Michele D'Aliessi Follow
Explaining Blockchain technology in simple words.
Jun 1, 2016 · 16 min read

How Does the Blockchain Work?

Blockchain technology explained in simple words

The blockchain technology is probably the best invention since the internet itself. It allows value exchange without the need for trust or for a central authority. Imagine you and I bet $50 on tomorrow's weather in San Francisco. I bet it will be sunny, you that it will rain. Today we have three options to manage this transaction:

1. We can *trust* each other. Rainy or sunny, the losing one will give $50 to the winner. If we are friends, this could be a good way of managing it. However, friends or strangers, one can easily not pay the other.

2. We can turn the bet into a *contract*. With a contract in place both parties will be more prone to pay, however, should any of the two decide not to pay, the winner will have to pay additional money to cover legal expenses and the verdict might take a long time. Especially for a small amount of cash, this doesn't seem the optimal way of managing the transaction.

3. We can involve a neutral third party. Each of us gives $50 to a third party, she then will give the total amount to the winner. But hey, she could also run away with all our money. So we end up in one of the first two options: *trust* or *contract*.

Both trust and contract aren't optimal solutions: we can't trust strangers and enforcing a contract requires time and money. The blockchain technology is interesting because it offers us a third option which is secure, quick and cheap.

Blockchain allows us to write a few lines of code, a program running on the blockchain, to which both of us send $50. This program will keep the $100 safe and check tomorrow's weather automatically on several data sources. Sunny or rainy it will transfer automatically the whole amount to the winner. Each party can check the contract logic, and once it's running on the blockchain it can't be changed or stopped. This effort can be quite too high for a $50 bet, but imagine when selling a house or a company.

The goal of this article is to explain how the blockchain works without discussing the technical details in depth, but digging just enough to give you a general idea of the underlying logic and mechanisms.

The most known and discussed application of the blockchain technology is called *Bitcoin*. A digital currency that can be used to exchange products and services, just like United States Dollar (USD), Euro (EUR), Chinese Yuan (CNY), and other national currencies. Let's use this first application of the blockchain technology to learn how it works.

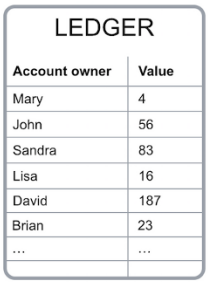
> *"Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate."*
> *- Marc Andreessen*

. . .

So, what is a Bitcoin?

One Bitcoin is a single unit of the Bitcoin (BTC) digital currency, just like a Dollar it has no value by itself, it has value only because we agree to trade goods and services in exchange for a higher amount of the currency under our control and we believe others will do the same.

To keep track of the amount of Bitcoins each of us owns the blockchain uses a *ledger*, a digital file that keeps track of all Bitcoin transactions.



LEDGER

Account owner	Value
Mary	4
John	56
Sandra	83
Lisa	16
David	187
Brian	23
…	…

Fig. 1 - Bitcoin ledger digital file simplified

The *ledger* file is not stored in a central entity servers, like a bank, or in a single data center. It is distributed across the world via a network of private computers that are both storing data and executing computations. Each of these computers represents a "*node*" of the *blockchain* network and has a copy of the *ledger* file.

If David wants to send Bitcoins to Sandra, he broadcasts a message to the network that says the amount of Bitcoins in his account should go down by 5 BTC, and the amount of Sandra's account should go up by the same quantity. Each *node* in the network will receive the message and apply the requested transaction to their copy of the ledger, thus updating the account balances.

