that close user accounts all the time and constantly change the rules.

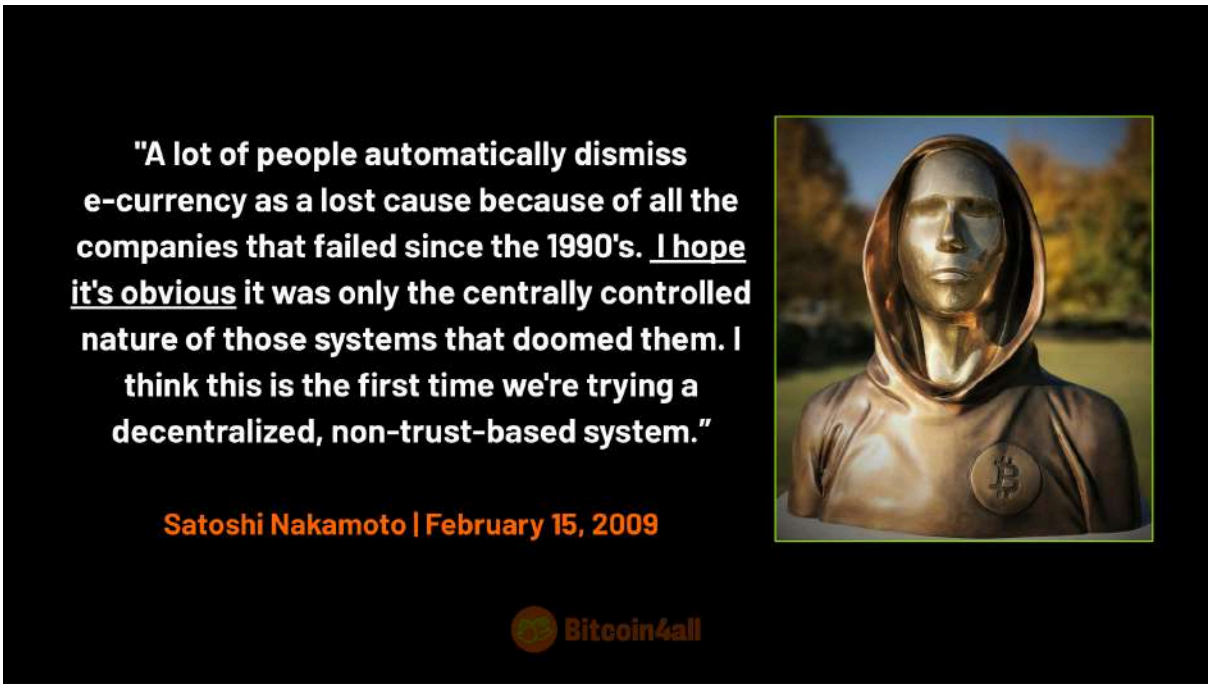
Many protocols even claim to be decentralized, but when you look deeply they are quite the opposite: they are just like companies. These protocols have leaders and a concentration of decision-making power, are easily censored and would not survive hacker attacks or government censorship. Bitcoin, on the other hand, has been under constant attack and has been running non-stop for more than 10 years due to its resilient and decentralized structure.



