# How Does the Blockchain Work?

Blockchain technology is probably the best invention since the internet itself. It allows value exchange without the need for trust or 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 loser 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 either of the two decide not to pay, the winner will have to pay additional money to cover legal expenses and the court case might take a long time. Especially for a small amount of cash, this doesn't seem like the optimal way to manage the transaction.

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

Neither trust nor contract is an optimal solution: 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 automatically transfer 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 may be too much effort for a $50 bet, but imagine selling a house or a company.

This article explains how the blockchain works without discussing the technical details in depth, but by digging just enough to give you a general idea of the underlying logic and mechanisms.

*Also available in Simplified Chinese and Mandarin thanks to volunteering efforts and blockchain community support.*

## The Basics of Bitcoin

THE FUTURE OF
GLOBAL
TRANSACTIONS
Blockchain network
Node

Images courtesy of author.

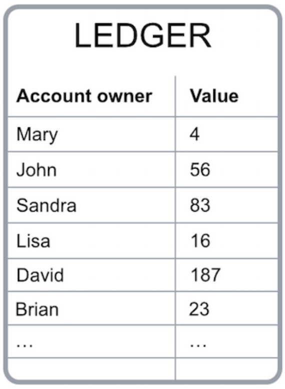
The most known and discussed application of the blockchain technology is bitcoin, a digital currency that can be used to exchange products and services, just like the U.S. dollar, euro, Chinese yuan, and other national currencies. Let's use this first application of the blockchain technology to learn 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*

One bitcoin is a single unit of the Bitcoin (BTC) digital currency. Just like a dollar, a bitcoin has no value by itself; it has value only because we agree to trade goods and services to bring more of the currency under our control, and we believe others will do the same.

To keep track of the amount of bitcoin each of us owns, the blockchain uses a ledger, a digital file that tracks all bitcoin transactions.



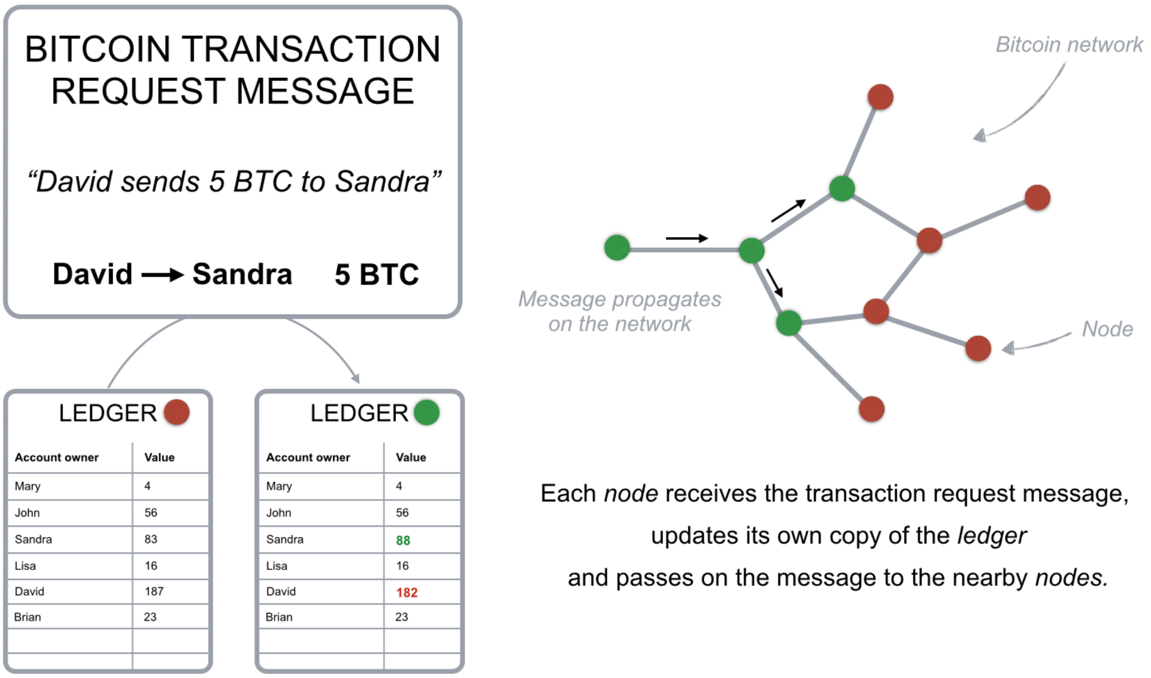
LEDGER

| 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 server, 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 bitcoin in his account should go down by 5 BTC, and the amount in Sandra's account should increase by the same quantity. Each node in the network will receive the message and apply the requested transaction to its copy of the ledger, updating the account balances.



