Mastering Bitcoin

By O'Reilly Media, Inc.

[Source](https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/)

Table des matières

[1. Overview 3](#_Toc91013102)

[2. Keys, Addresses, Wallets 4](#_Toc91013103)

[a. Keys 4](#_Toc91013104)

[b. Wallet 4](#_Toc91013105)

[3. Transactions 5](#_Toc91013106)

[c. Lifecycle 5](#_Toc91013107)

[d. Outputs and Inputs 5](#_Toc91013108)

[e. Transactions Scripts 5](#_Toc91013109)

[f. Standard Transactions 5](#_Toc91013110)

[4. Network 6](#_Toc91013111)

[a. P2P 6](#_Toc91013112)

[b. Nodes 6](#_Toc91013113)

[5. Blockchain 8](#_Toc91013114)

[a. Structure 8](#_Toc91013115)

[b. Linking 8](#_Toc91013116)

[6. Mining and Consensus 9](#_Toc91013117)

[a. Verification 9](#_Toc91013118)

[b. Aggregating Transactions 9](#_Toc91013119)

[c. Mining the Block 9](#_Toc91013120)

[d. Assembling 9](#_Toc91013121)

[e. Hashing Race 9](#_Toc91013122)

[f. Attacks 9](#_Toc91013123)

[7. Alts Chains, Currencies and Applications 9](#_Toc91013124)

[8. Bitcoin Security 9](#_Toc91013125)

[a. Security 9](#_Toc91013126)

[b. User Best Practises 9](#_Toc91013127)

[9. Tokenomics 9](#_Toc91013128)

# Overview

* A decentralized peer-to-peer network (the bitcoin protocol)
* A public transaction ledger (the **blockchain**)
* A decentralized mathematical and deterministic currency issuance (distributed mining)
* A decentralized transaction verification system (**transaction script**)

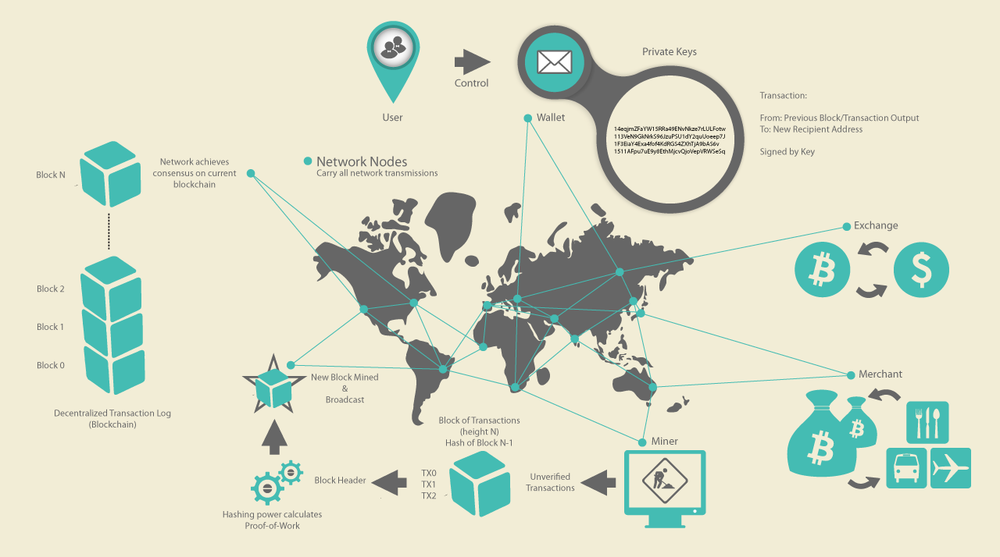


Figure 1: Bitcoin overview

# Keys, Addresses, Wallets

## Keys

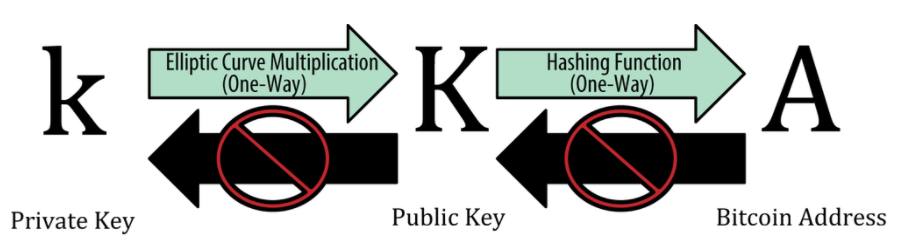


Figure 2: Private key, public key, and bitcoin address

## Wallet

* Bitcoin wallets contain **keys**, not **coins**.
* Users sign transactions with the keys.
* The coins are stored on the blockchain in the form of transaction-ouputs, precisely unspent transaction outputs (**UTXO**).
* **Hot** wallets are connected to the internet
* **Cold** wallets aren’t.

