FTEC 5520 (Week 4)

Agenda – Concept of Blockchain – Week 4

- Concept of Blockchain from Bitcoins
- 1. Basics of Blockchain from Bitcoins
- 2. How to transact Bitcoins (Simple version)
- 3. Bitcoins transaction (Technical view)
- 4. Bitcoin Address
- 5. Crypto Mining
- 6. Merkle Tree
- 7. Beyond Satoshi Paper

Basics of Blockchain

Concept of Blockchain – 6 key elements

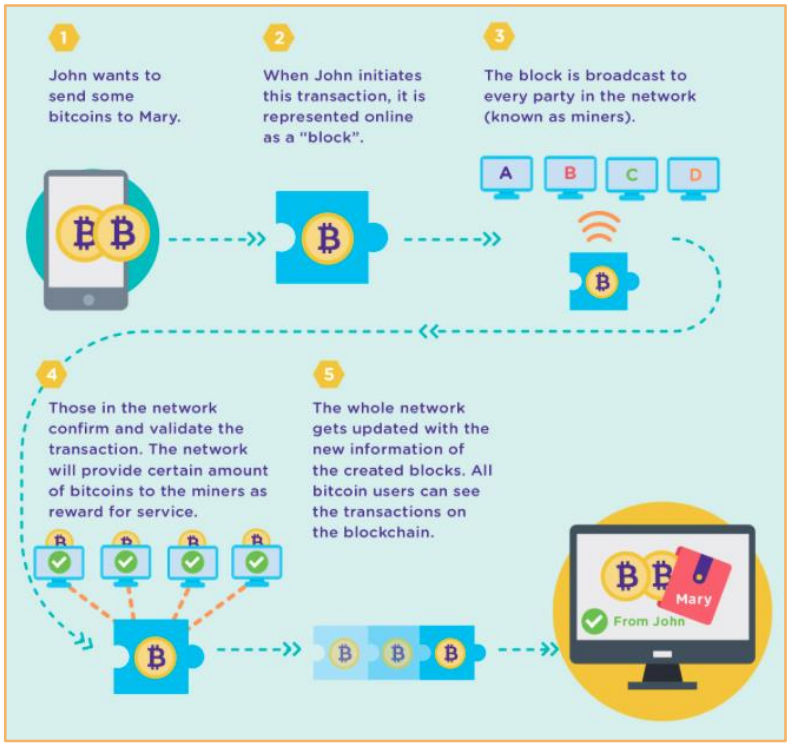
- Decentralized
- Transparent
- Open Source
- Autonomy
- Immutable
- Anonymity

What is Blockchain (Starts from Bitcoin)

Blockchain technology is the underlying foundation of “cryptocurrencies”.

Every single transaction that takes place in bitcoin network is recorded in a shared public ledger.

Whenever a new block of transactions is created, it is added to the blockchain.



Bitcoin usage

Bank and decentralized digital cash

Bank transaction ledger in centralized bank. Decentralized by putting to the internet

But in the Internet, then can it be broadcast or shared via the Internet?

Who can write the content to the ledger?

How can we consider the ledger info is correct?

How can we ensure ledger info synchronised are correct?

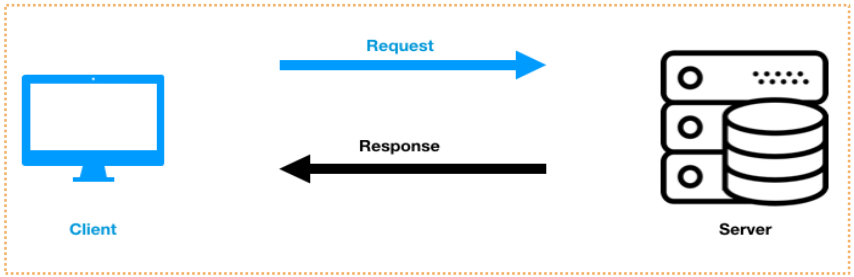
Which chain is correct?

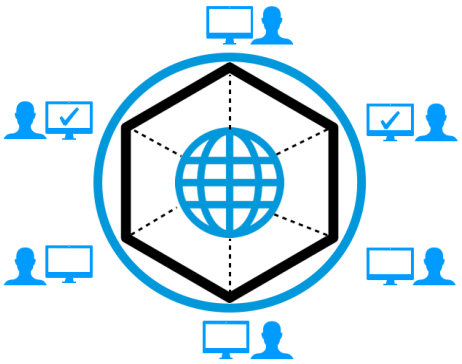
Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System"

"Bitcoin: A Peer-to-Peer Electronic Cash System," Satoshi Nakamoto (https://bitcoin.org/bitcoin.pdf), 2008

Nakamoto combined the ideas

- B-money and HashCash to create a completely decentralized electronic cash system
- Proof-of-Work algorithm for consensus about the state of transactions
- Prevent and resolve the double-spending





Peer-to-Peer Blockchain Network

Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Problems that this paper aim to solve

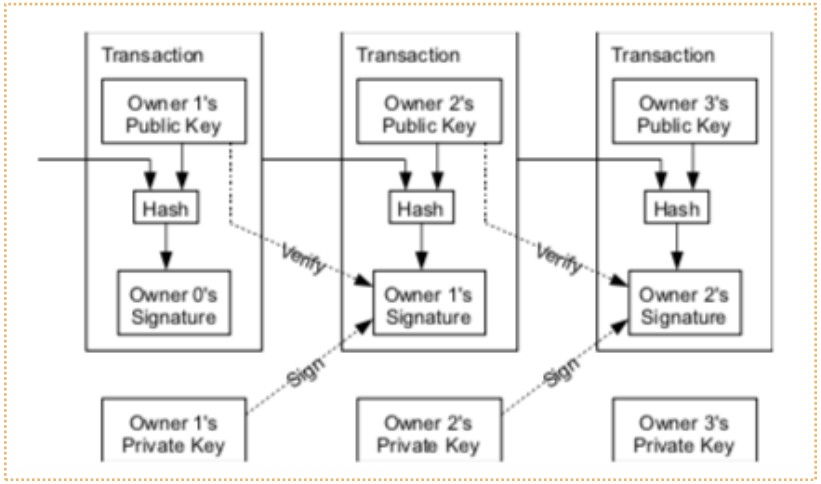
- Non-reversible transactions
- Efficient transaction verification
- Double spending in distribution manner

Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Terminology

Terms	Definition
Blockchain	The actual Ledger
Blockchain technology	a term to describe the technology in the most generic form
Blockchain network	the network in which a blockchain is being used
Blockchain implementation	a specific blockchain
Blockchain network user	a person, organization, entity, business, government, etc. which is utilizing the blockchain network
Node	an individual system within a blockchain network
Full node	a node that stores the entire blockchain, ensures transactions are valid
Publishing node	a full node that also publishes new blocks
Lightweight node	a node that does not store or maintain a copy of the blockchain and must pass their transactions to full nodes
UTXO	An abbreviation for Unspent Transaction Output, also referred to as an "output".
satoshi	1 BTC = 100,000,000 satoshi

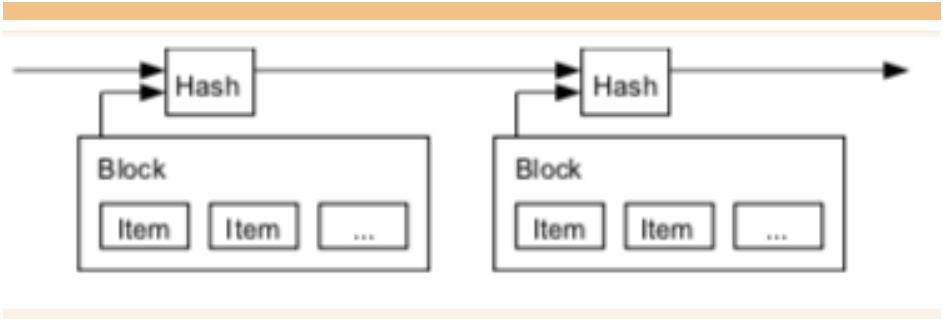
Terminology adopted from NIST IR 8202

Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Non-reversible transactions



Hash Chain

Timestamp of hash



Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Non-reversible transactions

Data structure of the Blockchain

- Block size (4 byte)
- Block header having Meta information (80 byte)
- Whenever a transaction occurs, a block of the transaction record is created and linked
- The transaction is transmitted to all participants, and the validity of the transaction is approved. The approval method is a proof of work
- the parent block constitute a chain connected to the first block. 32 byte value generated by encoding of the block header through SHA256 encoding hash algorithm is called the block hash
- In the connecting structure of the block, the block has an identifiable hash value for header information of the previous block, while the block has a structure connected by referring to the value.

Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" What's in a Block

Data structure of the blockchain

Table 1 Block structure

Size	Field	Description
4 byte	Block size	Size of block
80 byte	Block header	Meta information recorded in block
1–9 byte (varInt)	Block transaction no	No of block transactions
Variable	Transaction record	Transaction recorded in block

Data: Antonopoulos (2015)

Table 2 Structure of block header

Size	Field	Description
4 byte	Version	Version no for tracking of software/protocol upgrade
32 byte	Hash of previous block	Value allowing reference to the hash data of previous block/parent block that the chain has
32 byte	Merkle root	Root of Merkle tree included in transaction information that the relevant block has
4 byte	Time stamp	Time for block generation
4 byte	Difficulty target	Difficult target of difficulty for algorithm that the operation proof method has
4 byte	Nonce	Counter applied to the algorithm that the operation proof method has

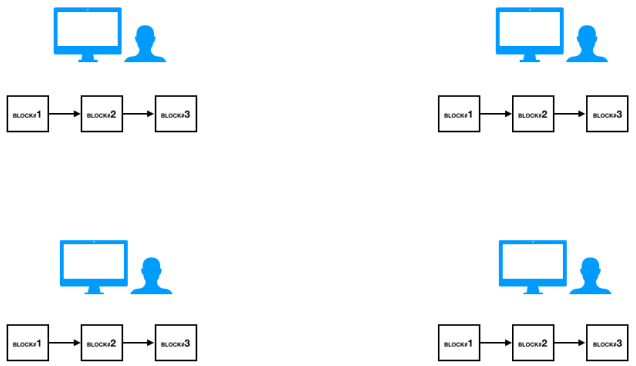
Data: Antonopoulos (2015)

Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Non-reversible transactions

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof- of-work system similar to Adam Back's Hashcash