BITCOIN TRANSACTION REQUEST MESSAGE

*"David sends 5 BTC to Sandra"*

**David → Sandra 5 BTC**

LEDGER 🔴

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

LEDGER 🟢

| Account owner | Value |
|---|---|
| Mary | 4 |
| John | 56 |
| Sandra | **88** |
| Lisa | 16 |
| David | **182** |
| Brian | 23 |

Each *node* receives the transaction request message,
updates its own copy of the *ledger*
and passes on the message to the nearby *nodes.*

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:

- In our bank system we only know our own transactions and account balances; on the blockchain everyone can see everyone else's 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 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 distinct 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 can decrypt and read the message. The reverse is also true: If you encrypt a message with your private key, only the paired public key can decrypt it. When David wants to send bitcoins, he needs to broadcast a message encrypted with the private key of his wallet. As David is the only one who knows the private key necessary to unlock his wallet, he is the only one who can spend his bitcoins. Each node in the network can cross-check that the transaction request is coming from David by decrypting the message with the public key of his wallet.

When you encrypt a transaction request with your wallet's private key, you are generating a digital signature that is used by blockchain computers to verify the source and authenticity of the transaction. The digital signature is a string of text resulting from 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 bitcoin you are sending.

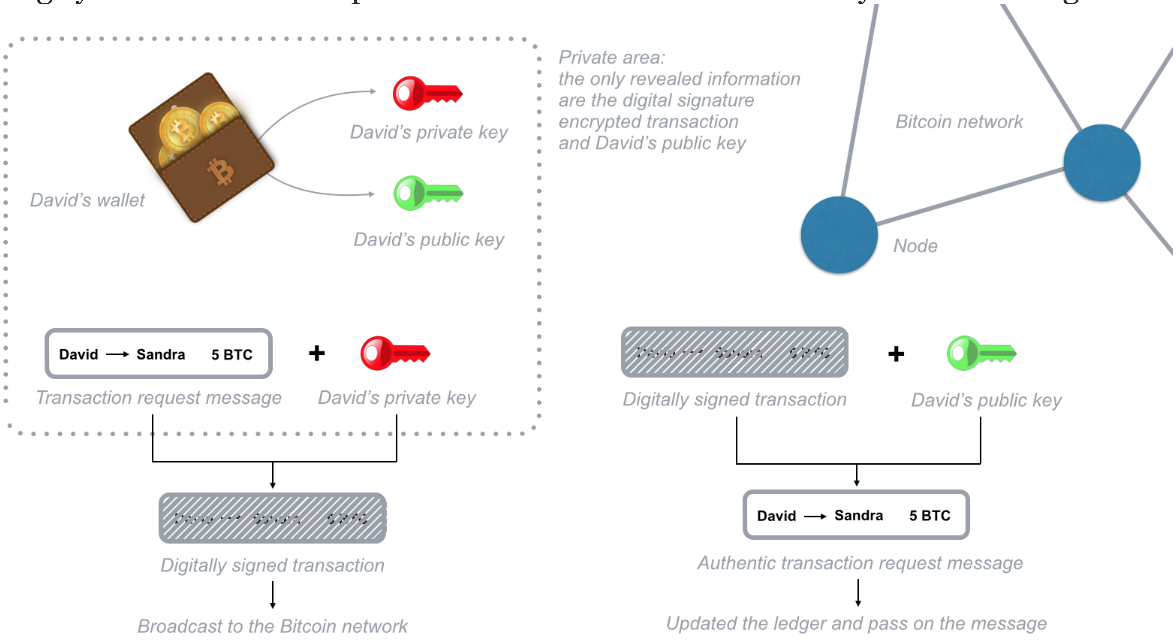
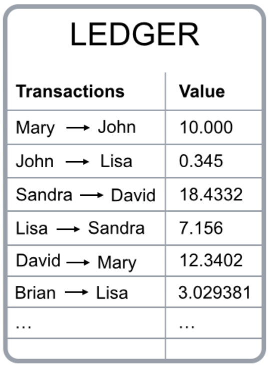

Private area:
the only revealed information are the digital signature encrypted transaction and David's public key
David's wallet
David's private key
David's public key
Bitcoin network
Node
David → Sandra 5 BTC
+
Transaction request message
David's private key
Digitally signed transaction
Broadcast to the Bitcoin network
Digitally signed transaction
David's public key
David → Sandra 5 BTC
Authentic transaction request message
Updated the ledger and pass on the message

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 the key to encrypt your transaction request message. Since you broadcast the message only after it has been encrypted, you never have to reveal your private key.