(slide 99) - Bitcoin 4 All

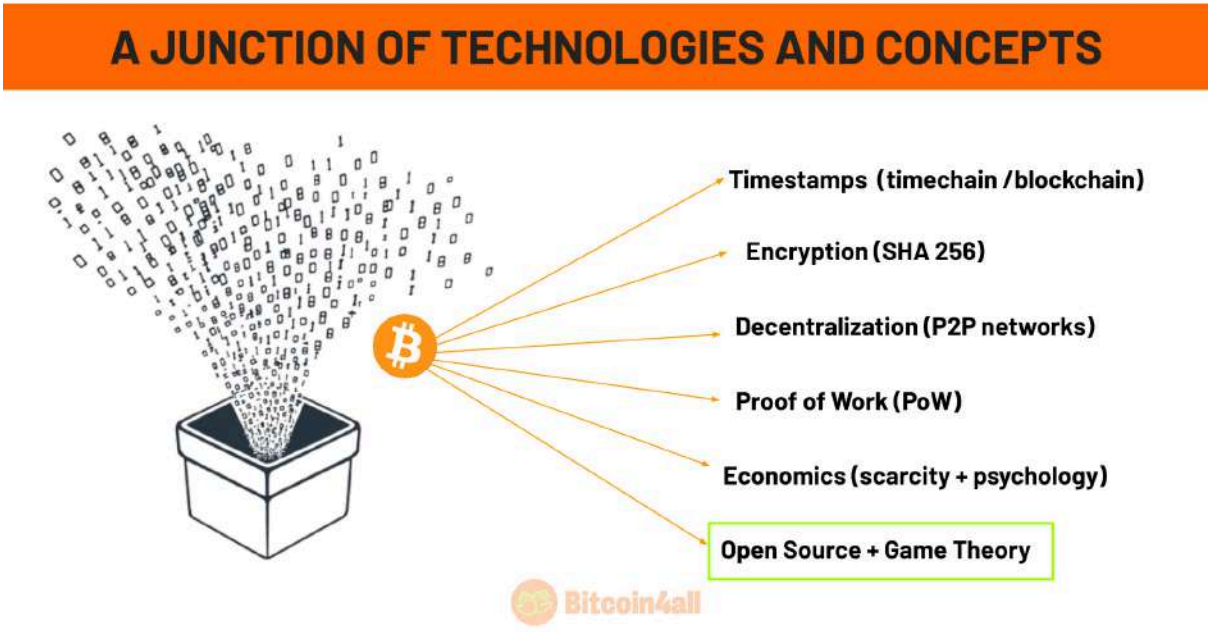
Even though there have been hundreds of copies, none of them have managed to overtake Bitcoin -- not even any other cryptocurrency that has emerged since. This image shows the forks, the copies that have already been made of Bitcoin from 2015 to 2018. Many called themselves "the real Bitcoin" and have tried to steal its narrative, visibility and liquidity, but none have really succeeded. No project can steal the properties and network effect that Bitcoin has. Any level of centralization is already a point of mutability, a monopoly of

decision-making power and also a potential point of failure that can be exploited by attackers.



(slide 100) - Bitcoin 4 All

Satoshi knew from the start that decentralization was the key to Bitcoin and one of the main reasons why previous digital money projects failed. He even wrote in 2009: "A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990's. I hope it's obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time we're trying a decentralized, non-trust-based system".