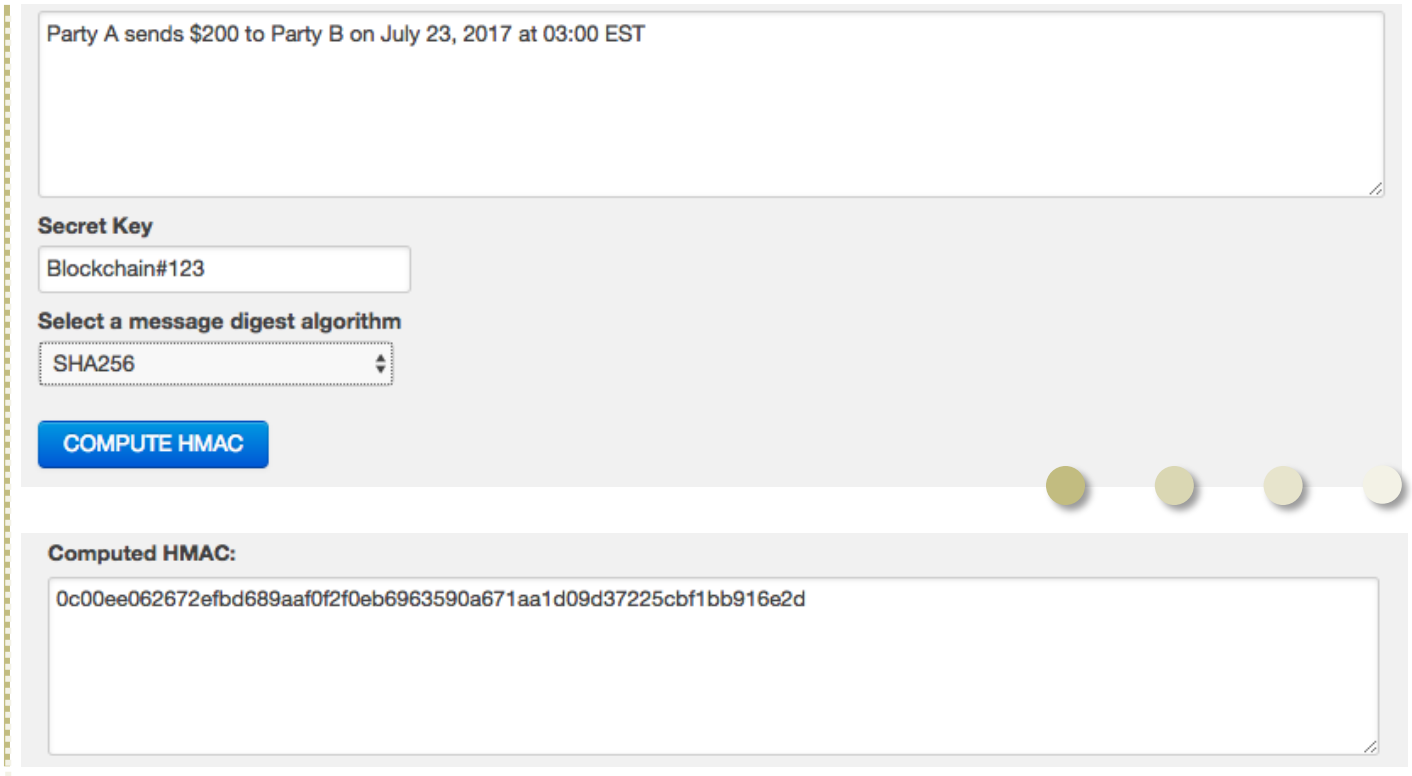
The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits.

The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs.



Blockchain Nodes with ledgered blocks

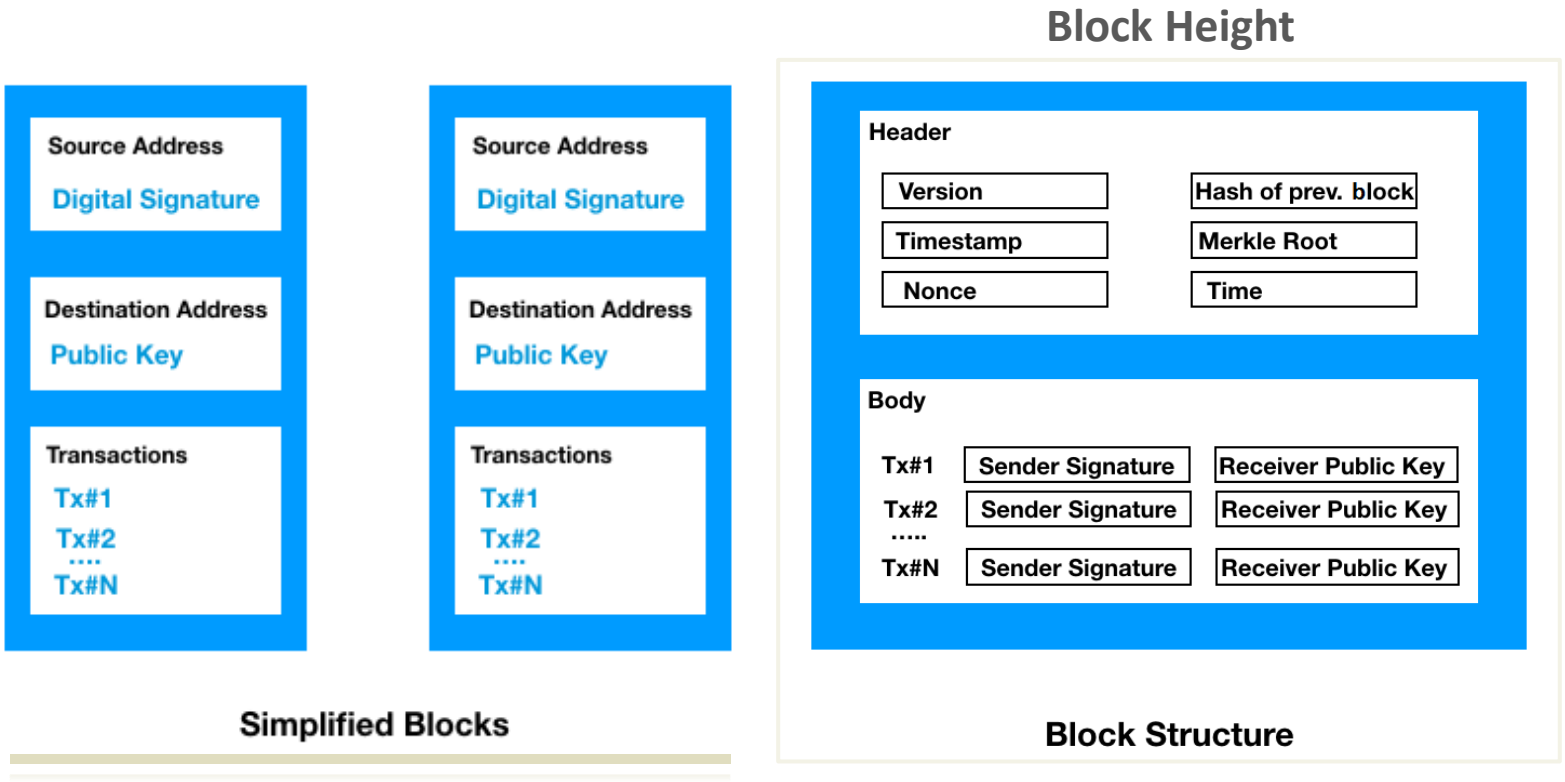
Template to store hash and transaction in Blockchain



https://www.freeformatter.com/hmac-generator.html.

Excerpt From: Rajneesh Gupta. “Hands-On Cybersecurity with Blockchain”. Apple Books.

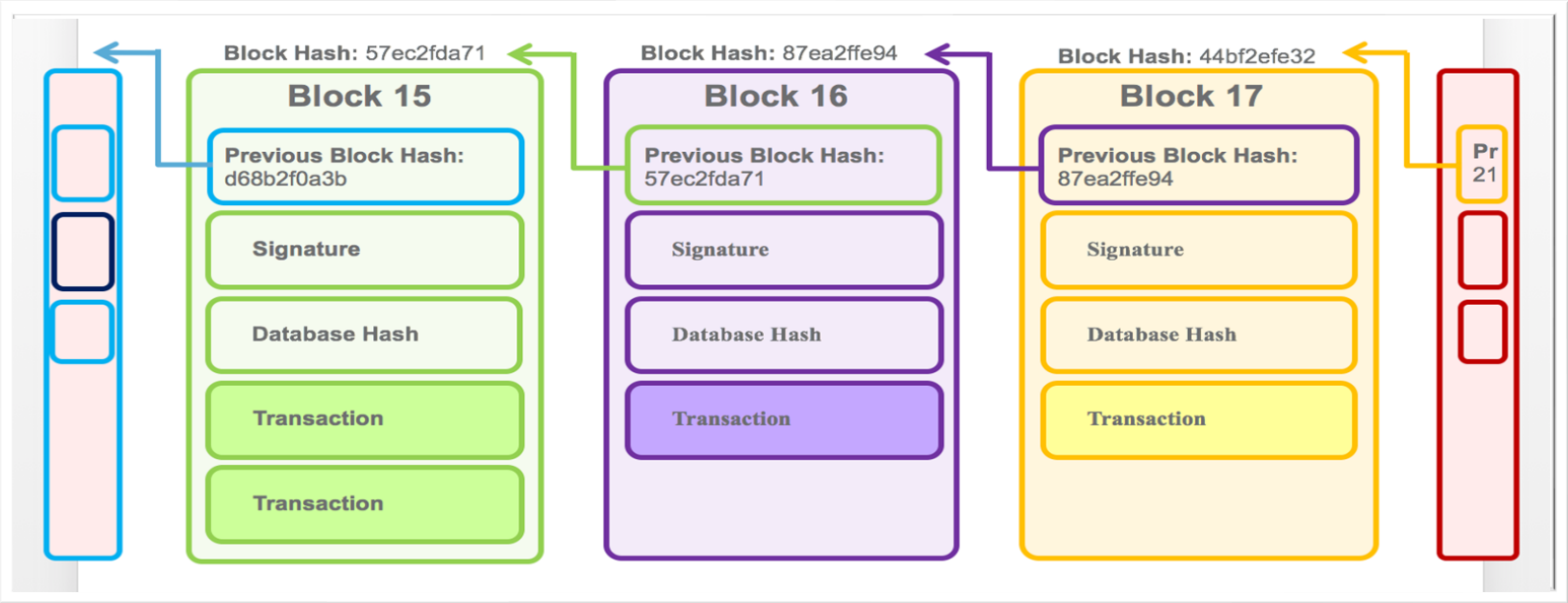
Transaction and storage in Blockchain



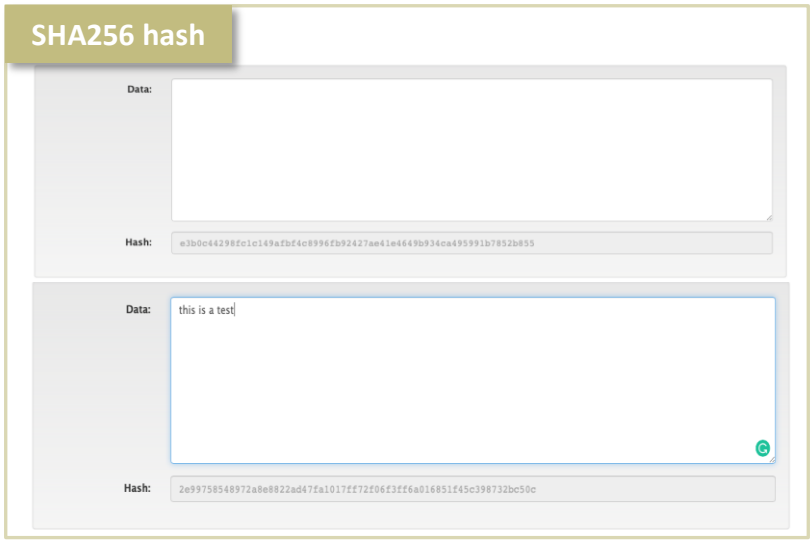
From Hands-on Cybersecurity with Blockchain