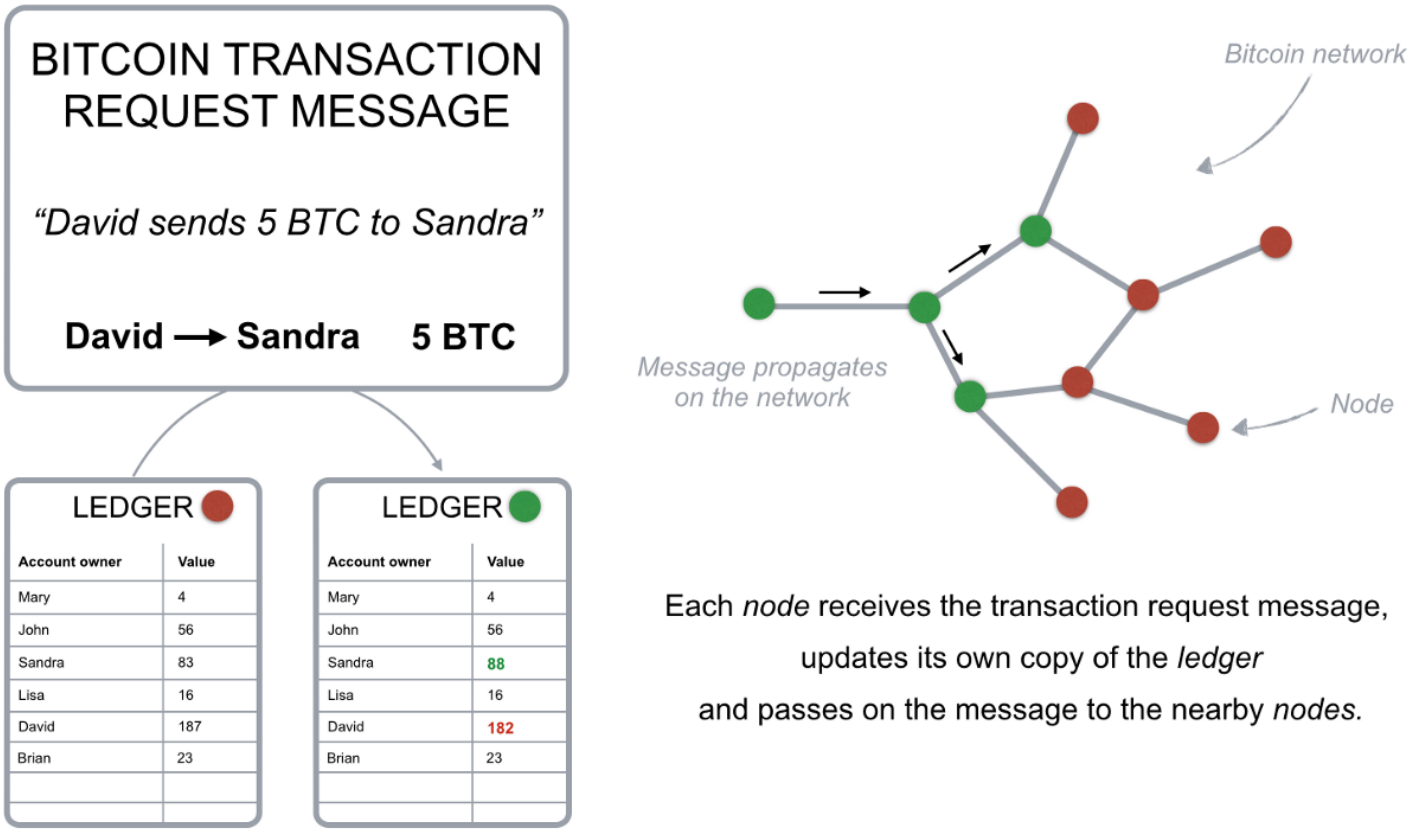


Fig 2 - Transaction request message simplified

The fact that the ledger is maintained by a group of connected computers rather than by a centralized entity like a bank has several implications:

- While in our bank system we only know our own transactions and account balances, on the blockchain everyone can see everyone's else transactions.
- While you can generally trust your bank, the Bitcoin network is distributed and if something goes wrong there is no help desk to call or anyone to sue.
- The blockchain system is designed in such a way that no trust is needed, security and reliability are obtained via special mathematical functions and code.

> *"We can define the blockchain as a system that allows a group of connected computers to maintain a single updated and secure ledger."*

In order to be able to perform transactions on the blockchain, you need a *wallet*, a program that allows you to store and exchange your Bitcoins. Since only you should be able to spend your Bitcoins, each *wallet* is protected by a special cryptographic method that uses a unique pair of different but connected keys: a private and a public key.

If a message is encrypted with a specific public key, only the owner of the paired private key will be able to decrypt and read the message. On the other way, if you encrypt a message with your private key, only the paired public key can be used to decrypt it. When David wants to send Bitcoins, he needs to broadcast a message encrypted with the private key of his *wallet*, so he and only he can spend the Bitcoins he owns as David is the only one to know his own private key necessary to unlock his *wallet*. Each node in the network can cross check that the transaction request is coming from David by decrypting the transaction request message with the public key of his wallet.

When encrypting a transaction request with your wallet's private key you are generating a digital signature that is used by blockchain computers to double check the source and the authenticity of the transaction. The digital signature is a string of text that is the result of a combination of your transaction request and your private key, therefore it cannot be used for other transactions. If you change a single character in the transaction request message the digital signature will change, so no potential attacker can change your transaction requests or alter the amount of Bitcoins you are sending.