# Transactions

## Lifecycle

* User create the transaction and assigned to an address, this process is called an **encumbrance**
* Broadcasting to the Bitcoin Network
* Each node propagates the transaction on the Bitcoin Network if valid

## Outputs and Inputs

* There are no accounts or balances in bitcoin; there are only unspent transaction outputs (**UTXO**) scattered in the blockchain.
* Coinbase transactions (reward for mining a block) have no input and create outputs from nothing.

## Transactions Scripts

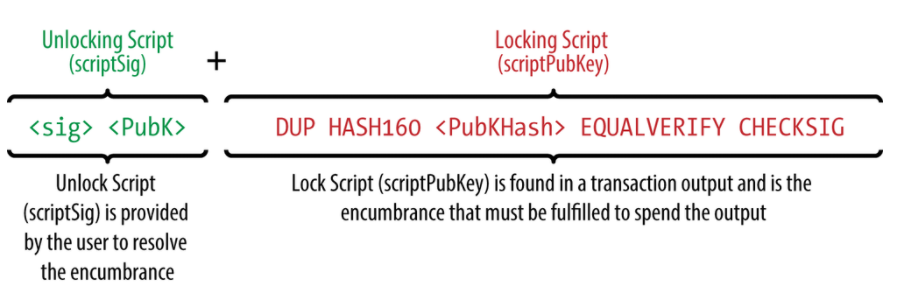


Figure 3: Combining scriptSig and scriptPubKey to evaluate a transaction script

## Standard Transactions

* **Pay-to-Public-Key-Hash (P2PKH):** contain a locking script that encumbers the output with a bitcoin address. Can be unlocked (spent) by presenting a public key and a digital signature created by the corresponding private key.
* **Pay-to-Public-Key (P2PK):** simpler form of P2PKH. The output is encumbered with public key rather than bitcoin address.
* **Multi-Signature**: set a condition where N public keys are recorded in the script and at least M of those must provide signatures to release the encumbrance.
* **Pay-to-Script-Hash (P2SH):** simplify complex script.
* **Pay-to-script-hash address(P2SHA):** hide all of the complexity, so that the person making a payment does not see the script.

# Network

## P2P

* Computers that participate in the network are peers to each other.
* They are all equal, that there are no “special” nodes.
* All nodes share the burden of providing network services.

## Nodes

* Although nodes in the bitcoin P2P network are equal, they may take on different roles depending on the functionality they are supporting
* A bitcoin node is a collection of functions: routing, the blockchain database, mining, and wallet services

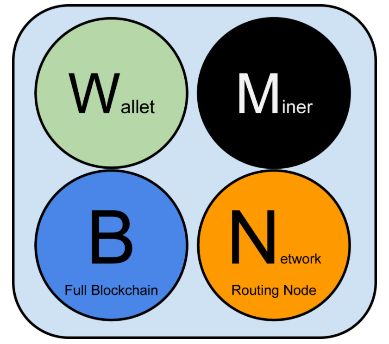


Figure 4: A bitcoin network node with all four functions: wallet, miner, full blockchain database, and network routing

Functionalities a node can support:

* **Wallet (W):** tracks transactions of particular interest plus it holds keys.
* **Miner (M):** compete to create new blocks by running specialized hardware to solve the proof-of-work algorithm.
* **Full Blockchain (B):** maintain a complete and up-to-date copy of the blockchain.
* **Network Routing Node (N):** all nodes include the routing function to participate in the network. All nodes validate and propagate transactions and blocks, and discover and maintain connections to peers.