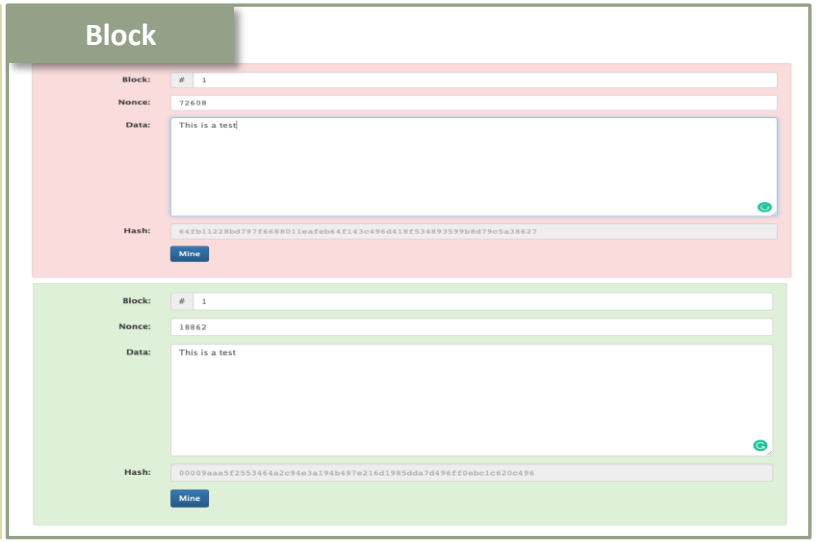
Transaction and storage in Blockchain

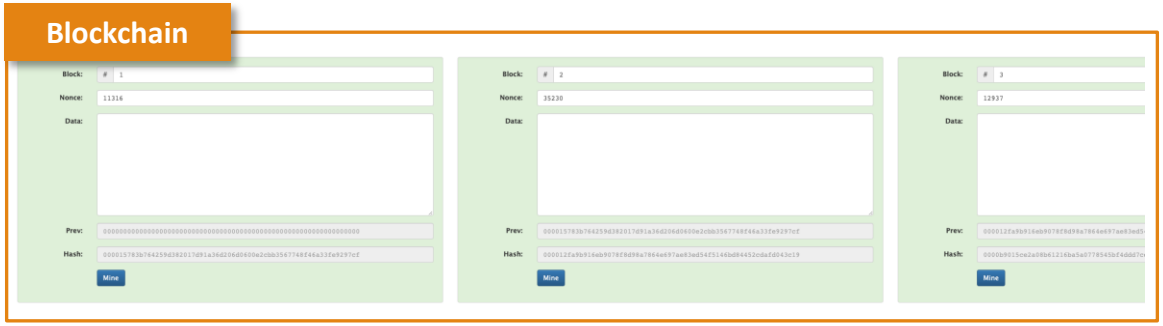
- Another form of identification for a block is the ‘Block Height’.
- Each block is ‘piled’ on top of another therefore adding +1 to the count of the ‘height’.
- Meaning that starting from block #0 (Genesis block) each new block adds to the total height.



Cryptography applied to blockchain







https://andersbrownworth.com/blockchain/hash
https://andersbrownworth.com/blockchain

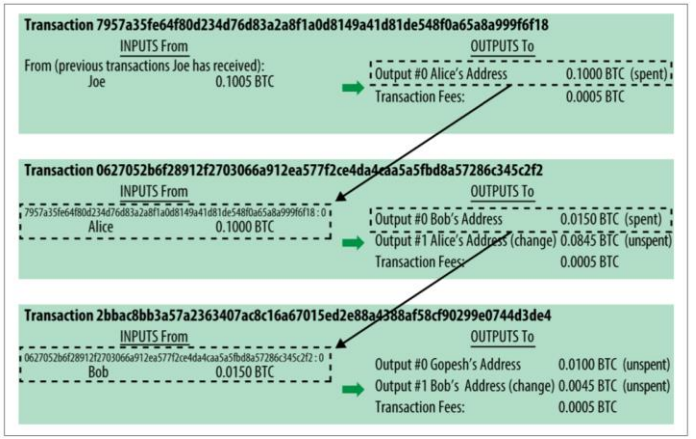
Bitcoin Transaction

A Bitcoin transaction is a set of records and data about transactions kept in a decentralized public ledger.

Once a transaction is confirmed, its record goes to the main blockchain.

This enables Bitcoin wallets to figure out a spendable balance and for new transactions to pass the process of verification

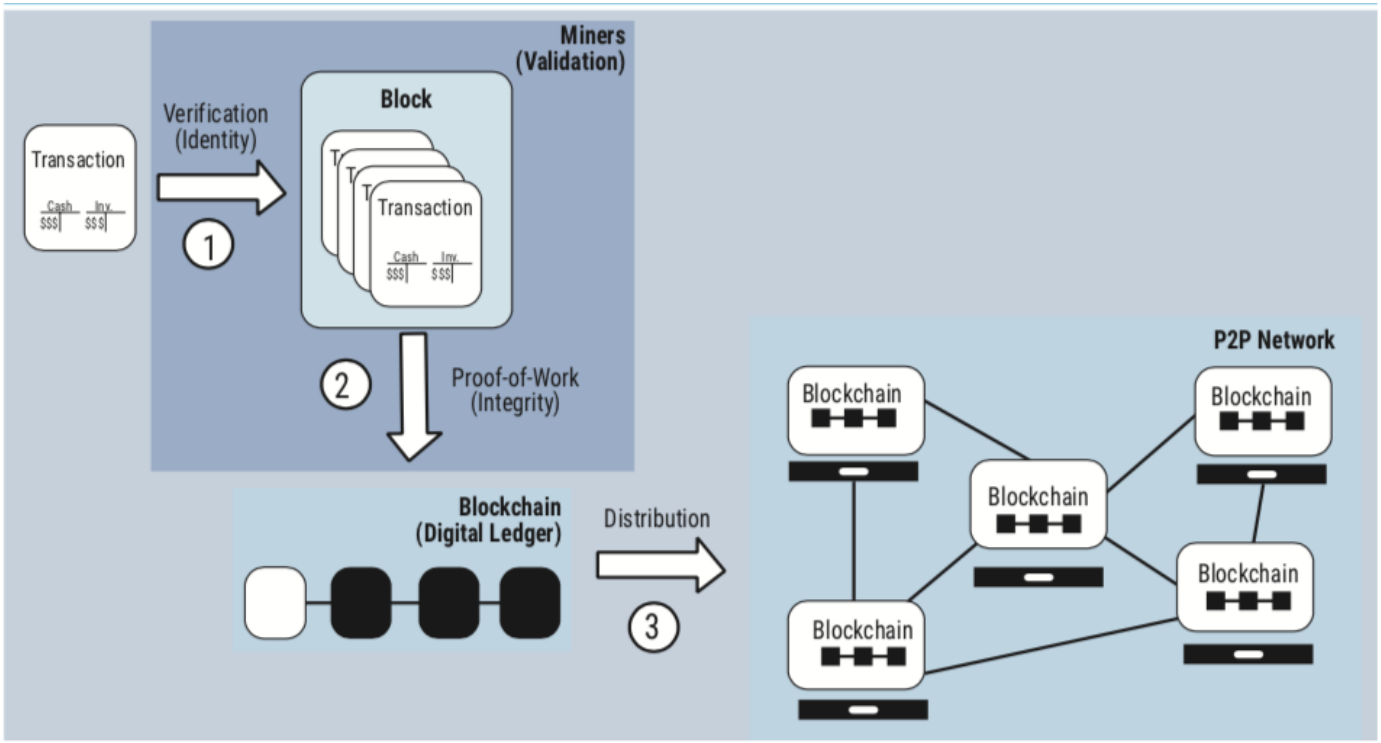
In addition, this allows the actual owner to determine whether or not he or she has sufficient funds to proceed with a transaction.



A Chain of transactions

A transaction can contain multiple inputs and outputs. As long as each output has an associated amount and the input amounts total more than the output amounts, the transaction is valid.

Transaction Process in Blockchain (Diagram)



From ISACA, “Blockchain Explained and Implications for Accountancy”, 2019

Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Double spending in distribution manner

According to the paper

- Nodes always consider the longest chain to be the correct one and will keep working on extending it.
- If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer.
- The tie will be broken when the next proof- of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Efficient transaction verification

According to the paper

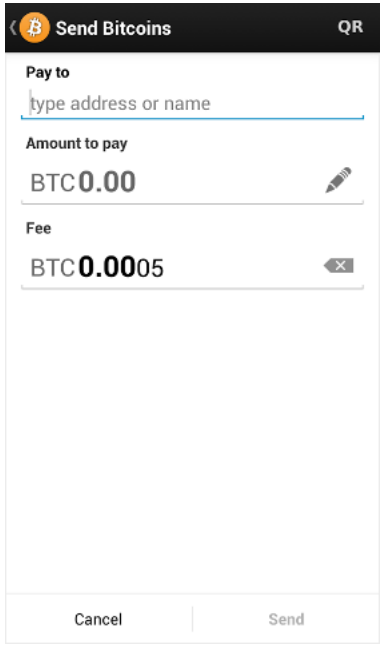
- To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash.
- A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in

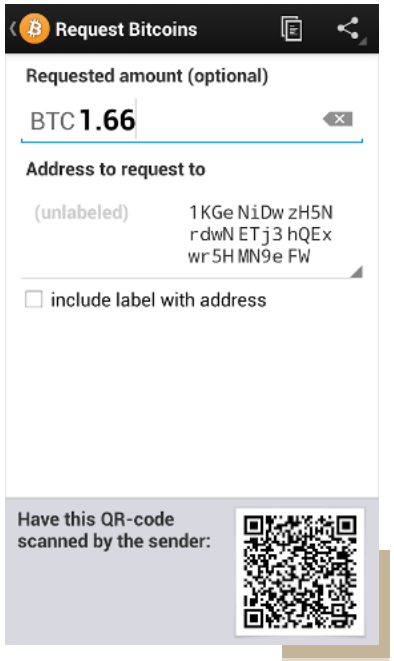
How bitcoin payment can be performed

Bitcoin payments are easier to make than debit or credit card purchases, and can be received without a merchant account.

Payments are made from a wallet application, either on your computer or smartphone, by entering the recipient's address, the payment amount, and pressing send.

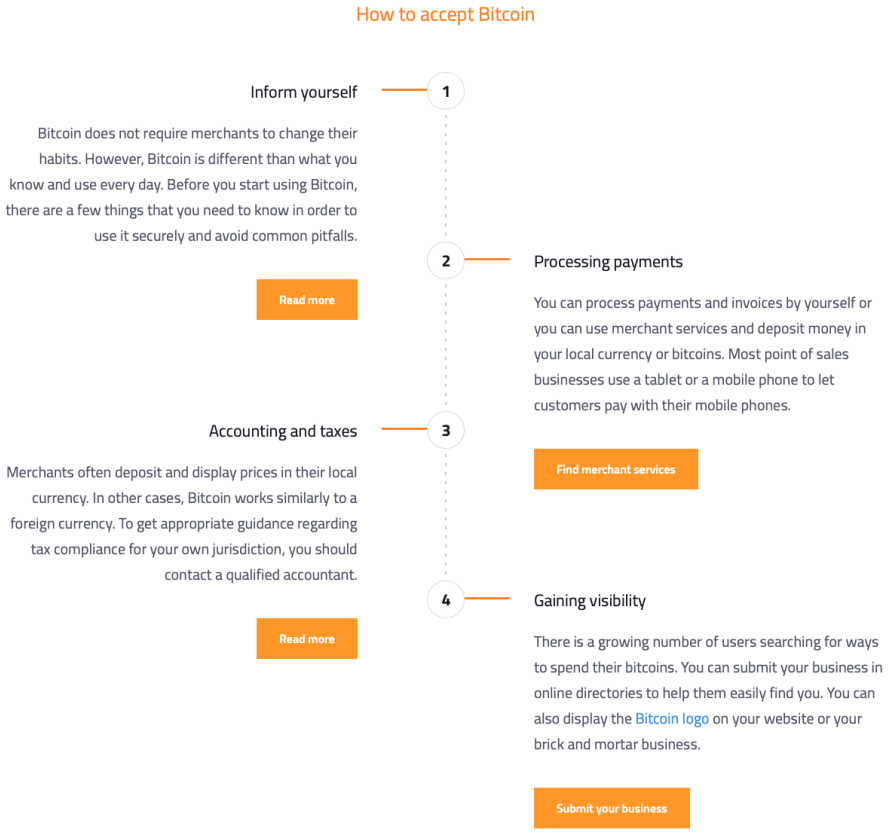
To make it easier to enter a recipient's address, many wallets can obtain the address by scanning a QR code or touching two phones together with NFC technology.