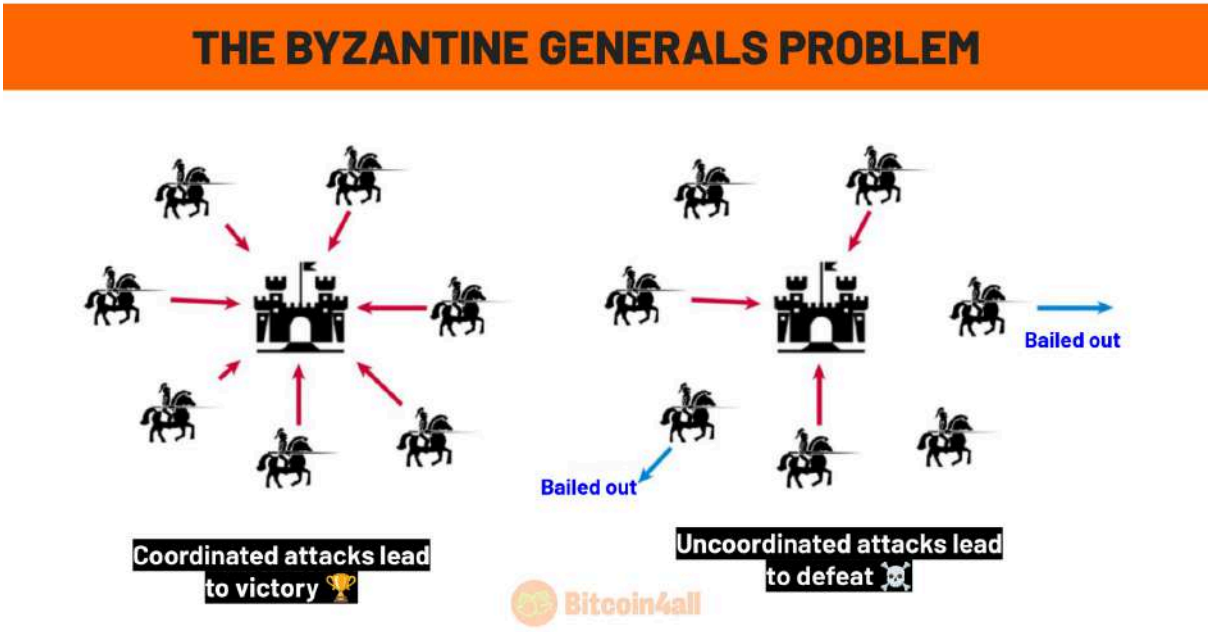
(slide 101) - Bitcoin 4 All

Bitcoin's decentralization is the result of a unique combination of factors that work together to protect the network. To compromise the system would require an attack that required extreme coordination, huge financial resources and a colossal amount of energy. This almost insurmountable barrier is supported by the practical application of game theory, which encourages participants to collaborate with each other to strengthen the network rather than trying to hack or trick each other.

In Bitcoin game theory, collaboration is always more profitable than sabotage. Miners, validators and other participants have financial and structural incentives to act in favor of the network, since any attempt to attack it would be extremely expensive and, in most cases, futile.

Furthermore, to make this collaboration possible and reliable, Bitcoin operates with total transparency. Its code is open source: it is public and accessible to everyone, allowing continuous auditing and ensuring that no rules are changed without the consensus of the network. This alignment between decentralization, economic incentives and transparency is what makes Bitcoin the most robust and secure monetary network ever created.

Satoshi managed to connect the dots by solving one of the oldest problems: the problem of the Byzantine generals.



(slide 110) - Bitcoin 4 All

This analogy tries to answer, by visualizing a war scenario, how computer systems could communicate in a decentralized fashion. Until Bitcoin came along, there was no answer to this problem.

Have you ever watched Game of Thrones? If you've watched it, imagine a scene of a city invasion just like the ones in the series. This city is called Byzantium and several generals want to attack it. They have surrounded the city and must decide together when to attack. If

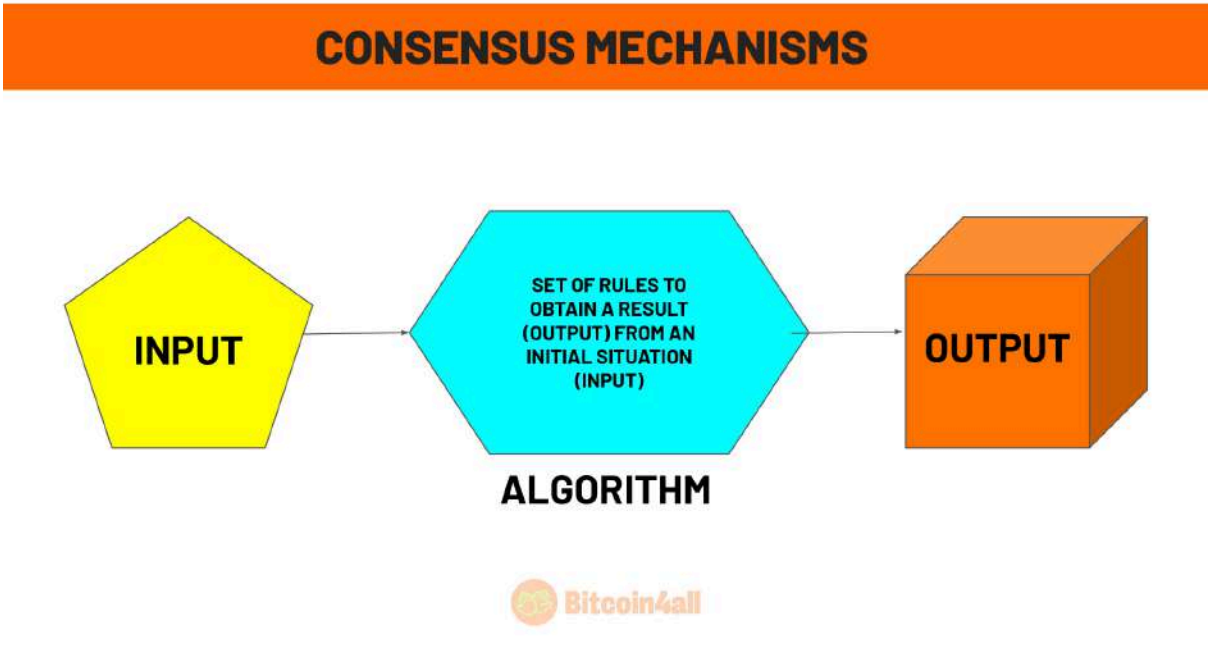
everyone attacks at the same time, they win the battle because there has been coordination. However, if they attack at different times, they lose because they are uncoordinated and susceptible to being attacked.