Different type of node: (not exhaustive)

* **Full node**: contains those 4 functionalities. Can autonomously and authoritatively verify any transaction without external reference.
* **Lightweight node:** maintain only a subset of the blockchain and verify transactions using a method called simplified payment verification, or **SPV**.
* **Mining node:** Some mining nodes are also full nodes, maintaining a full copy of the blockchain, while others are lightweight nodes participating in pool mining and depending on a pool server to maintain a full node.
* **User wallet**: many user wallets, especially those running on resource-constrained devices such as smartphones, are SPV nodes.
* **Full block chain node.**

Miscellaneous:

* **Bloom Filters:** offer an efficient way to express a search pattern while protecting privacy. Ask their peers for transactions matching a specific pattern, without revealing exactly which addresses they are searching for.
* **Transaction pools:** temporary list of unconfirmed transactions called the memory pool, or transaction pool. They are known to the network but are not yet included in the blockchain.

# Blockchain

## Structure

* A block is a container data structure that aggregates transactions for inclusion in the public ledger, the blockchain.
* Each block within the blockchain is identified by a hash on his header.
* The block is made of a header, containing metadata, followed by a long list of transactions that make up the bulk of its size.
* A complete block, with all transactions, is 1,000 times larger than the block header.
* **Merkle tree root**:
  + Data structure used to efficiently summarize and verify integrity of all the transactions in the block.
  + Is used extensively by SPV nodes.
  + SPV nodes don’t have all transactions and do not download full blocks, just block headers.
  + In order to verify that a transaction is included in a block, without having to download all the transactions in the block, they use an authentication path, or merkle path.
* **Genesis Block:** The first block in the blockchain, created in 2009, common ancestor of all blocks.

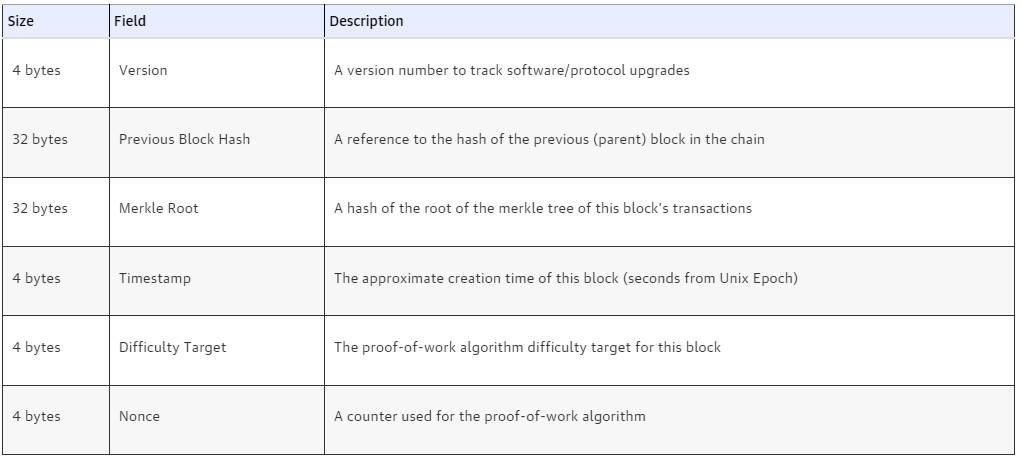


Figure 6: The structure of the block header

Figure 5: Blocks linked in a chain, by reference to the previous block header hash

## Linking

* Blocks are linked “back,” each referring to the previous block in the chain.
* The blockchain is often visualized as a vertical stack.
* Bitcoin full nodes maintain a local copy of the blockchain, starting at the genesis block.
* The local copy of the blockchain is constantly updated as new blocks are found and used to extend the chain.
* As a node receives incoming blocks from the network, it will validate these blocks and then link them to the existing blockchain.
* To establish a link, a node will examine the incoming block header and look for the “previous block hash.”
* The primary identifier of a block is its cryptographic hash
* A second way to identify a block is by its position in the blockchain, called the block height

# Mining and Consensus

## Verification

Bitcoin’s decentralized consensus emerges from the interplay of four processes that occur independently on nodes across the network:

* **Independent verification** of each transaction, by every full node, based on a comprehensive list of criteria
* **Independent aggregation** of those transactions into new blocks by mining nodes, coupled with demonstrated computation through a **proof-of-work algorithm**
* **Independent verification** of the new blocks by every node and assembly into a chain
* **Independent selection**, by every node, of the chain with the most cumulative computation demonstrated through proof of work