How to transact Bitcoins

How to transact Bitcoins



Use a Bitcoin Exchange

Our Bitcoin Exchange page, lists many different businesses that can help you buy bitcoin using your bank account.

Browse a P2P Directory

Using an exchange based off of a peer-to-peer directory lets you search and browse through various sellers of bitcoin. Sellers have reviews and feedback scores to help you choose.

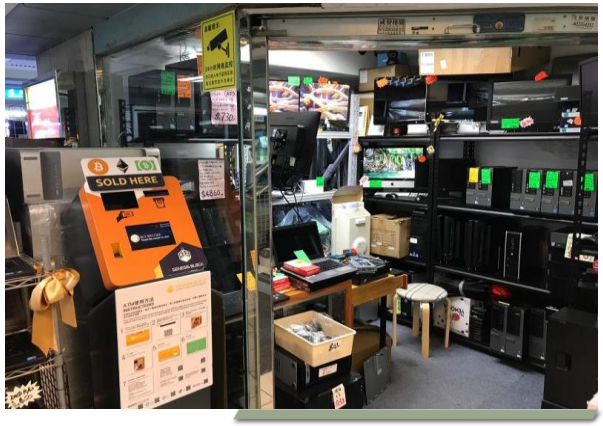
Use a Bitcoin ATM

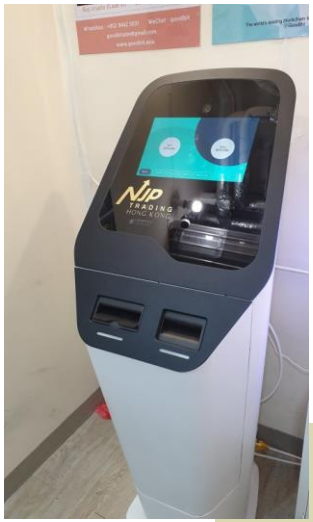
Bitcoin ATMs work like a regular ATM, except they allow you to deposit and withdrawal money so that you can buy and sell bitcoin. Coin ATM Radar has an interactive map to help you find the closest bitcoin ATM near you.

Cryptocurrency ATM machines

Cryptocurrency ATM machines

Cryptocurrency ATM machines





Bitcoin transactions (technical view)

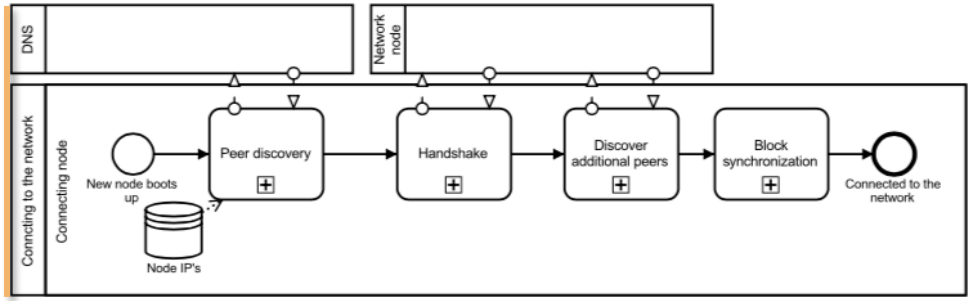
Four Reference Processes in Blockchain

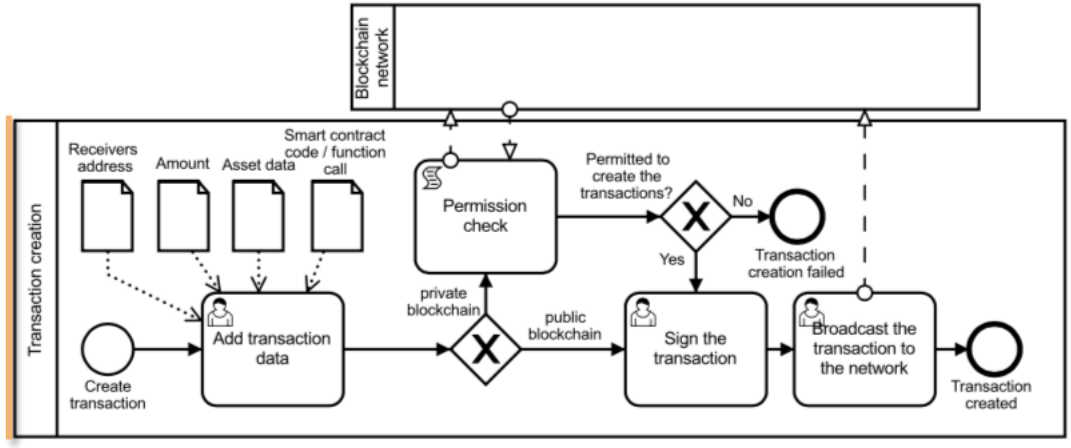
Network discovery process

Transaction process

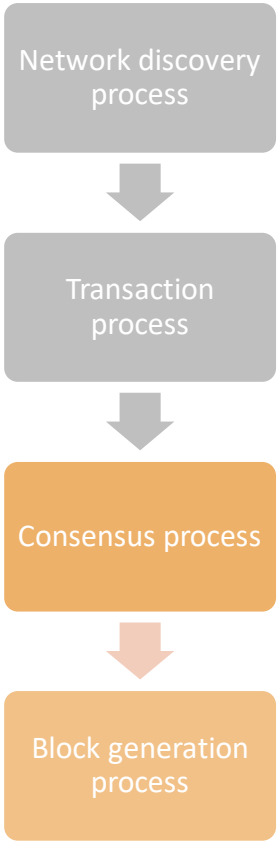
Consensus process

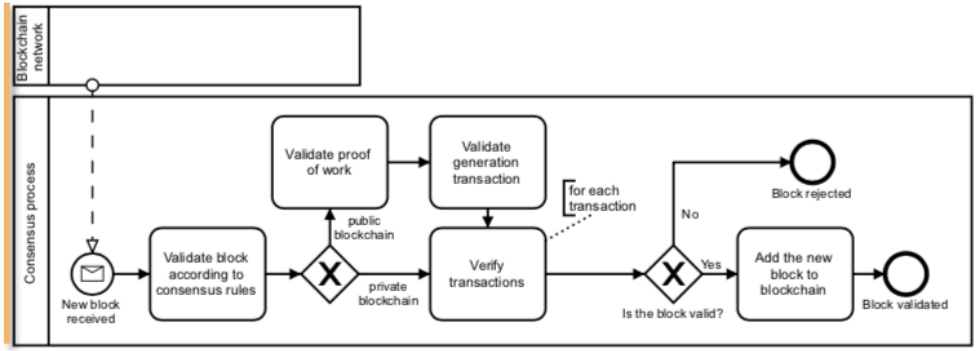
Block generation process

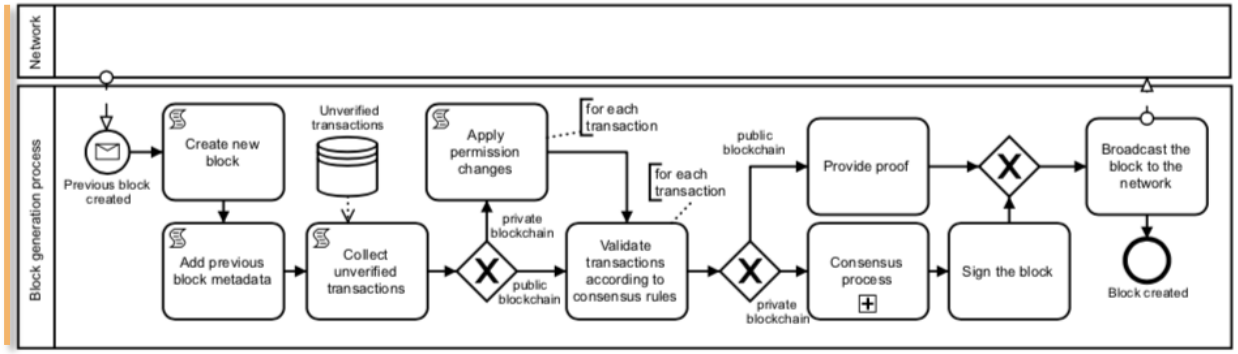




Four Reference Processes in Blockchain





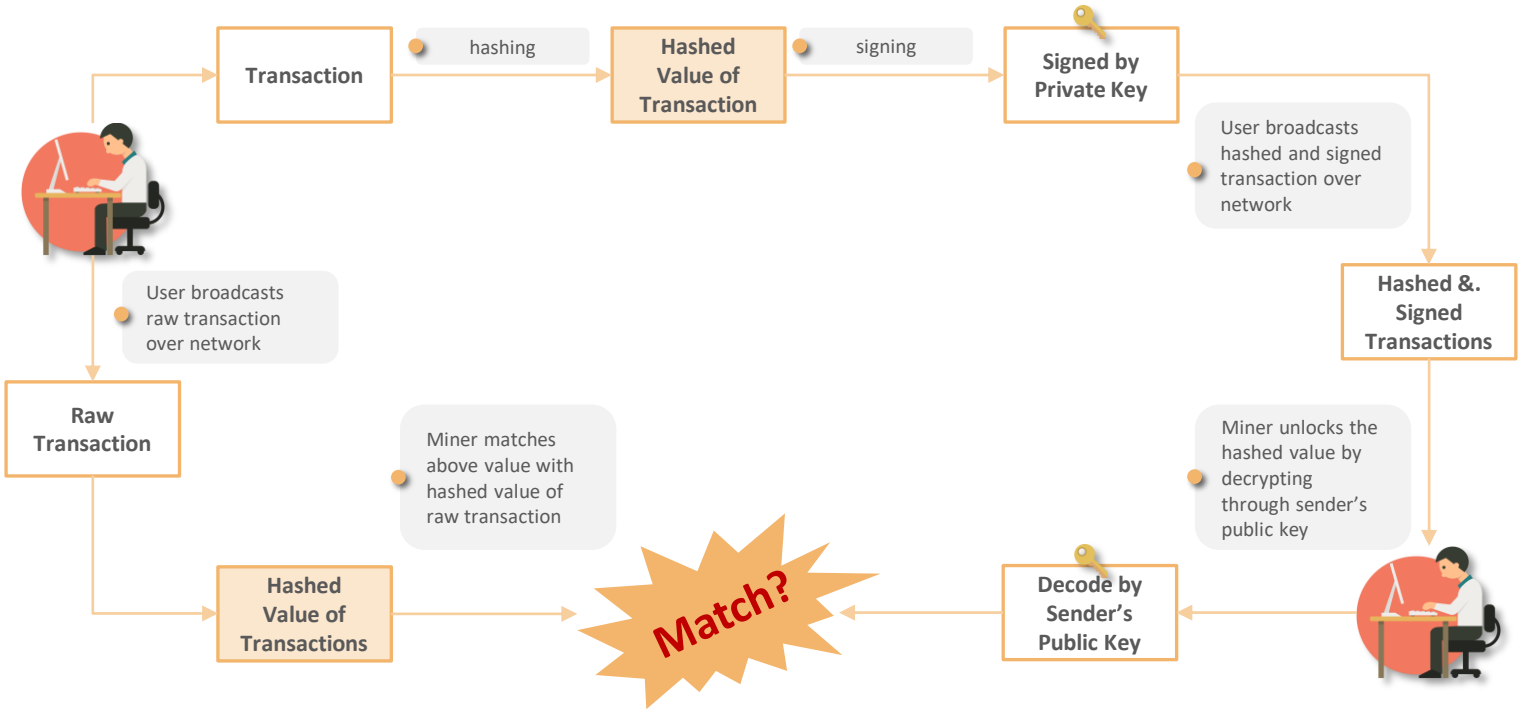


How Bitcoin works

Each full node in the Bitcoin network independently stores a block chain containing only blocks validated by that node. When several nodes all have the same blocks in their block chain, they are considered to be in consensus.