## Tracking Your Wallet Balance

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

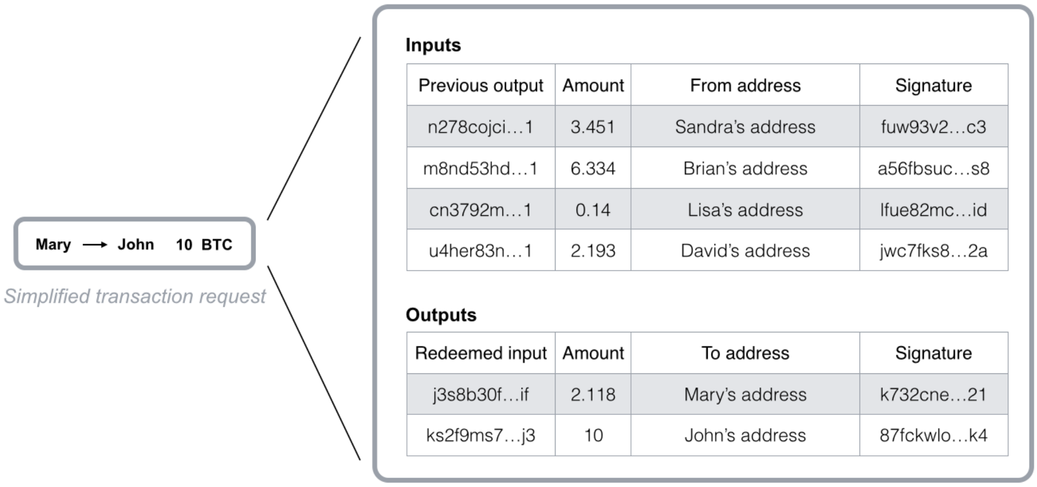


LEDGER

| 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 based on 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 that add up to at least 10 bitcoins. These links are called "inputs." Nodes in the network verify the amount and ensure that these inputs haven't been spent yet. In fact, each time you reference inputs in a transaction, they are deemed invalid for any future transaction. This is all 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.



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 that input transactions are valid? It checks all the previous transactions correlated to the wallet you use to send bitcoins via the input references. To 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 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 used to broadcast a transaction request message, the associated bitcoins will be permanently lost.

Remember that since the network is distributed, there is no customer support to call nor anyone who could help you restore a lost transaction or forgotten wallet password. For this reason, if you are interested in transacting on the bitcoin network, it's a good idea 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.

## But Is It Really Safe? And Why Is It Called Blockchain?

Anyone can access the bitcoin network via an anonymous connection (for example, the 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 with its own private and public keys. This allows you to receive payments on different wallets, and there is no way for anyone 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 bitcoins after spending them. Transactions are passed from node to node within the network, so the order in which two 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 and therefore consider the initial payment transaction invalid, as the transaction inputs would be marked as 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 disagreement among the network nodes regarding the order of transactions each of them received. So the blockchain system has been designed to use node agreement to order transactions and prevent the fraud described above.

The bitcoin network orders transactions by grouping them into blocks; each block contains a definite number 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*.