## Aggregating Transactions

* Bitcoin node selects transactions from the memory pool by applying a priority metric to each transaction and adding the highest priority transactions first.
* Priority is calculated by the value of the UTXO, its age and its size

## Mining the Block

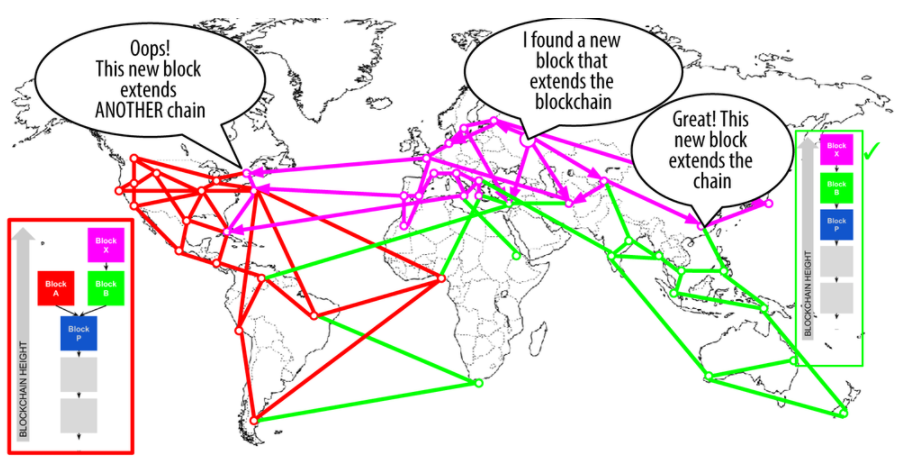
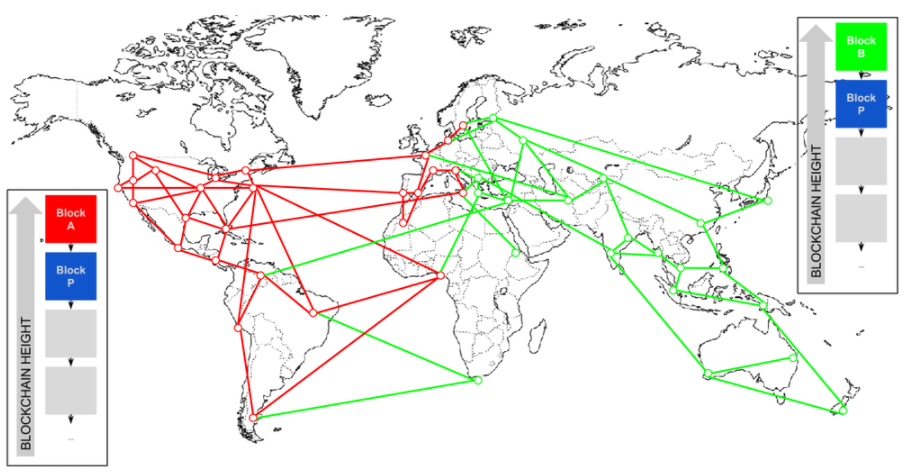
* Mining is the process by which new bitcoin is added to the money supply.
* Mining also serves to secure the bitcoin system.
* Miners validate new transactions and record them on the global Ledger.
* In the simplest terms, mining is the process of **hashing the block header repeatedly**, changing one parameter, the nonce, **until the resulting hash matches a specific target**, below a certain number causes by the difficulty.
* Every 2,016 blocks, all nodes retarget the proof-of-work difficulty.
* The equation for retargeting difficulty measures the time it took to find the last 2,016 blocks and compares that to the expected time of 20,160 minutes (two weeks based upon a desired 10-minute block time).
* If the network is finding blocks **faster** than every 10 minutes, the **difficulty increases**.
* If block discovery is **slower** than expected, the **difficulty decreases**.