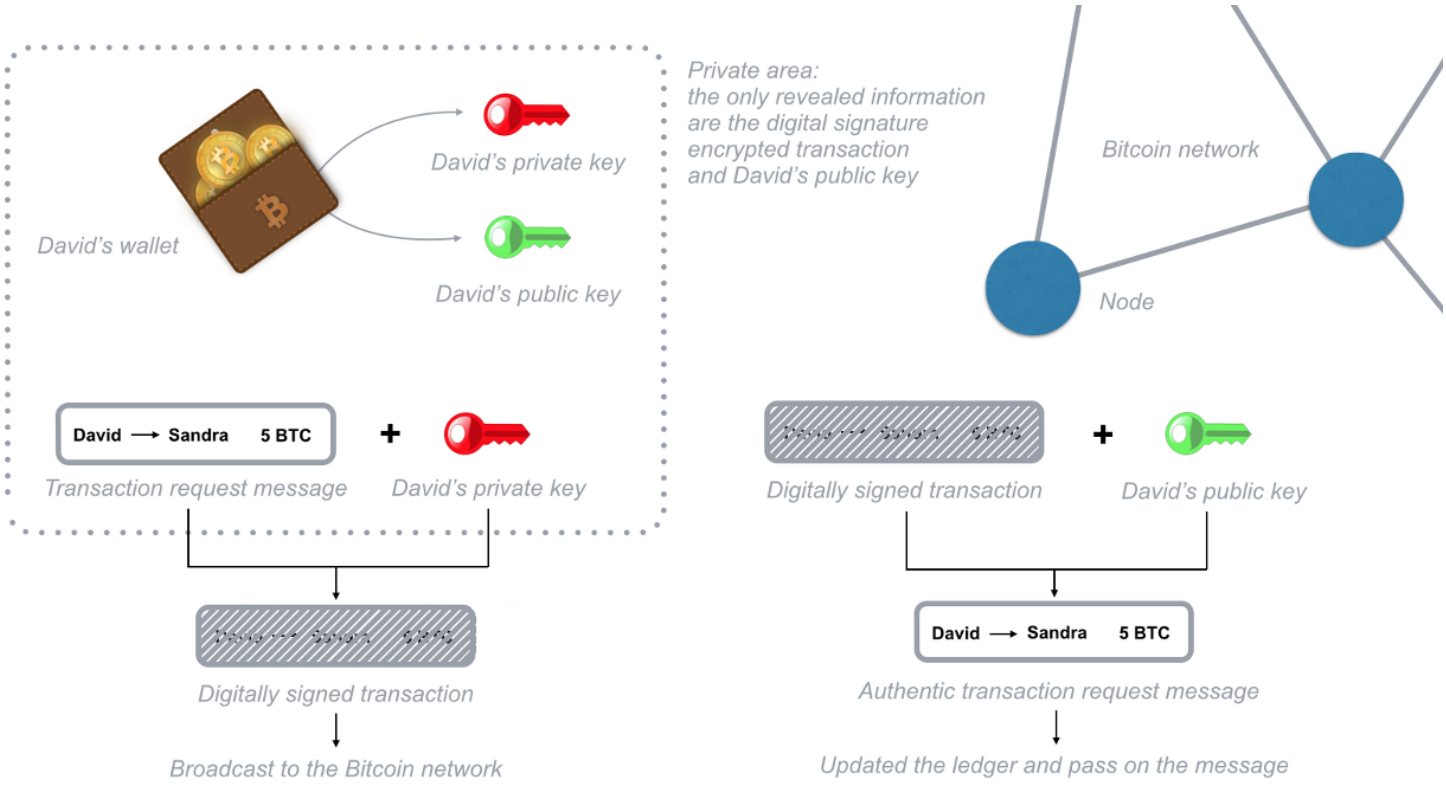


Fig. 3 - Digital Signature transaction encryption simplified

To send bitcoin you need to prove that you own the private key of a specific wallet as you need to use it to encrypt the transaction request message. Please note that since you broadcast the message only after it has been encrypted, you never have to reveal your private key.

Each node in the blockchain is keeping a copy of the ledger. So, how does a node know what's your account balance? The blockchain system doesn't keep track of account balances at all (as suggested in Fig. 1), it only records each and every transaction that is requested. The ledger in fact does not keep track of balances, it only keeps track of every transaction that is broadcasted within the Bitcoin network (Fig. 4). To know your wallet balance, you need to analyze and verify all the transactions that ever took place on the whole network connected to your wallet.

LEDGER

Transactions	Value
Mary → John	10.000
John → Lisa	0.345
Sandra → David	18.4332
Lisa → Sandra	7.156
David → Mary	12.3402
Brian → Lisa	3.029381
...	...