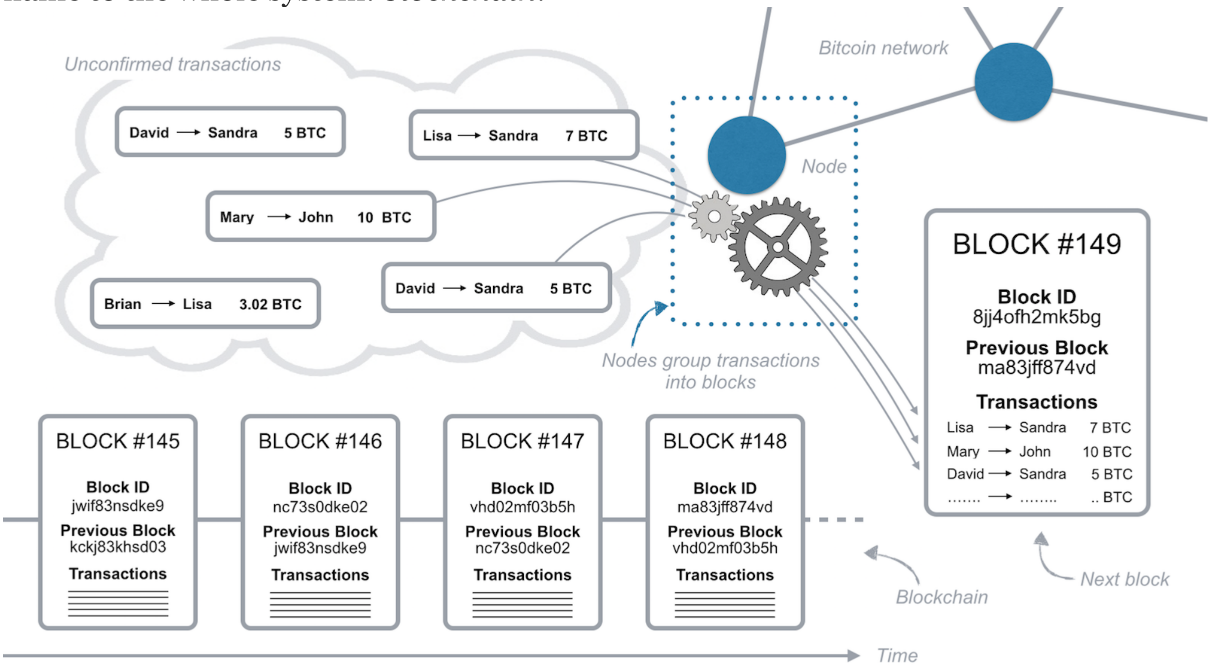


Fig. 6 — The block chain sequence structure simplified

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 into a block and broadcast it to the network as a suggestion for which block should be next. Since any node can suggest a new block, how does the system agree on which block should be the next?

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 a mathematical problem is to guess random numbers that, combined with the previous block content, generate a defined result. It could take about a year for a typical computer to guess the right number and solve the mathematical problem. However, due to the large number of computers in the network that are guessing numbers, a block is solved on average every 10 minutes. The node that solves the mathematical problem acquires the right to place the next block on the chain and broadcast it to the network.

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

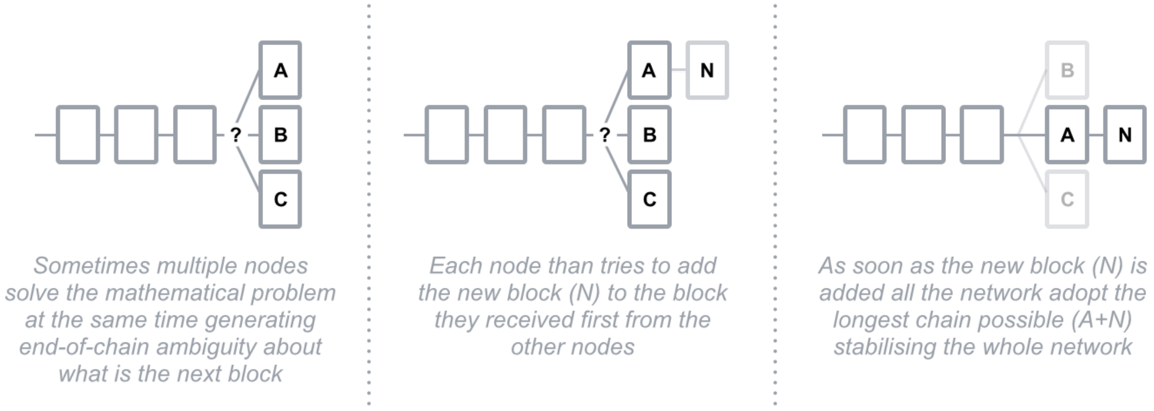

A
?
B
C
Sometimes multiple nodes solve the mathematical problem at the same time generating end-of-chain ambiguity about what is the next block
A
N
?
B
C
Each node than tries to add the new block (N) to the block they received first from the other nodes
B
A
N
C
As soon as the new block (N) is added all the network adopt the longest chain possible (A+N) stabilising the whole network

Fig.7 - End of chain ambiguity logic

Due to the low probability of solving blocks simultaneously, it’s almost impossible that multiple blocks would be solved at the same time over and over, building different “tails,” so the whole blockchain stabilizes quickly to one single string of blocks that every node agrees on.