The generals don't have secure communication channels with each other to create this coordinated action. Firstly, because they are in different positions around the city, and secondly because they can't be sure that the message will arrive: the chances of a messenger being intercepted by the enemy are very high.

So they need to find a way to communicate, to agree on the right time to attack. The first general can start by sending an attack message at 9 AM, but he has no way of knowing whether the messenger has delivered the message or not. This uncertainty could lead the first general to give up attacking. Dilemmas like this led to many failures in the digital currencies that preceded Bitcoin.

Bitcoin has managed to solve the Byzantine generals' problem by having: complete coordination through Proof of Work, which establishes a set of network processing rules that coordinate everyone; through P2P networks that connect all participants to the same system; and through blockchain, a system of chained cryptographic records that everyone can verify without depending on any "messenger" from outside the system.

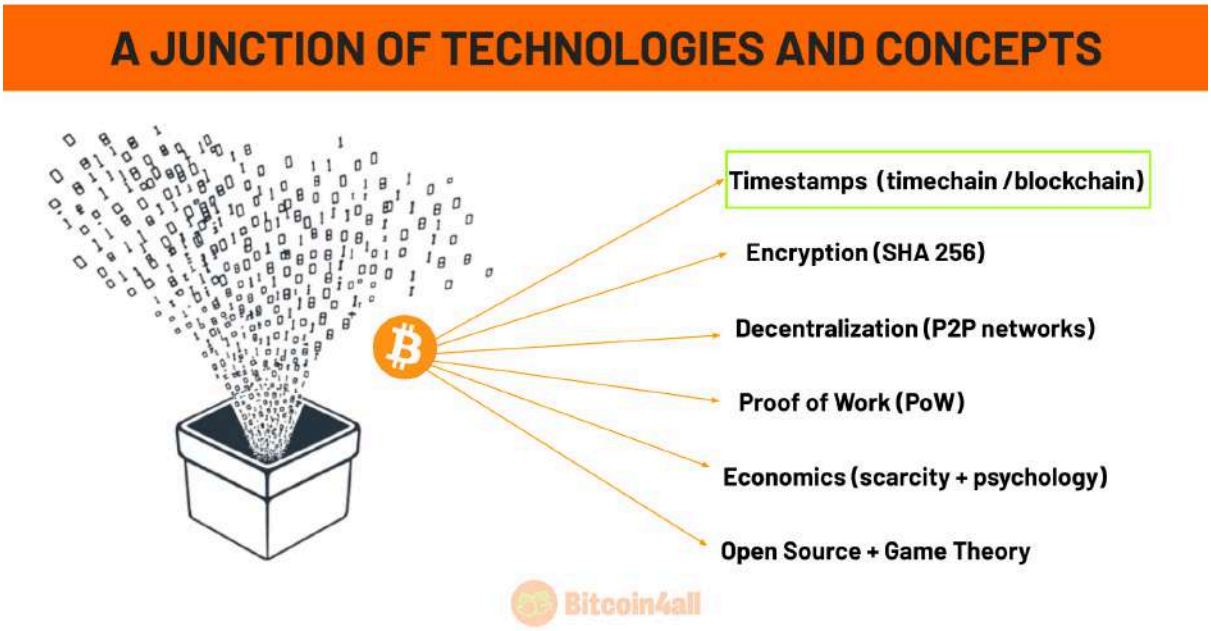
Through this system, all the generals would be able to coordinate on the right moment to attack Byzantium without depending on third parties, in a synchronized, safe manner -- and without anyone hesitating to attack.