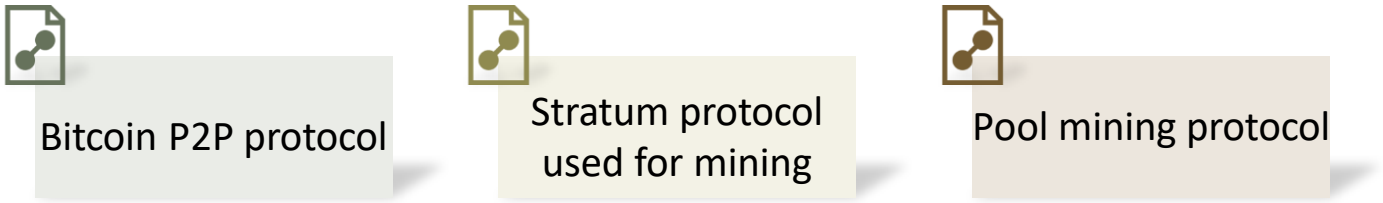
A block of one or more new transactions is collected into the transaction data part of a block. Copies of each transaction are hashed, and the hashes are then paired, hashed, paired again, and hashed again until a single hash remains, the merkle root of a merkle tree for every 10 minutes of transactions. (Bitcoin – 7 transactions per second)

How Bitcoin works



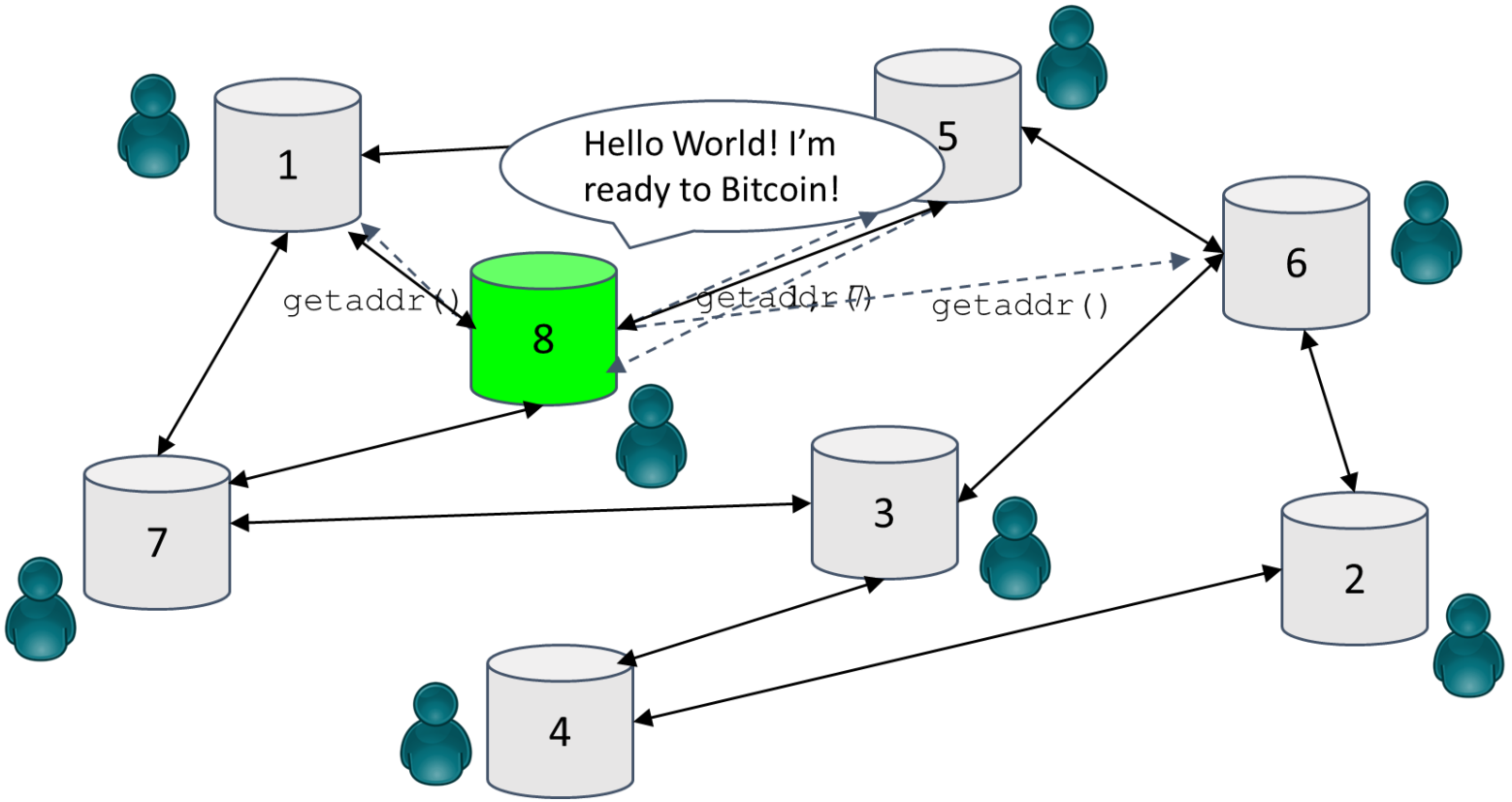
Bitcoin network

The term “bitcoin network” refers to the collection of nodes running the bitcoin P2P protocol including



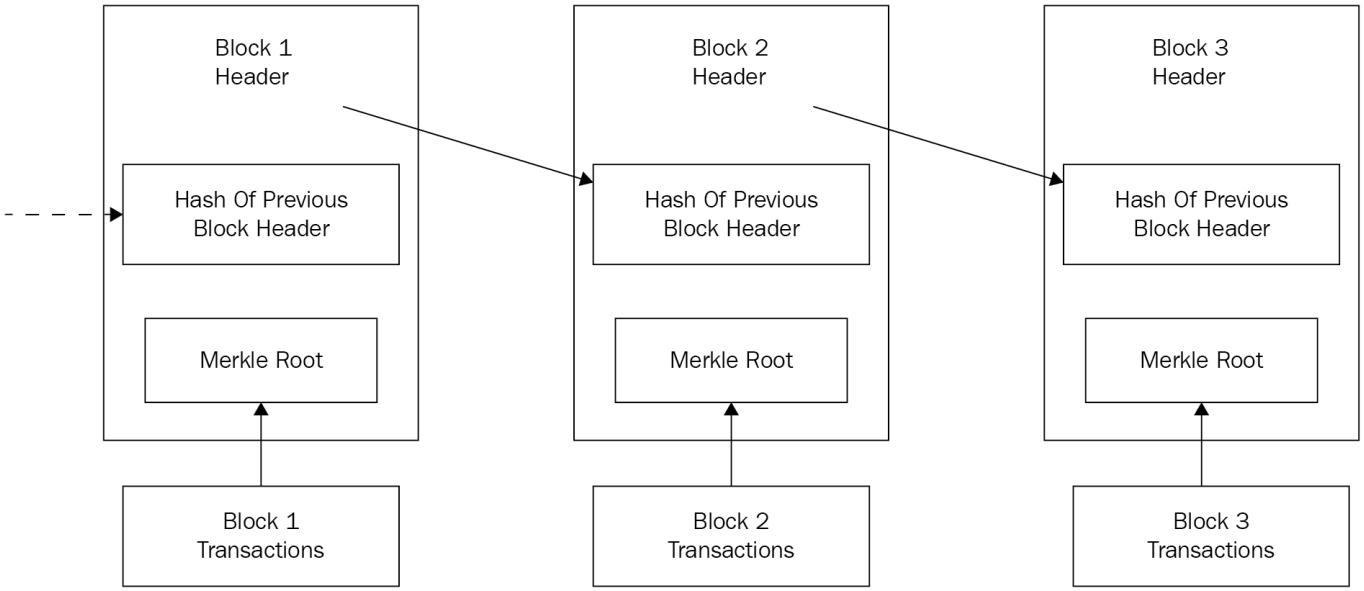
Network discovery process

Joining the Bitcoin P2P network



Transaction process

Transaction and storage in Blockchain



Simplified Bitcoin Block Chain

Transaction process

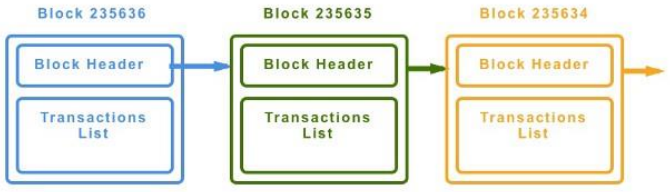
How Transaction is stored?

The Bitcoin Blockchain is a data structure for storing transactions in a series of back-linked blocks.

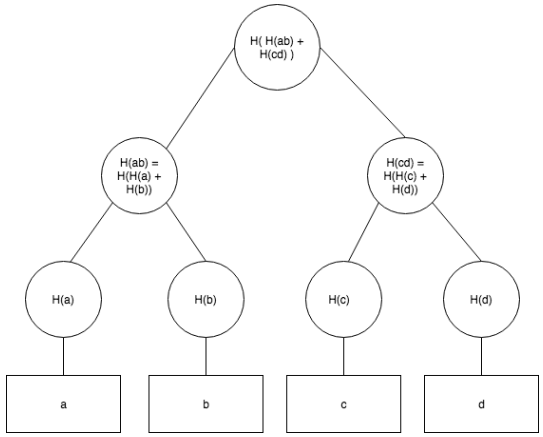
Every block has a list of transactions inside, and each block is linked to its 'parent' block. It can be stored on a file or a simple database.