Fig. 4 - Blockchain Ledger

This "balance" verification is performed thanks to links to previous transactions. In order to send 10 Bitcoins to John, Mary has to generate a transaction request that includes links to previous incoming transactions whose total balance equals or exceeds 10 Bitcoins. These links are called inputs, nodes in the network will verify that the total amount of these transactions equal or exceeds 10 Bitcoins and that these inputs were not yet spent. In fact, each time you reference inputs in a transaction those are considered not valid in any future transaction. This all is performed automatically in Mary's wallet and double checked by the Bitcoin network nodes, she only sends a 10 BTC transaction to John's wallet using his public key.

Mary → John 10 BTC

Simplified transaction request

Inputs

Previous output	Amount	From address	Signature
n278cojci…1	3.451	Sandra's address	fuw93v2…c3
m8nd53hd…1	6.334	Brian's address	a56fbsuc…s8
cn3792m…1	0.14	Lisa's address	lfue82mc…id
u4her83n…1	2.193	David's address	jwc7fks8…2a

Outputs

Redeemed input	Amount	To address	Signature
j3s8b30f…if	2.118	Mary's address	k732cne…21
ks2f9ms7…j3	10	John's address	87fckwlo…k4

Real transaction request structure

Fig. 5 - Blockchain transaction request structure

So, how can the system trust input transactions and consider them valid? It checks all the previous transactions that are correlated to the *wallet* you use to send Bitcoins via the references that each one has as inputs. To simplify and speed up the verification process a special record of unspent transactions is kept by the network *nodes*. Thanks to this security check, it is not possible to double-spend received Bitcoins.

> *"Owning Bitcoins means that there are transactions written in the ledger that point to your wallet address and haven't been used as inputs yet."*

All the code to perform transactions on the Bitcoin network is open source, this means that anyone with a laptop and an internet connection can operate transactions. However, should there be a mistake in the code that is used to broadcast a transaction request message, the associated Bitcoins will be permanently lost. Remember that since the network is distributed, there is no customers support to call nor anyone that could help you restore a lost transaction or your forgotten wallet password. For this reason, if you are interested in transacting on the Bitcoin network it's recommended to use the open source and official version of Bitcoin wallet software (such as Bitcoin Core) and to store your wallet's password or private key in a very safe repository.

. . .

Hum, ok, but is it really safe? And why is it called block-chain?

Anyone can access the Bitcoin network via an anonymous connection (i.e. a TOR network or a VPN network), and submit or receive transactions revealing nothing more than his public key. However if someone uses the same public key over and over, it's possible to connect all the transactions to the same owner. The Bitcoin network allows you to generate as many wallets as you like, each one with its own private and public keys. This allows you to receive payments on different wallets that cannot be linked together. There is no way to know that you own all these wallets private keys unless you send all the received Bitcoins to a single wallet.

> *The total number of possible Bitcoin addresses is 2^{160} or 1461501637330902918203684832716283019655932542976. This large number protects the network from possible attacks while allowing anyone to own a wallet.*

With this setup, there is still a major security hole that could be exploited to recall Bitcoin after spending them. Transactions are passed from node to node within the network, so the order in which 2 transactions reach each node can be different. An attacker could send a transaction, wait for the counterpart to ship a product and then send a reverse transaction back to his own account. In this case, some nodes could receive the second transaction before the first one and therefore consider they first payment transaction invalid as the transaction inputs result already spent. How do you know which transaction has been requested first? It's not secure to order the transactions by timestamp because it could easily be counterfeit. Therefore, there is no way to tell if a transaction happened before another, and this opens up the potential for fraud.

If this happens, there will be disagreements between the network *nodes* regarding the order of transactions each of them received. So the *blockchain* system has been designed to use *nodes* agreement to order transactions and prevent the fraud described above.

The Bitcoin network orders transaction by putting them together into groups called b*locks*, each *block* contains a definite amount of transactions and a link to the previous *block*. This is what puts one *block* after the other in time. *Blocks* are therefore organized into a time-related chain (Fig. 6), that gives the name to the whole system: *blockchain*.