(slide 102) - Bitcoin 4 All

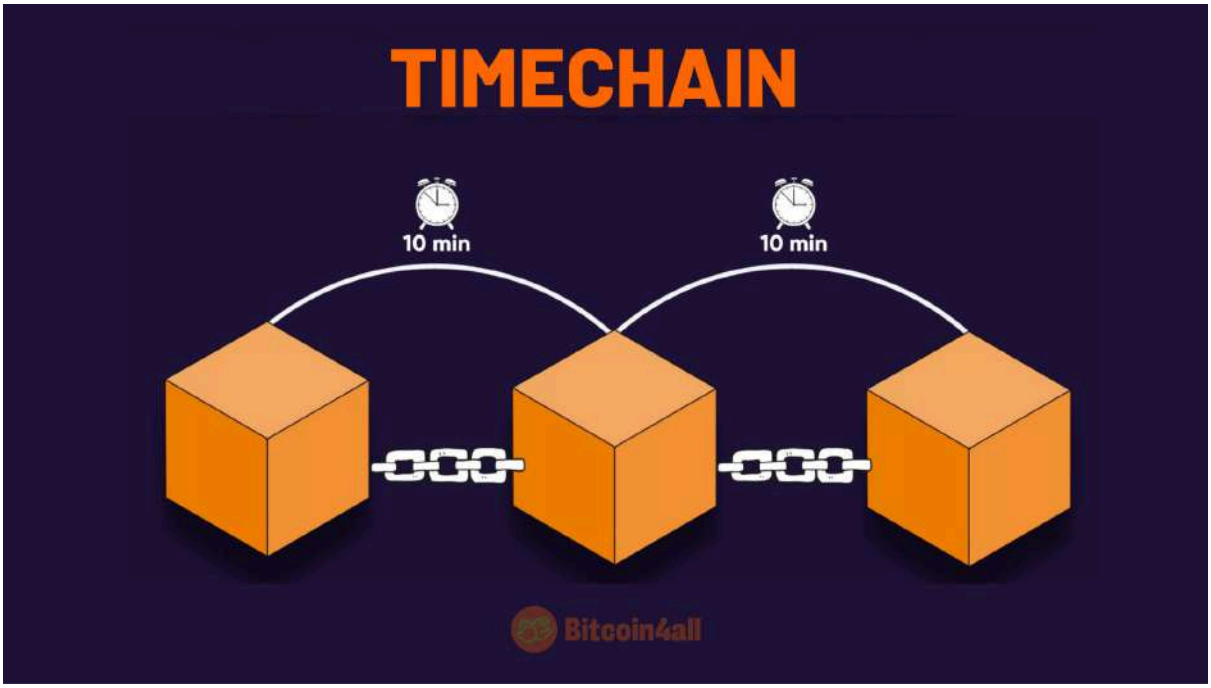
We just talked about proof of work and consensus mechanisms: these terms are the rules that guide the protocol. These are algorithms that establish how the network will coordinate

itself. This set of rules seeks, from an initial situation (an input), to achieve a final result (an output).



(slide 103) - Bitcoin 4 All

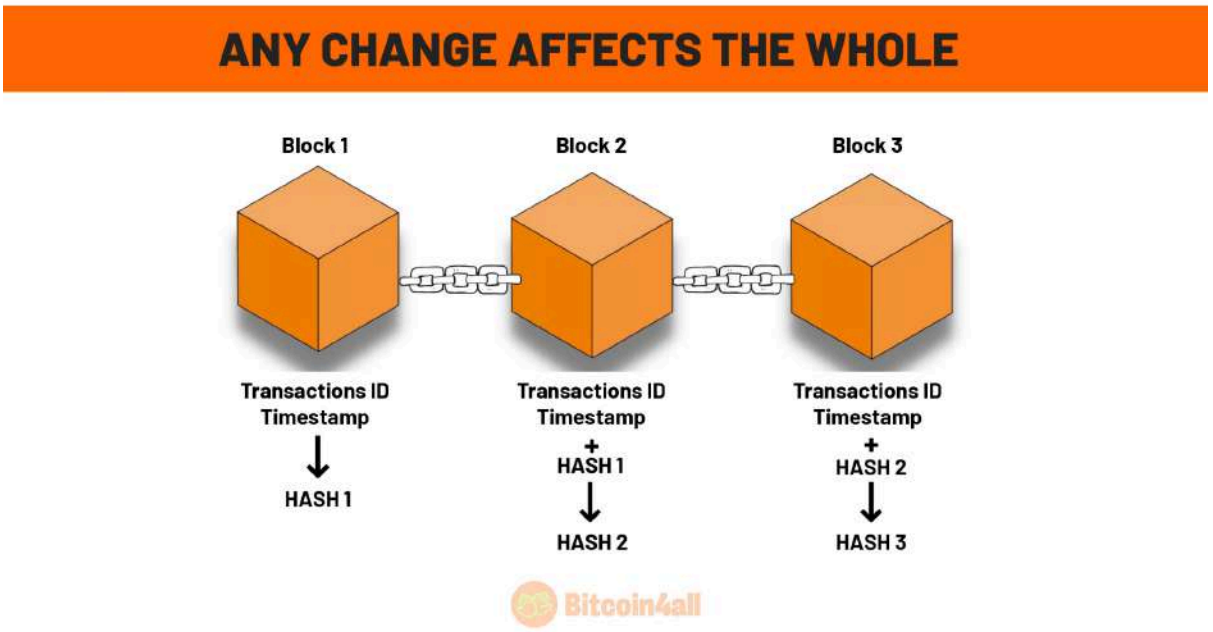
All of this works by recording information in a chained, distributed and undeletable system called a blockchain or timechain. Satoshi used timestamps and timechain to describe this mechanism in the Bitcoin whitepaper.