## Mining pool

* In this highly competitive environment, individual miners working don’t stand a chance.
* Even the fastest consumer ASIC mining system cannot keep up with commercial systems that stack tens of thousands of these chips.
* Miners now collaborate to form mining pools, pooling their hashing power and sharing the reward among thousands of participants.
* By participating in a pool, miners get a smaller share of the overall reward, but typically get rewarded every day, reducing uncertainty.
* The mining pool sets a lower difficulty target for earning a share, typically more than 1,000 times easier than the bitcoin network’s difficulty.
* When someone in the pool successfully mines a block, the reward is earned by the pool and then shared with all miners in proportion to the number of shares they contributed to the effort.

## Assembling

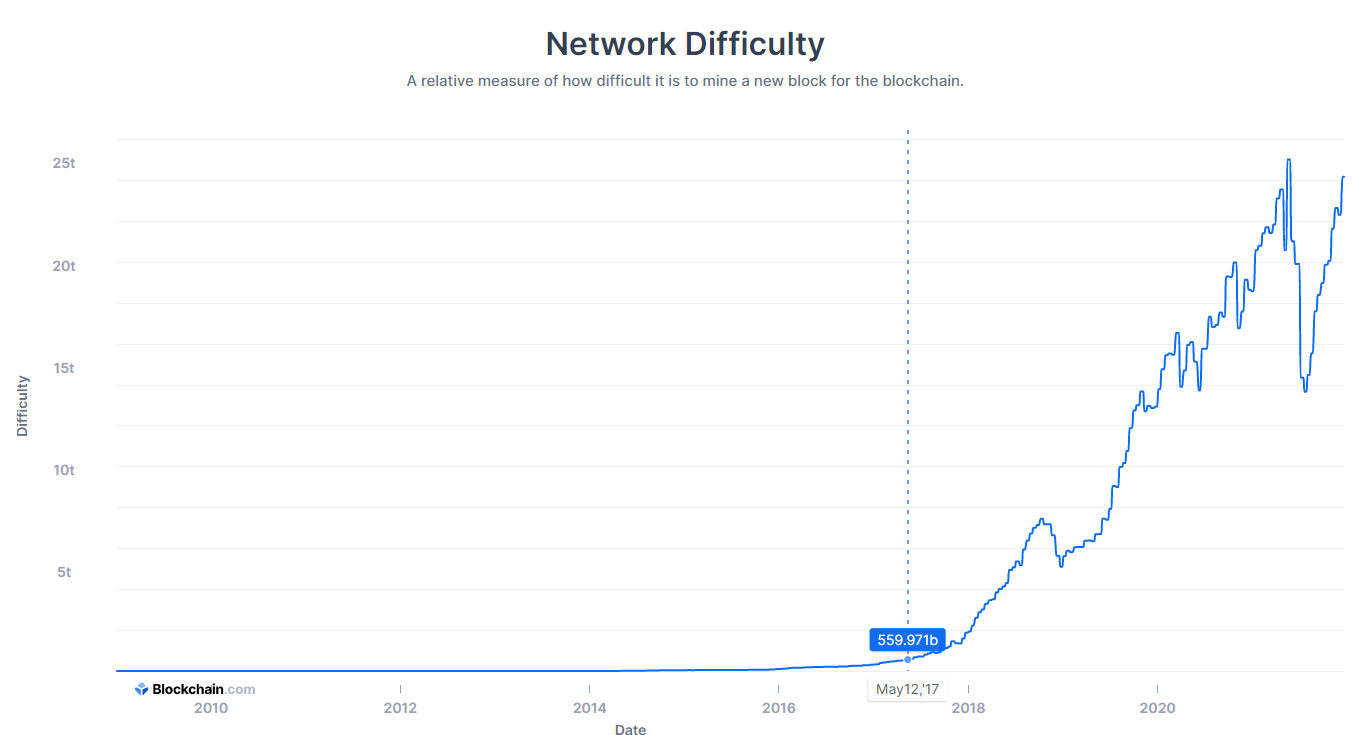
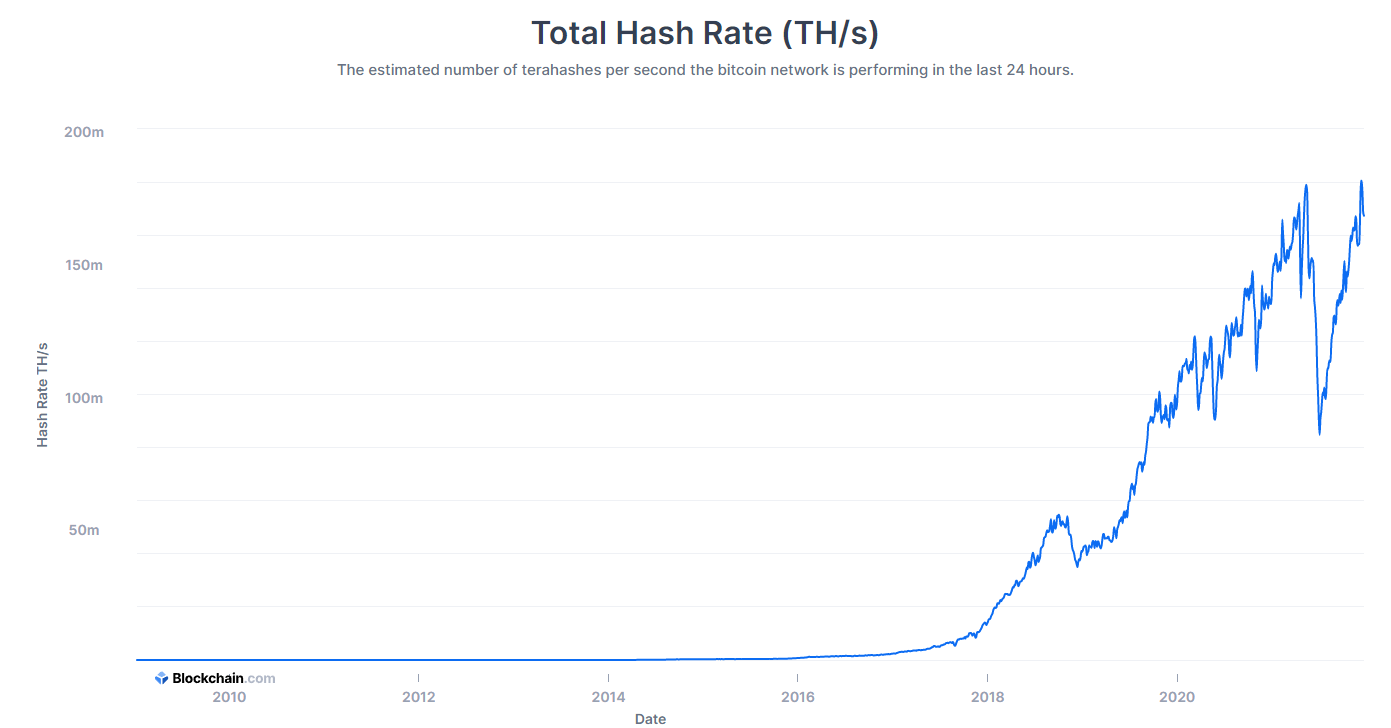
* Blocks might arrive at different nodes at different times, causing the nodes to have different perspectives of the blockchain, creating a **blockchain fork**.
* To resolve this, each node always selects and attempts to extend the chain of blocks that represents the most proof of work, thus the longest chain or greatest cumulative difficulty chain.