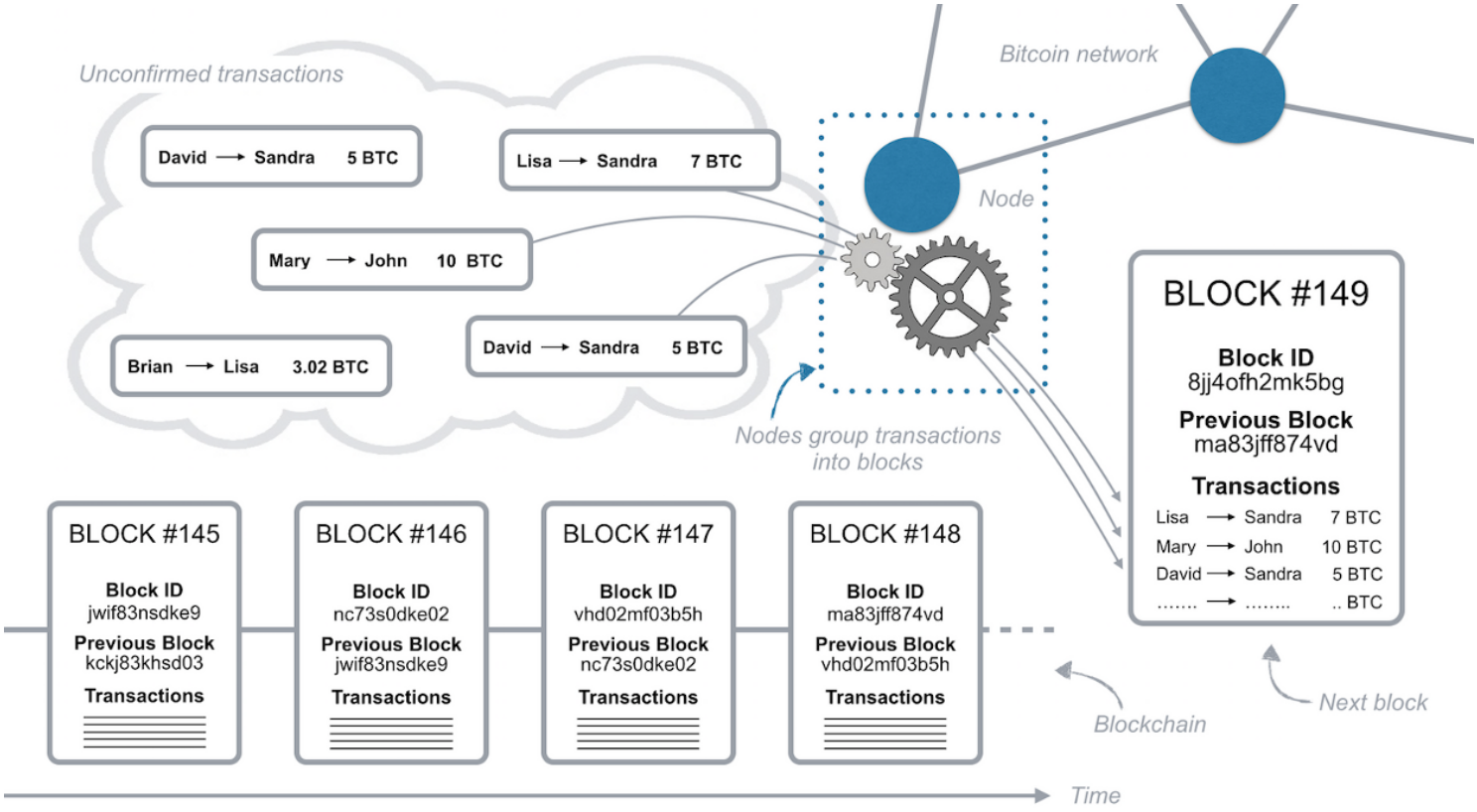


Fig. 6—The block chain sequence structure simplified

Transactions in the same *block* are considered to have happened at the same time and transactions not yet in a *block* are considered unconfirmed. Each node can group transactions together into a *block* and broadcast it to the network as a suggestion for what block should be the next. Since any node can suggest a *new block*, how does the system agree on what *block* should be the next?

In order to be added to the blockchain, each block must contain the answer to a complex mathematical problem created using an irreversible cryptographic hash function. The only way to solve such mathematical problem is to guess random numbers that combined with the previous block content generate a defined result (usually a number below a certain value). It could take about a year for a typical computer to guess the right number and solve the mathematical problem. However due to the high number of computers in the network that are guessing numbers a block is solved on average every 10 minutes. The node that solves such mathematical problem acquires the right to place the next block on the chain and broadcast it to the whole network.

And what if two nodes solve the problem at the same time and spread their blocks to the network simultaneously? In this case, both blocks are broadcasted and each node builds on the block that it received first, however the blockchain system requires each node to build immediately on the longest block chain available. So if there is ambiguity about which is the last block, as soon as the following block gets solved each node will adopt the longest chain as the only option.