Main purpose of the chain is to keep the time-sequence of the block

a, b, c, and d can be some data elements (files, public/private keys, JSON, etc)

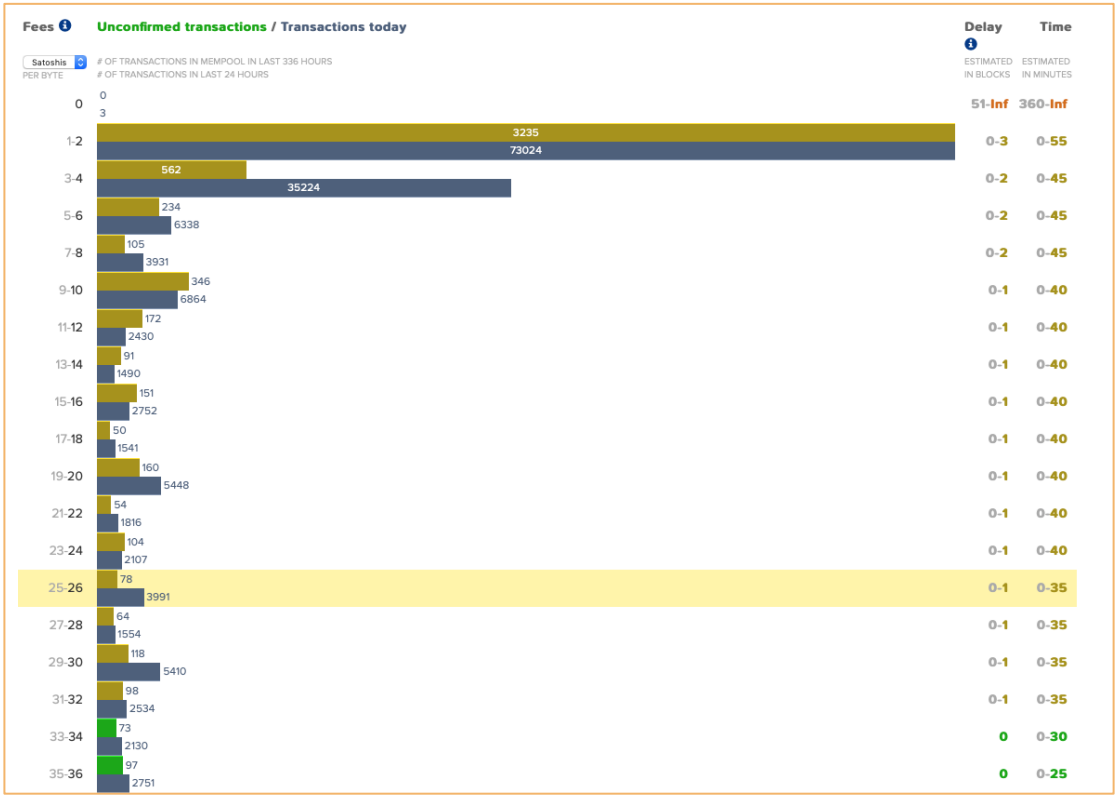


Merkle root



Transaction process

Transaction fee



Fee estimation from https://bitcoinfees.earn.com

Extended Bitcoin network nodes

Reference Client (Bitcoin Core)

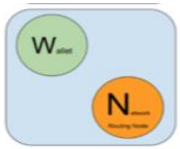
Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.

Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.

Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



Lightweight (SPV) wallet

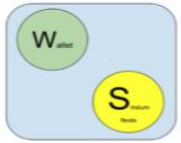
Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.

Mining Nodes

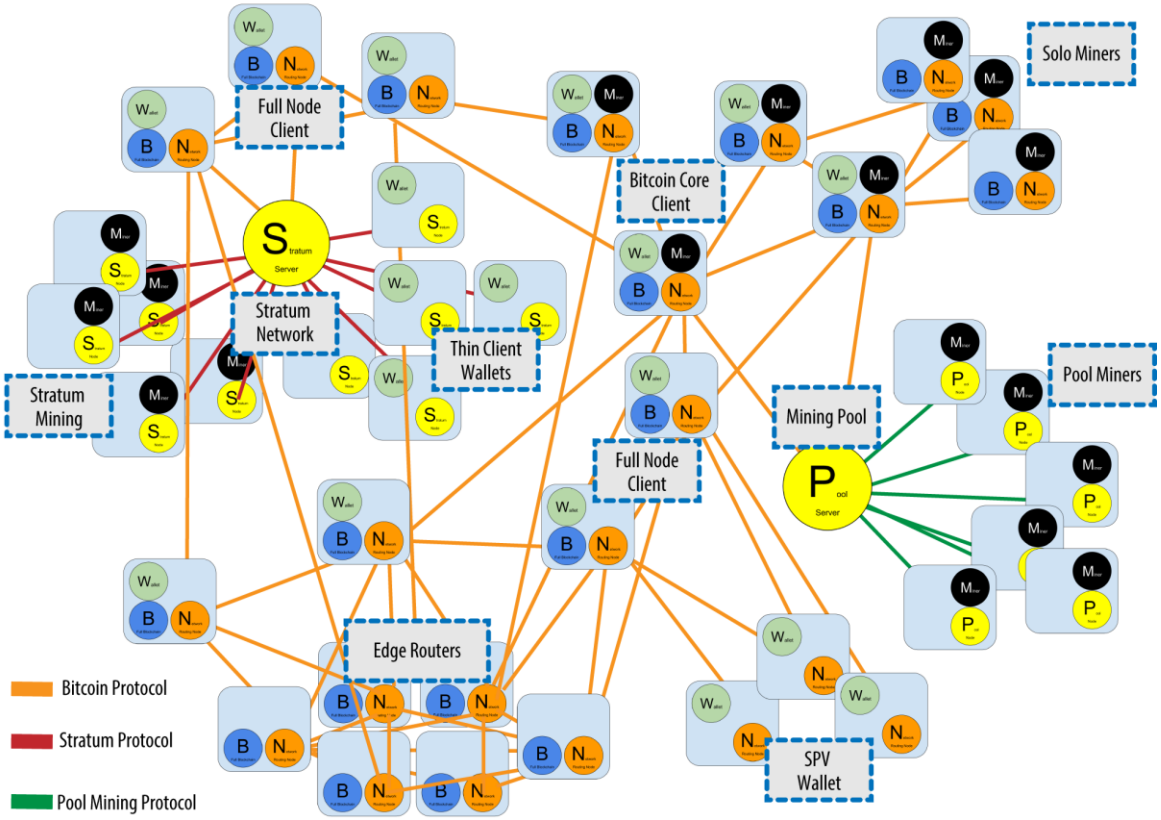
Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.



Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

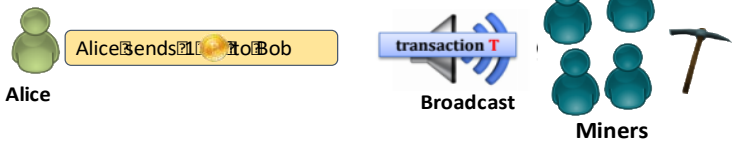
Extended Bitcoin network



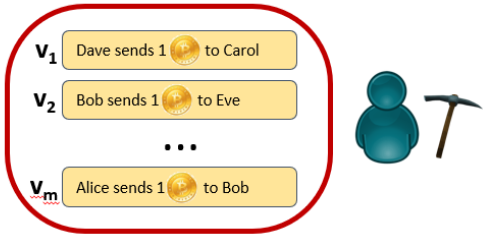
How is a new block added?

Puzzle:
Given "small" y find x such that SHA256(x) < y

1 Payer announces transaction

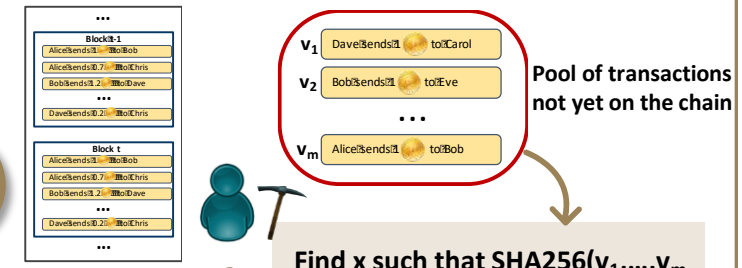


2 Miners receive & check transaction

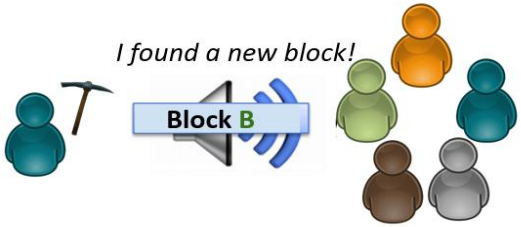


Pool of transactions not yet on the chain

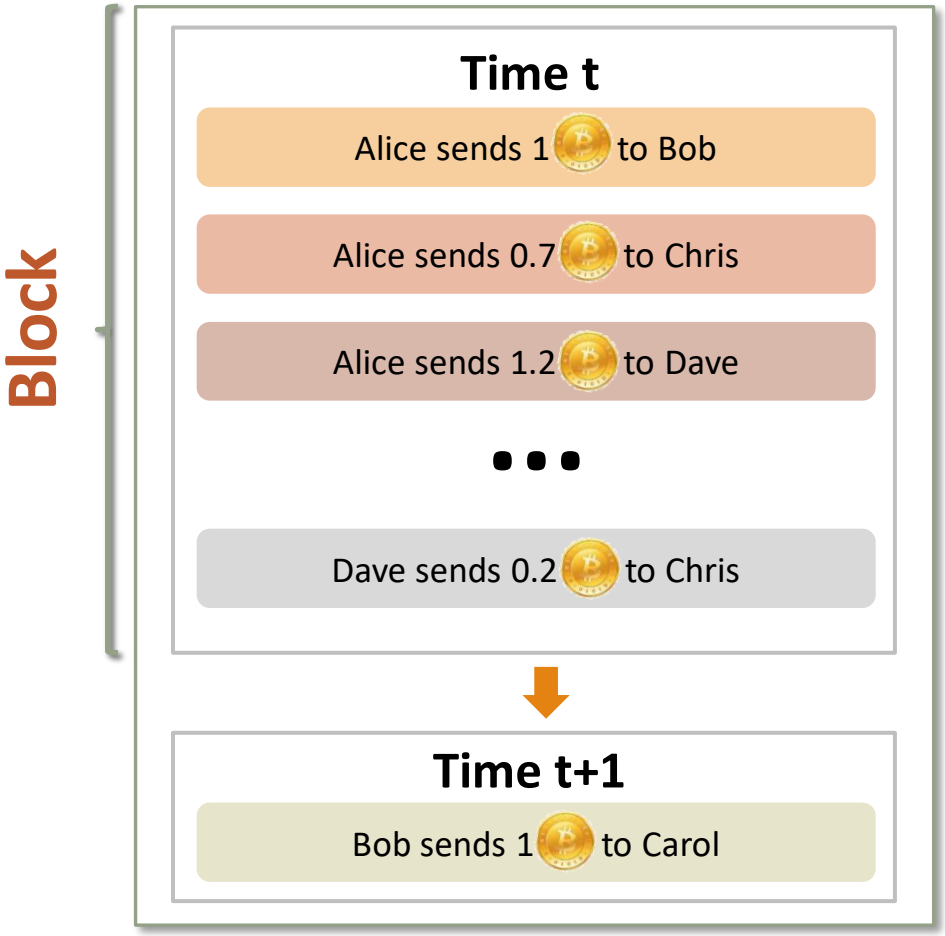
3 Miners "compete" to solve puzzle



4 New block announcement



Where Transaction Ledger will be kept?