(slide 104) - Bitcoin 4 All

There are people who say that blockchain is the real innovation behind Bitcoin, but that's nonsense. Blockchain is important, but on its own and without other properties, it's just a slow, expensive database that is just as centralized as a company's Excel spread sheet!

Blockchain or timechain means chain of blocks. These are blocks of information linked together and processed by the network every 10 minutes on average. This means that it often takes less than 10 minutes -- other times, it can take hours. It depends on the computing power of the miners and the difficulty of the network.



(slide 105) - Bitcoin 4 All

The immutability of registers means that you can't remove or change the block in the middle of the chain. If you have 200 blocks and you try to delete or modify the middle one, the neighboring blocks will be affected, changing the hash.

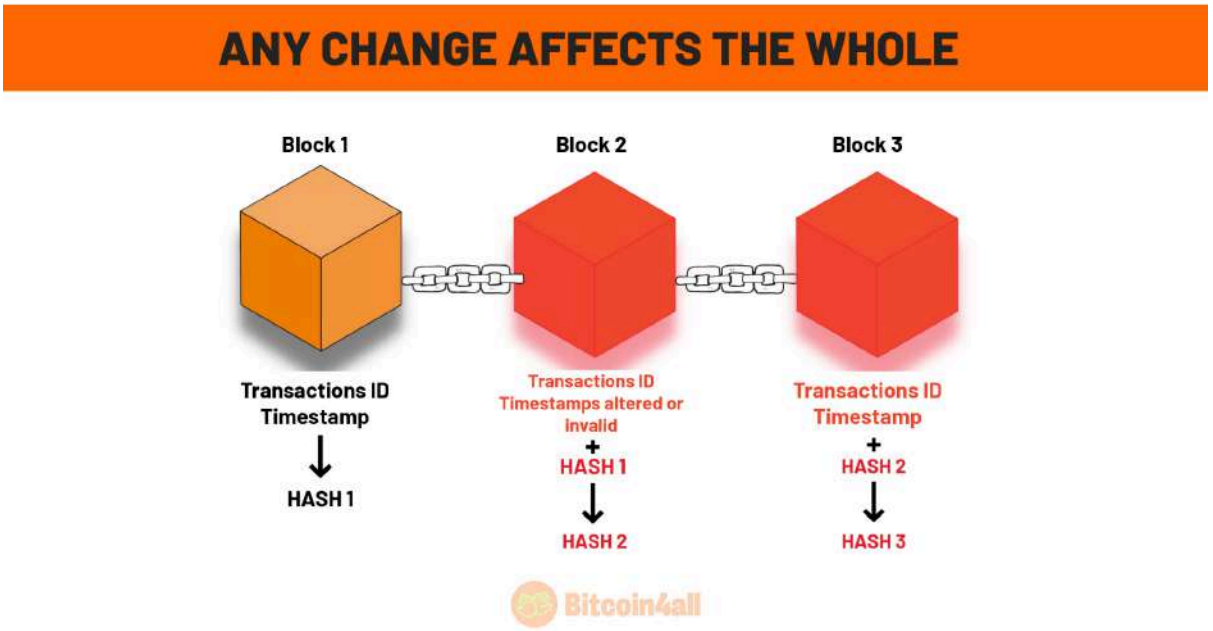
It's like a digital seam. If you pull the thread out of the middle of a seam, it distorts all the next stitches, doesn't it? Bitcoin is very similar. If any information is changed in one block, it ends up distorting all the following blocks.