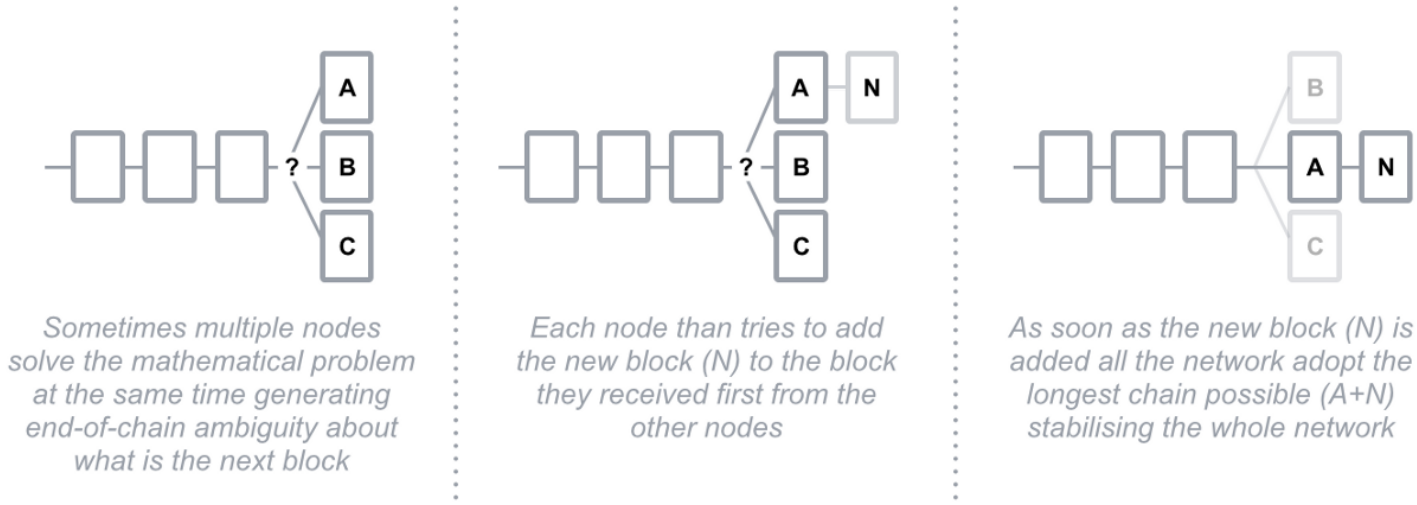


Fig.7 - End of chain ambiguity logic

Due to the low probability of solving blocks simultaneously, it's almost impossible that multiple *blocks* are solved at the same time over and over again building different "tails", so the whole *blockchain* stabilizes quickly to one single string of *blocks* that every node agrees on.

The disagreement about which *block* represent the end of the chain "tail", opens up the potential for fraud again. If a transaction happens to be in a *block* that belongs to a shorter tail (like *block B in Fig. 7*), once the next *block* is solved such transaction will go back to the unconfirmed transactions as all the others included in *block B*.

Let's see how Mary could leverage the end-of-chain ambiguity to perform a double-spending attack. Mary sends money to John, John then ships the product to Mary, now since nodes always adopt the longer tail as the confirmed transactions, if Mary could generate a

longer tail that contains a reverse transaction with the same input references, John would be out of both his money and his product.