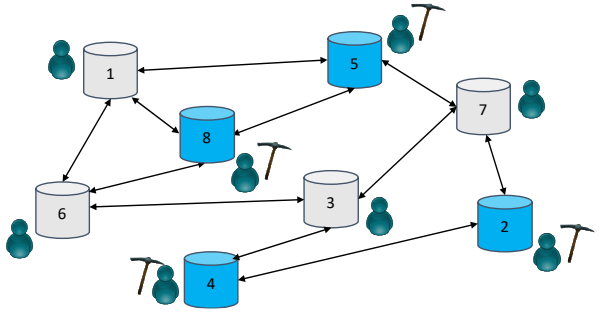


Required properties:

1) Append-only
2) Cannot revise existing blocks
3) Global

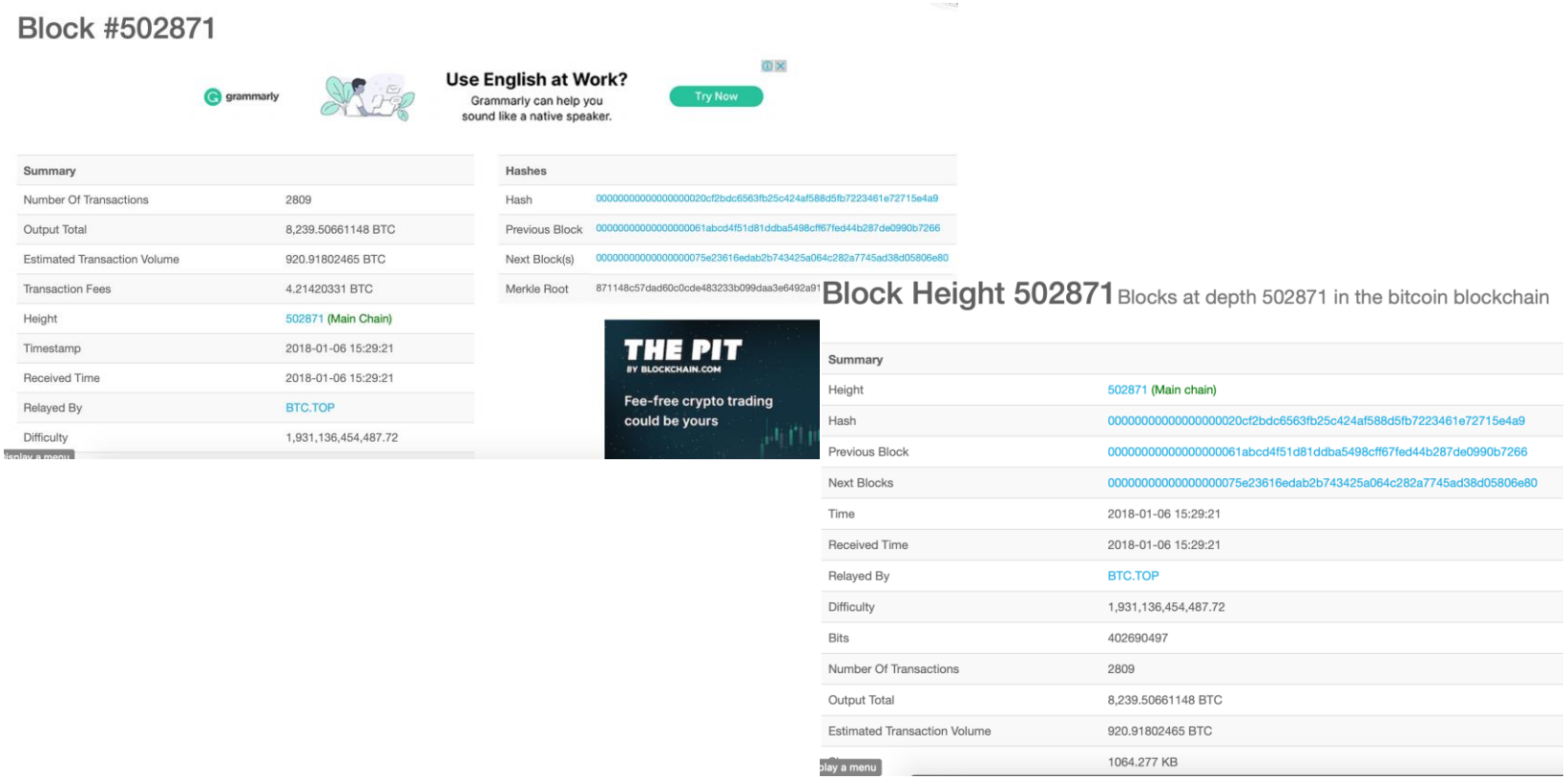
Who maintains it?

The users themselves!



Miners: special types of users

Bitcoin calculations



Block #502871

Summary	
Number Of Transactions	2809
Output Total	8,239.50661148 BTC
Estimated Transaction Volume	920.91802465 BTC
Transaction Fees	4.21420331 BTC
Height	502871 (Main Chain)
Timestamp	2018-01-06 15:29:21
Received Time	2018-01-06 15:29:21
Relayed By	BTC.TOP
Difficulty	1,931,136,454,487.72

Hashes	
Hash	00000000000000000020cf2bdc6563fb25c424af588d5fb7223461e72715e4a9
Previous Block	00000000000000000061abcd4f51d81ddba5498cff67fed44b287de0990b7266
Next Block(s)	00000000000000000075e23616edab2b743425a064c282a7745ad38d05806e80
Merkle Root	871148c57dad60c0cde483233b099daa3e6492a91

Block Height 502871 Blocks at depth 502871 in the bitcoin blockchain

Summary	
Height	502871 (Main chain)
Hash	00000000000000000020cf2bdc6563fb25c424af588d5fb7223461e72715e4a9
Previous Block	00000000000000000061abcd4f51d81ddba5498cff67fed44b287de0990b7266
Next Blocks	00000000000000000075e23616edab2b743425a064c282a7745ad38d05806e80
Time	2018-01-06 15:29:21
Received Time	2018-01-06 15:29:21
Relayed By	BTC.TOP
Difficulty	1,931,136,454,487.72
Bits	402690497
Number Of Transactions	2809
Output Total	8,239.50661148 BTC
Estimated Transaction Volume	920.91802465 BTC
	1064.277 KB

https://www.blockchain.com/btc/block/00000000000000000020cf2bdc6563fb25c424af588d5fb7223461e72715e4a9

Bitcoin calculations

According to https://en.bitcoin.it/wiki/Block_hashing_algorithm

```
versionHex: 20000000
previousblockhash:
00000000000000000061abcd4f51d81ddba5498cff67fed44b287de0990b7266
merkleroot: 871148c57dad60c0cde483233b099daa3e6492a91c13b337a5413a4c4f842978
time: 1515252561
bits: 180091c1
nonce: 45291998
```

version: 02000000

previousblockhash: 66720b99e07d284bd4fe67ff8c49a5db1dd8514fcdab61000000000000000000

merkleroot: 7829844f4c3a41a537b3131ca992643eaa9d093b2383e4cdc060ad7dc5481187

time: (5A50EB51)_16 -> 51eb505a

bits: c1910018

nonce: (02B319DE)_16 -> de19b302

00000020**66720b99e07d284bd4fe67ff8c49a5db1dd8514fcdab61000000000000000000**7829844f4c3a41a537b3131ca992643eaa9d093b2383e4cdc060ad7dc548118**751eb505a**c1910018**de19b302**

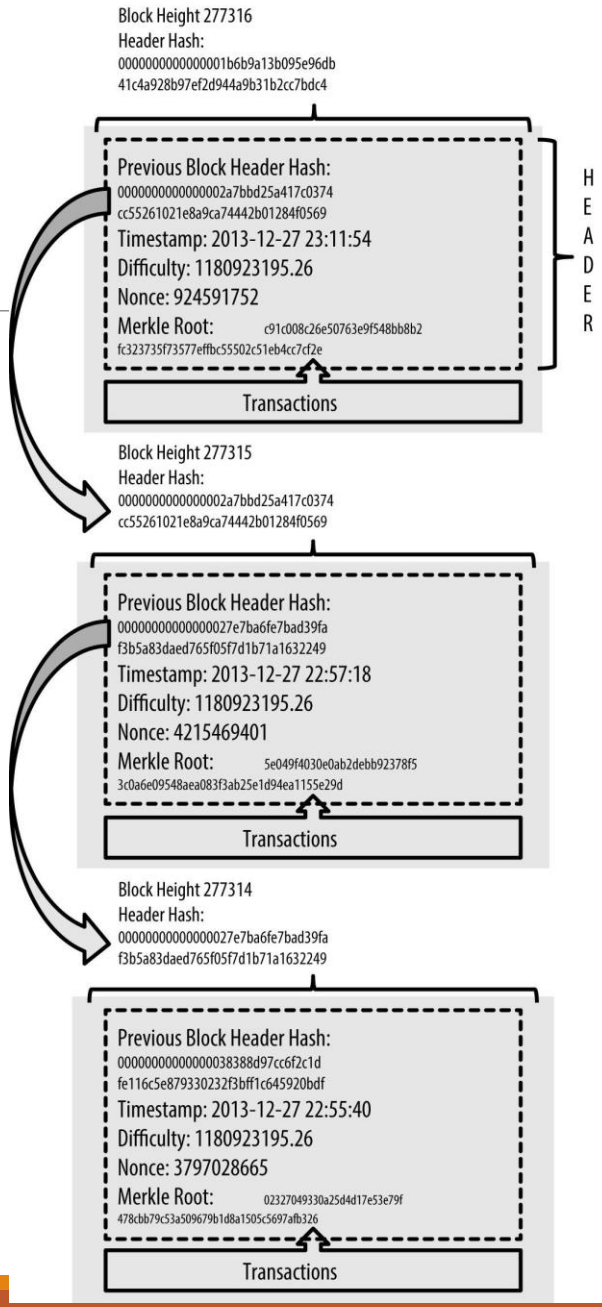
block header

https://www.blockchain.com/btc/block/00000000000000000020cf2bdc6563fb25c424af588d5fb7223461e72715e4a9

Bitcoin calculations

Calculations of

- Pending transactions
- Bundled into a block
- Calculate the Header hash value using:
  - SHA256 (SHA256 (data+ nonce) < difficulty
- Data:
  - Timestamp
  - Merkle Root (Hash of merkle tree of transactions)
- Nonce:
  - The ”mined” random integer performed by the miner
- Difficulty:
  - The value (difficulty) that the hash below the given target

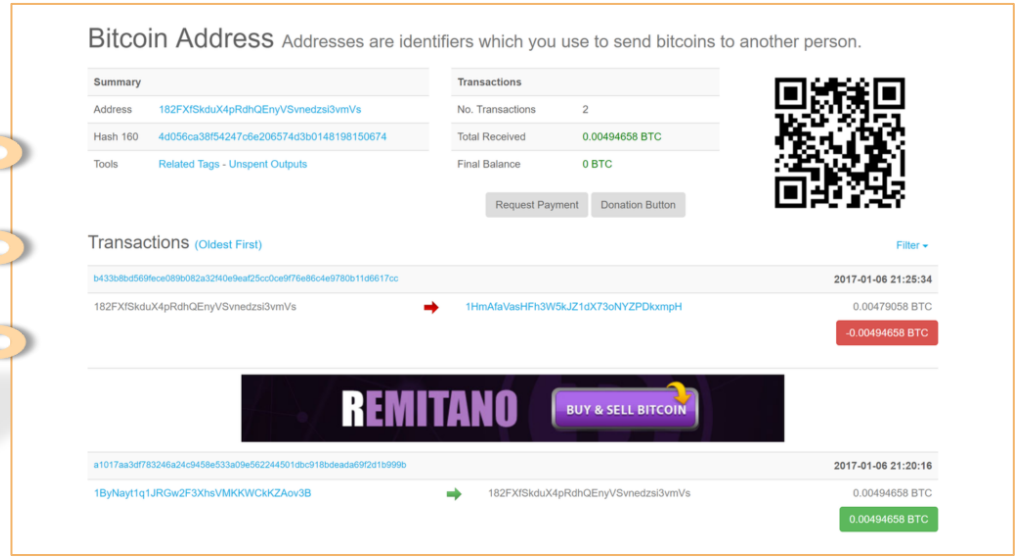


From “Mastering Bitcoin”

How to check bitcoin transaction

Some of the most popular include:

- blockchain.com/explorer
- etherscan.io
- insight.litecore.io
- xrpcharts.ripple.com
- https://explorer.zcha.in/
- blockexplorer.com



https://applicature.com/blog/crypto-enthusiasts/bitcoin-transaction

How to check bitcoin transaction

$ curl https://blockchain.info/unspent?active=1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

- {
  - **"unspent_outputs"**:[
    - {
      - **"tx_hash"**:"186f9f998a5...2836dd734d2804fe65fa35779",
      - **"tx_index"**:104810202,
      - **"tx_output_n"**: 0,
- **"script"**:"76a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac",
    - **"value"**: 10000000,
    - **"value_hex"**: "00989680",
    - **"confirmations"**:0
    - }
  -]
- }

Bitcoin token vs Bitcoin address

Bitcoin tokens don't actually "belong" to addresses. The idea of an address is purely a convenient abstraction.