So let's say we're looking at the Bitcoin blockchain right now. Each mined block contains information about the financial transactions made on the network and about the block itself where they were recorded. But the network summarizes all these formations in a code called "hash". The hash is the cryptographic phrase that summarizes all the information inside the block of information. It is from the hash that the chained database takes place.

Once the hash 1 of block 1 has been created, it will be inserted along with the contents of the next block, block 2. It will be "mixed randomly" to form the hash 2.

Hash 2 summarizes all the content of its block and also of the previous block, because Hash 1 was inserted inside the content of block 2 and so on.

Hash 3 will be the cryptographic summary of block 3, which contains the hash of the previous block, 2. These hash functions are used to chain the network. In other words, the following blocks will always have a summary of the previous ones. This is how information is always correlated.



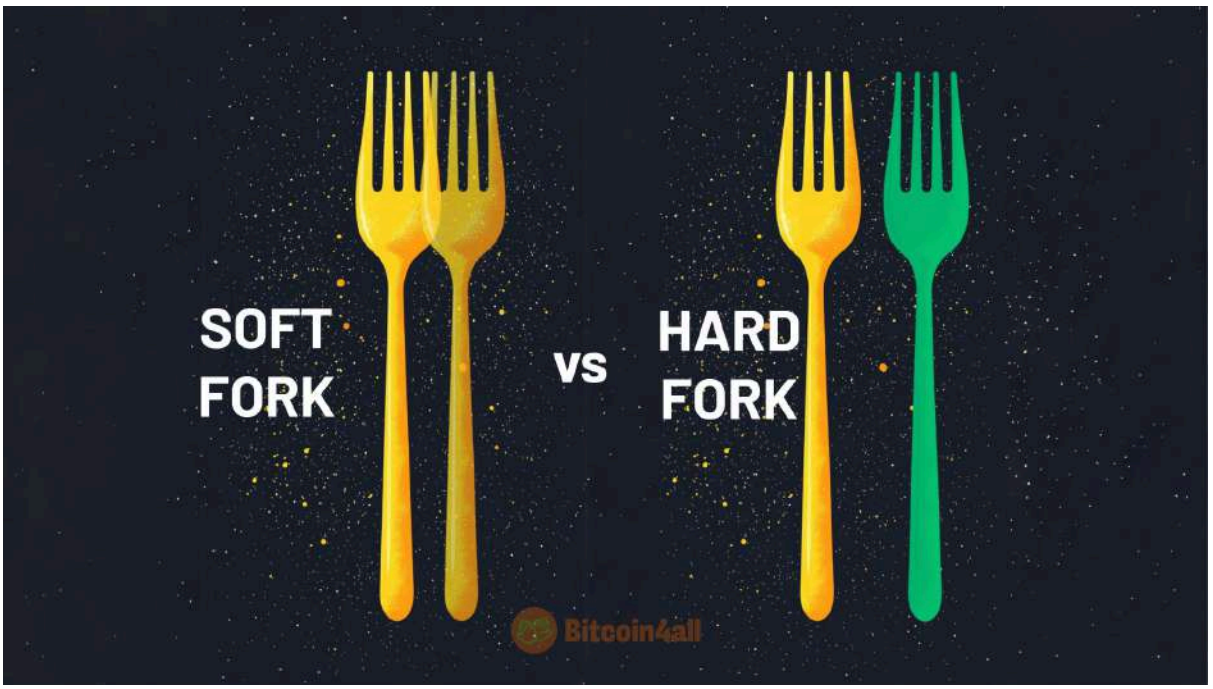
(slide 106) - Bitcoin 4 All

It's because of this chain of information that the network keeps confirming everything before mining the next block. So, if you change anything in block 1, the hash of all the following blocks will also change. If you change a comma, a space, a letter, anything, it changes the hash. If something is changed after it has been registered on the blockchain, the miners or nodes that verify the network will identify the change through the hash and will not accept that information as valid.

This mechanism makes it absurdly easy to check if there has been an attack on the transaction history, while making it very difficult to edit past records effectively. This is because both nodes and miners have copies of the Bitcoin blockchain, so if any information from the past is changed and doesn't match the copies that exist on their computers, they will be easily identified and won't accept that block as valid.