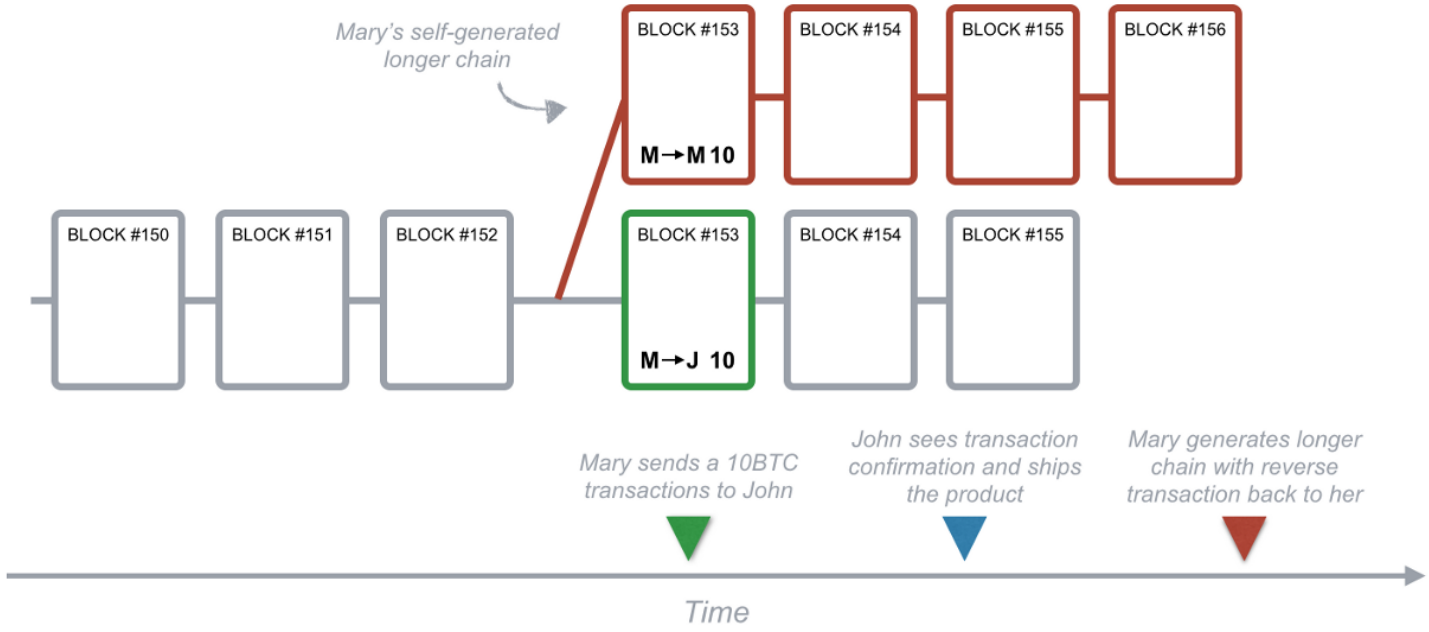


Fig. 8 - Mary's double-spending attack

So how does the system prevent this kind of fraud? Each *block* contains a reference to the previous *block (see Fig. 6)*, and that reference is part of the mathematical problem that needs to be solved in order to spread the following *block* to the network. So it's extremely hard to pre-compute a series of blocks due to the high number of random guesses needed to solve a *block* and place it on the blockchain. Mary is in a race against the rest of the network to solve the math problem that allows her to place the next block on the chain. And even if she solves it before anyone else, it's very unlikely she could solve 2, 3 or more blocks in a row, since every time she is competing against the whole network. So, could Mary use a super fast computer to generate enough random guesses to compete with the whole network in solving blocks? Yes, but even with a very very fast computer, due to the large amount of members in the network, it's very unlikely Mary could solve several blocks in a row at the exact time needed to perform a double-spending attack.

She would need control of 50% of the computing power of the whole network to have a 50% chance to solve a block before some other node does, and even in this case, she has a 25% chance to solve two blocks in a row. The more blocks to be solved in a row, the lower the probability that Mary can succeed.

> *"Transactions in the Bitcoin blockchain system are protected by a mathematical race: any attacker is competing against the whole network."*

Therefore, transactions get more and more secure with time. Those included in *blocks* that have been confirmed in the past are more secure than those included in the last *block*. Since a *block* is added to the chain every 10 minutes on average, waiting for about 1 hour from when the transaction is included in a *block* for the first time gives a quite high probability that the transaction has been processed and is non reversible.

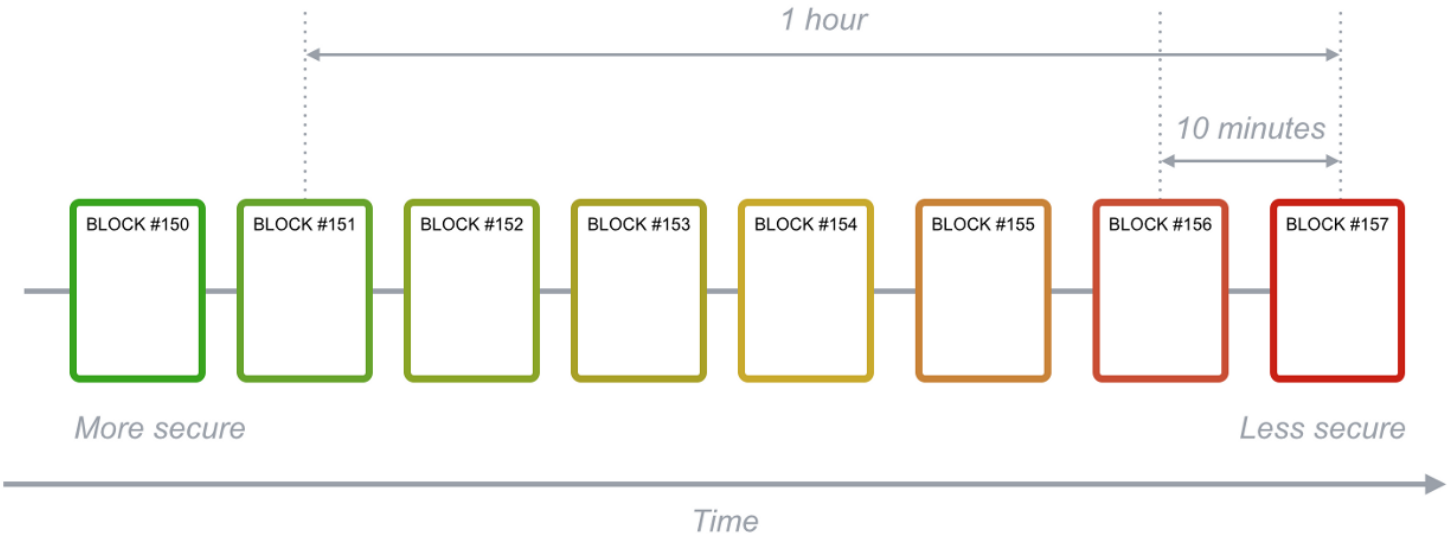


Fig. 9 - Blockchain transactions security

. . .