A disagreement about which block represents 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, this transaction, along with all others in its block, will go back to the unconfirmed transactions.

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

Let’s see how Mary could leverage this end-of-chain ambiguity to perform a double-spending attack. Mary sends money to John, John ships the product to Mary. 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.

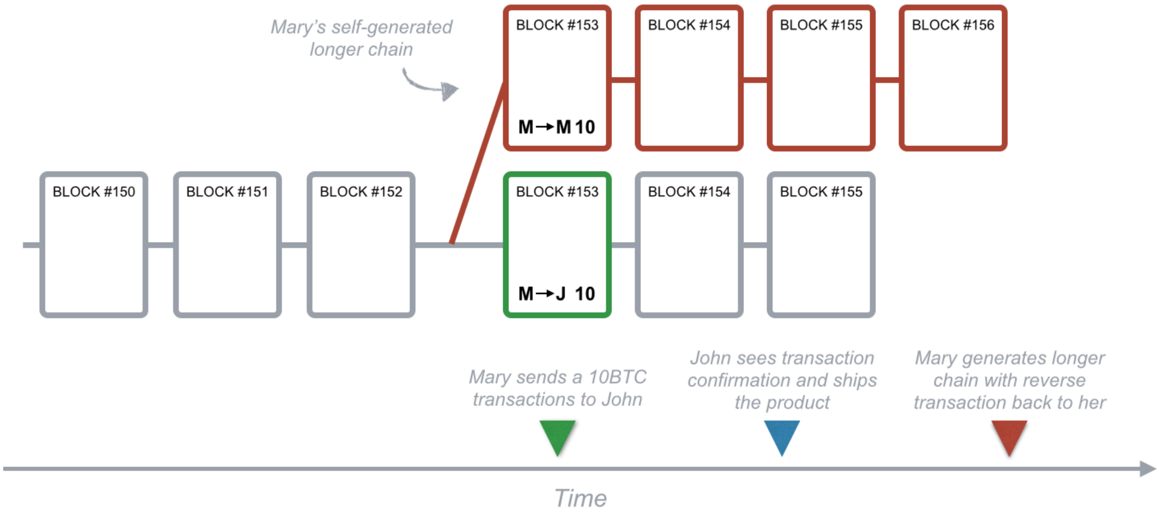

Mary’s self-generated longer chain
BLOCK #153
M→M 10
BLOCK #154
BLOCK #155
BLOCK #156
BLOCK #150
BLOCK #151
BLOCK #152
BLOCK #153
M→J 10
BLOCK #154
BLOCK #155
Mary sends a 10BTC transactions to John
John sees transaction confirmation and ships the product
Mary generates longer chain with reverse transaction back to her
Time

Fig. 8 - Mary’s double-spending attack

How does the system prevent this kind of fraud? Each block contains a reference to the previous block (see Fig. 6). 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. Even if she solves it before anyone else, it’s very unlikely she could solve two, three, or more blocks in a row, since each time she is competing against the whole network.

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 number of members in the network, it's highly 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 percent of the computing power of the whole network to have a 50 percent chance of solving a block before some other node does — and even in this case, she'd only have a 25 percent chance of solving two blocks in a row. The more blocks to be solves in a row, the lower the probability of her success. Transactions in the bitcoin blockchain system are protected by a mathematical race: Any attacker is competing against the entire network.

Therefore, transactions grow more secure with time. Those included in a block confirmed one hour ago, for example, are more secure than those in a block confirmed in the last 10 minutes. Since a block is added to the chain every 10 minutes on average, a transaction included in a block for the first time an hour ago has most likely been processed and is now irreversible.