|  |  |
| --- | --- |
| Figure 7-a: Visualization of a blockchain  fork event: two blocks propagate, splitting the network | Figure 7-b: Visualization of a blockchain fork event: the network reconverges on a new longest chain |

## Hashing Race

* Bitcoin mining is an extremely competitive industry.
* The hashing power has increased exponentially.
* CPU -> GPA -> FPGA -> ASIC: application-specific integrated circuit with SHA256 function directly on silicon chips.



|  |  |
| --- | --- |
| Figure 8-a: The estimated number of terahashes () per second the bitcoin network is performing | Figure 8-b: A relative measure of how difficult it is to mine a new block for the blockchain. |

## Consensus Attacks

* If a miner or group of miners can achieve a significant share of the mining power, they can attack the consensus mechanism so as to disrupt the security and availability of the bitcoin network.
* It is important to note that consensus attacks can only affect future consensus, or at best the most recent past (tens of blocks).
* Bitcoin’s ledger becomes more and more immutable as time passes.
* While in theory, a fork can be achieved at any depth, in practice, the computing power needed to force a very deep fork is immense, making old blocks practically immutable.
* Consensus attacks also do not affect the security of the private keys and signing algorithm (ECDSA).
* The attacking miners can cause deliberate “forks” in the blockchain and double-spend transactions or execute denial-of-service attacks against specific transactions or addresses.
* Those attacks might be possible but increasingly impractical as the bitcoin network’s overall hashing power continues to grow exponentially.