This is one of the constant verification factors that makes the Bitcoin network very secure and difficult to hack. It's a network that manages to decentralize trust, because everything fits togheter: nothing has changed. All the information matches. This ease of verification and difficulty of manipulation is what makes the records on the Bitcoin blockchain immutable.

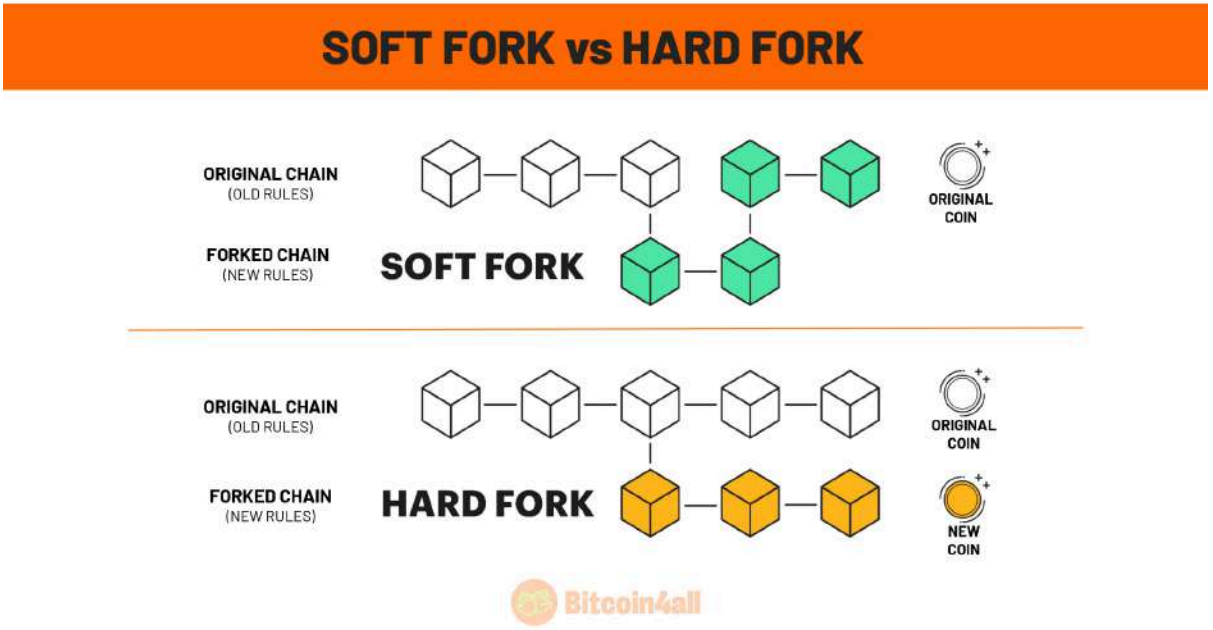
Even so, if someone decides to change the way the network works, they could cause a fork.



(slide 107) - Bitcoin 4 All

Blockchain version updates are called forks. There are two types of updates: soft forks and hard forks.

Forks comes from ramification, so you'll see images of, well, forks whenever someone talks about soft and hard forks. Forks are different versions of the initial rules.



(slide 109) - Bitcoin 4 All

So what's the difference between these two types of forks?

Soft forks are when the network performs an update in such a way that both those running the old version of the code or software and those running the new version can coordinate. It is a backward compatible and optional update; it does not change the consensus mechanism. It's still the same network and the same currency, just with a few different details in the versions.

Hard forks, on the other hand, are when radical updates are made, to the point of changing protocol consensus. Those running the old version are unable to coordinate with those running the new version. Old users can't join the new network if they don't update. As a result, a new currency and a new network are created. This type of update forces users to upgrade to the new version.

Bitcoin doesn't do hard forks, only soft forks. Because hard forks are centralizing forces, they exclude users who may not agree with the new version and end network immutability. Hard forks are more frequently observed in other cryptocurrency protocols and in private company blockchains.

Well, in this lesson we've started to delve into how Bitcoin works, but that's only a piece of the puzzle. There's a lot more content for you to learn. Soak up this knowledge, give your brain a break and when you're ready to continue I'll be there for you at the next class.