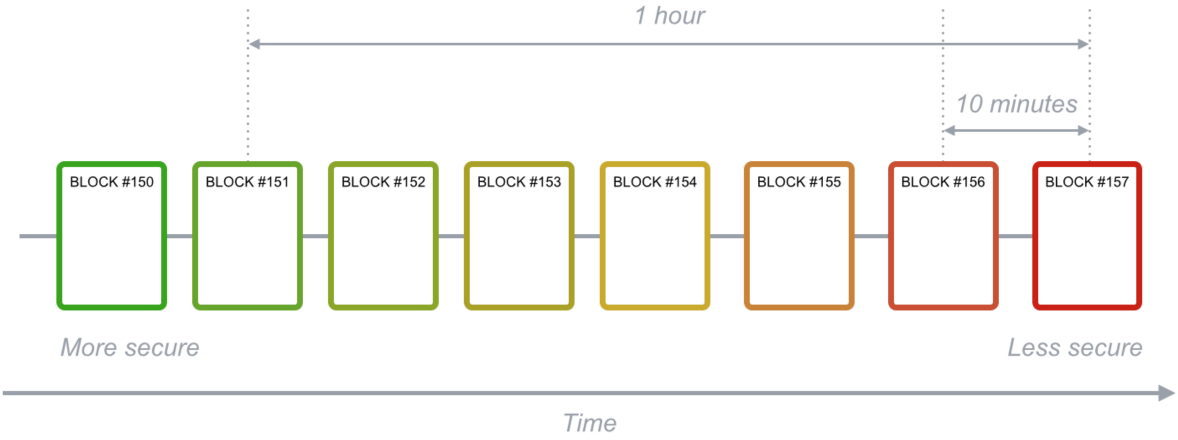


Fig. 9 - Blockchain transactions security

# Mining Bitcoin

In order to send bitcoins, you need to reference an incoming transaction to your own wallet. This applies to every single transaction across the network. So, where do bitcoins come from in the first place?

As a way to balance the deflationary nature of bitcoin due to software errors and wallet password loss, a reward is given to those who 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” — and it’s very much like mining gold.

Rewards are the main incentive for private people to operate the nodes, thus providing the necessary computing power to process transactions and stabilize the blockchain network.

Because it takes a long time for a typical computer to solve a block (about one year on average), nodes band together in groups that divide up the number of guesses to solve the next block. Working as a group speeds up the process of guessing the right number and getting the reward, which is then shared among group members. These groups are called mining pools.

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

However, some of these mining pools with substantial computing power have decided to limit their members in order to safeguard 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 difficulty of solving the next block to target 10 minutes on average for the entire network. This ensures the network’s stability and overall security.

Moreover, every four years the block reward is cut in half, so mining bitcoin (running the network) gets less interesting over time. To encourage nodes to keep operating, small reward fees can be attached to each transaction; these rewards are collected by the node that successfully includes 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. What this means is that, when sending a transaction, you can decide if you’d like to process it faster (more expensive) or cheaper (takes more time). Transaction fees in the bitcoin network are currently very small compared with what banks charge, and they're not associated with the transaction amount.

## Blockchain Benefits and Challenges

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

Using blockchain technology has remarkable benefits:

- You have complete control of the value you own; there is no third party that holds your value or can limit your access to it.
- The cost to perform a value transaction from and to anywhere on the planet is very low. This allows micropayments.
- Value can be transferred in a few minutes, and the transaction can be considered secure after a few hours, rather than days or weeks.
- Anyone at any time can verify every transaction made on the blockchain, resulting in full transparency.
- It's possible to leverage the blockchain technology to build decentralized applications that would be able to manage information and transfer value fast and securely.

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

- Transactions can be sent and received anonymously. This preserves user privacy, but it also allows illegal activity on the network.
- Though many exchange platforms are emerging, and digital currencies are gaining popularity, it's still not easy to trade bitcoins for goods and services.

- Bitcoin, like many other cryptocurrencies, is very volatile: There aren’t many bitcoins available in the market and the demand is changing rapidly. Bitcoin price is erratic, changing based on large events or announcements in the cryptocurrencies industry.

Overall, the blockchain technology has the potential to revolutionize several industries, from advertising to energy distribution. Its main power lies in its decentralized nature and ability to eliminate the need for trust.

New use cases are arising all the time — like the possibility of creating a fully decentralized platform that runs smart contracts like Ethereum. But it’s important to remember that the technology is still in its infancy. New tools are being developed every day to improve blockchain security while offering a broader range of features, tools, and services.

Reference: https://onezero.medium.com/how-does-the-blockchain-work-98c8cd01d2ae