In order to be able to send Bitcoins you need to reference a transaction that sends Bitcoin to your wallet, and this applies to all the transactions

that ever took place in the network. So, where does Bitcoins come from originally?

As a way to balance the deflationary nature of Bitcoin due to software errors and wallets password loss, a reward is given to those that solve the mathematical problem of each block. The activity of running the Bitcoin *blockchain* software in order to obtain these Bitcoin rewards is called "mining" - very much like mining gold.

This reward is the main incentive that pushes private people to operate the *nodes*, thus providing the necessary computing power needed to process Bitcoin transactions and to stabilize the blockchain network.

Since it takes a long time for a typical computer to solve a block (about 1 year on average), nodes get together in groups that divide the number of guesses each one has to try in order to solve the next block. In this way it's faster for the group to guess the right number and get the reward that is than shared among the group members. Such groups are called *mining pools*.

Some of these *mining pools* are pretty large and represent more than 20% of the total network computing power. This has clear implications for the network security as seen above in the Mary double spend attack example. Even if one of these pools could potentially gain 50% of the network computing power, the further back along the chain a block gets, the more secure are the transactions included in it.

However, some of these mining pools that gained substantial computing power share decided to limit the number of their members in order to safeguard the overall network security.

Since the overall network computing power is likely to increase over time due to technological innovation and the increasing number of nodes, the blockchain system recalibrates the mathematical problem difficulty to solve the next block in order to target 10 minutes on average for the whole network. This ensures the network stability and overall security.

Moreover, every 4 years the block reward is cut in half, so mining bitcoin (=running the network) gets less interesting over time. To prevent nodes from stopping running the network small reward fees can be attached to each transaction, these rewards are collected by the

node that successfully include such transactions in a block and solves its mathematical problem. Due to this mechanism, transactions associated with a higher reward are usually processed faster than those associated with a low reward. This means that when sending a transaction you can decide if you would like to process it faster (=more expensive) or cheaper (=takes more time). Transactions fees in the bitcoin network are currently very small if compared with what banks charges and are not associated with the transactions amount.

. . .

Now that you have a general understanding of how the blockchain works, let's have a quick look at why it's so interesting.

Using the blockchain technology has quite remarkable **benefits**:

- You have complete control of the value you own, there is no third party that holds your value or that can limit your access to it.
- The cost to perform a value transaction from and to anywhere in the planet is very low (in the order of a dollar cent fraction). This allows micropayments.
- Value can be transferred in few minutes and the transaction can be considered secure in a few hours, not days or weeks.
- Since anyone at any time can verify every transaction made on the blockchain, full transparency is granted.
- It's possible to leverage the blockchain technology to build decentralized applications that would be able to manage information and value transfer fast and securely.

However, there are a few **challenges** that need to be addressed:

- Transactions can be sent and received anonymously. On one side this preserves the users privacy but on the other allows non legal activity on the network as institutions cannot track users identity.
- Even if many exchange platforms are emerging, it's still not that easy to trade bitcoins for goods and services. However, they are becoming more and more popular.

- Bitcoin, like many other cryptocurrencies, is very volatile: there aren't that many Bitcoins available in the market and the demand is changing rapidly. Bitcoin price is very effected by large events or announcements in the cryptocurrencies industry.
- The technology is still in its infancy. New tools are developed every day to improve the blockchain security stability while offering a broader range of features, tools and services.

Overall, the blockchain technology has the potential to revolutionize several industries from advertising to energy distribution. Its main power lies in its abilities of not requiring trust and being decentralized. Many use cases of this brilliant technology are arising (i.e. the possibility to create a fully decentralized platform that runs smart contracts like Ethereum), if you want to learn more please follow the links below.

. . .

> *"Internet is to information, what Blockchain is to value"*

. . .

Useful links

- Get your own Bitcoin wallet - link
- Buy your first Bitcoins - you can get 10$ for free with my invitation
- Start mining Bitcoin - link (beginner) - link (pro)
- Learn more about decentralized applications - link
- Make sure your Bitcoins are kept safe, away from hackers, with a Ledger Wallet - link

. . .

The ultimate guide to understand Ethereum in simple words.

medium.com