# Alts Chains

* With new coins introduced every day, it would be impossible not to miss some important coin, perhaps the one that changes history.
* The vast majority of alt coins are derived from bitcoin’s source code, also known as “forks.”
* Some are implemented “from scratch”.
* Reals alt chains try to use benefits of Bitcoin and adding new features at the cost of some feature in Bitcoin.
* **Blockchain trilemma:** a set of three main issues that developers encounter when building blockchains. More often than not, creators are forced to sacrifice one ‘aspect’ for the sake of the other two.

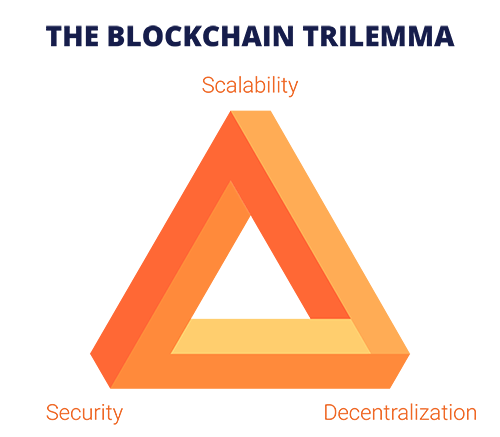
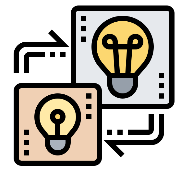
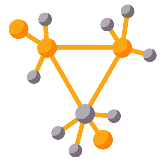


Figure 8: Blockchain trilemma

* **Scalability:** 
  + Enables the network to support a higher workload.
  + Helps specific protocols that inherently require support for a high number of transactions per second (TPS).
* **Security:**
  + Security is the only fundamental part required for the blockchain network to actually work.
  + Without security, blockchain networks are completely unreliable and useless.
* **Decentralization:** 
  + All participants have equal power.
  + Can change the protocol through governance proposals.
  + More nodes mean that larger entities control less power.
  + Democratic-like governance members can bring forward controversial features.
  + Most protocols achieve decentralization through a Proof of Work consensus mechanism: requires a lot of energy and incapable of reaching high TPS.

# Bitcoin Security

## Security

* A bitcoin wallet, containing your keys, can be backed up like any file.
* Bitcoin are represented by UTXO on the global ledger, the blockchain.

## User Best Practices

* Modern general-purpose operating systems are not very secure and not particularly suited to storing digital money.
* Our computers are constantly exposed to external threats via always-on Internet connections.
* They run thousands of software components from hundreds of authors, often with unconstrained access to the user’s files.
* The level of computer maintenance required to keep a computer virus-free and trojan-free is beyond the skill level of all but a tiny minority of computer users.
* That’s why it is highly recommended to store the key on **hardware wallet**.
* Keep hardware wallet on **different private location.**
* Diversify in multiple wallet.
* **Multi-signature addresses** secure funds by requiring more than one signature to make a payment.
* In case of death or incapacity you should consider **sharing access** details with a **trusted relative** or lawyer.

# Tokenomics

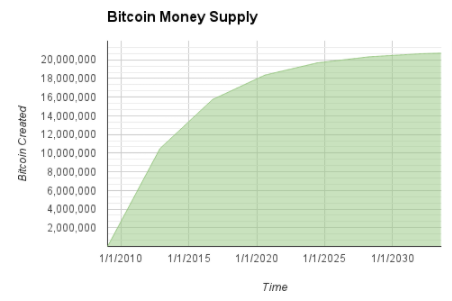
* 1 BTC = 100,000,000 Satoshis.

Figure 9: Supply of bitcoin currency over time based on a geometrically decreasing issuance rate

* Total supply: 21M BTC in 2140.
* BTC is deflationary.
* A new block is “mined” every 10 minutes.
* Miners receive two types of rewards for mining: new coins created with each new block, and transaction fees from all the transactions included in the block.
* Every four year (210,000 blocks) the currency issuance rate is decreased by 50%.