Bitcoin Address

- Addresses don't truly have a balance (nor does the Bitcoin blockchain even understand that addresses exist), but referring to an address balance is simply a quick way

Bitcoin tokens

- In Bitcoin (and similar UTXO-based blockchains), tokens are "stored" in unspent outputs.
- The sender of a transaction specifies the requirements that must be fulfilled in order for the transaction's outputs to be spent.
- Tokens that are "sent" to an address are actually just stored in an output which requires the spender to prove ownership of their address

Three Fundamental Rules in Bitcoin UTXO

3 fundamental rules in the UTXO scheme

- Every transaction must prove that the sum of its inputs are greater than the sum of its outputs.
- Every referenced input must be valid and not yet spent.
- The transaction must have a signature matching the owner of the input for every input.

When you receive a Bitcoin (or most other tokens), you aren't storing an asset in your wallet. Instead, you're storing a receipt of the transaction where someone sent you a Bitcoin. These receipts are called unspent transaction outputs (UTXOs). It basically says, "someone sent me a Bitcoin and I can prove I haven't spent that Bitcoin yet."

UTXO vs Account-Based Chains

UTXO

- UTXO stands for "Unspent Transaction Output". A UTXO chain is simply a blockchain which uses the UTXO accounting method (such as the Bitcoin and Litecoin blockchains)
- On the protocol layer of UTXO chains, there are no accounts or wallets. Instead, coins are stored as a list of UTXOs.
- A UTXO represents the output of a transaction received by a user, which that user can spend in the future (as it is still "unspent").
- Transactions conducted on a blockchain also require the payment of transaction fees, which are deducted from the amount of change you get in return - unlike when paying in cash.
- UTXOs can come in any amount.

UTXO vs Account-Based Chains

Account-Based Chains

- Account-based chains (such as the Ethereum and EOS blockchains) represent coins as balances within an account.
- Accounts can be controlled by a private key, or by a smart contract and account-based models are mostly popular among smart contract-focused blockchains.
- Account-Based Chain can be treated as similar to bank accounts, which represent user balances within a single account and allow for deposits and withdrawals in and out of that account.

Benefit and Limitation of UTXO

BENEFIT

Allows for Simple Payment Verifications (SPV) on the network. Because it can focus on the UTXO instead of having to download the entire Bitcoin blockchain.

UTXO model creates an environment where parallel processing capacity across multiple addresses is possible, enabling a much better infrastructure for scalability.

Transactions can be processed in parallel since they all refer to independent inputs.

Better for scalability and privacy

LIMITATIONS

Not easy to be implemented in generic smart contract environment unless limit the amount of state of output.

Only suitable for use in applications where each output is only owned by one person.

Use of larger space for storing

Bitcoin Address

The address used for denoting the address for transaction purpose

Most blockchain implementations make use of addresses as the “to” and “from” endpoints in a transaction.

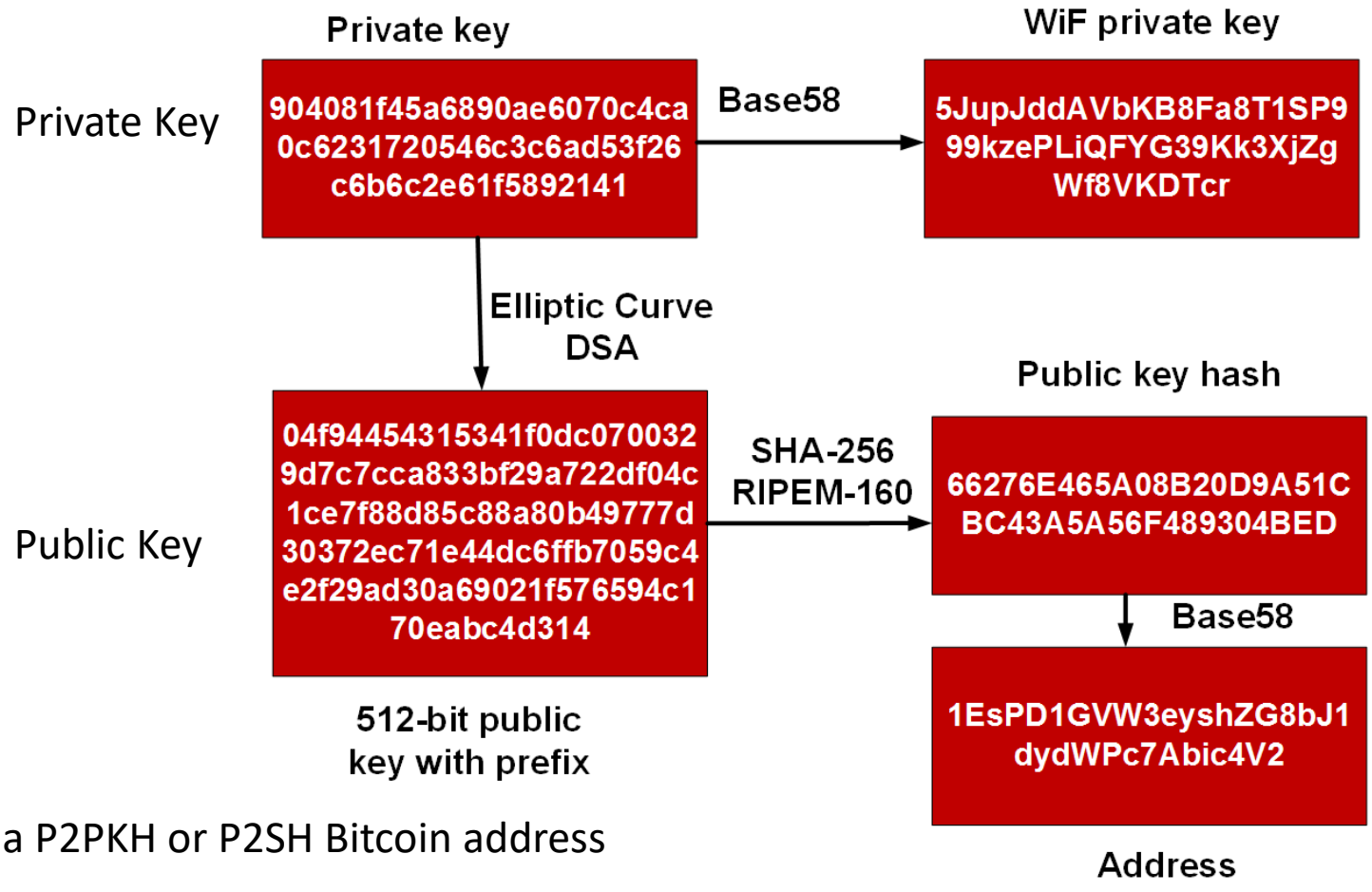
One method to generate an address is to create a public key, applying a cryptographic hash function to it, and converting the hash to text:

- Public Key -> Cryptographic hash function -> address
  - Public keys are generated from the private keys in Bitcoin using elliptic curve (secp256k1)
  - Public keys are then hashed first using sha256 and then hashed using ripemd160
- Addresses may act as the public-facing identifier in a blockchain network for a user, and oftentimes an address will be converted into a QR code

Bitcoin address

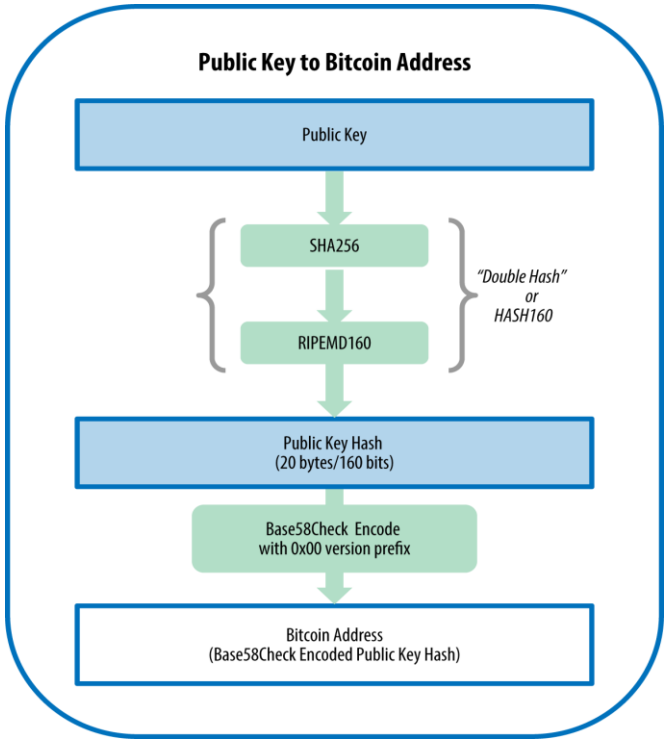
- A 20-byte hash formatted using base58 to produce either a P2PKH or P2SH Bitcoin address.
- P2PKH scripts allow bitcoin to be sent to a Bitcoin address, such that only the owner of the corresponding private key can spend the bitcoin
- Elliptic Curve Digital Signature Algorithm (ECDSA) was used

Bitcoin Address



a P2PKH or P2SH Bitcoin address

Base58



Base64 representation uses 26 lowercase letters, 26 capital letters, 10 numerals, and 2 more characters such as "+" and "/" to transmit binary data over text-based media such as email.

Base58 is a subset of Base64, using upper- and lower- case letters and numbers, but omitting some characters that are frequently mistaken for one another and can appear identical when displayed in certain fonts.

Specifically, Base58 is Base64 without the 0 (number zero), O (capital o), l (lower L), I (capital i), and the symbols "+" and "/".

Bitcoin's Base58 alphabet

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

Encrypted Private Keys (BIP-38)

Keeping the private key private is much harder when you need to store backups of the private key to avoid losing it.

A private key stored in a wallet that is encrypted by a password might be secure, but that wallet needs to be backed up.

Private key backups might also be stored on paper (see “Paper Wallets” on page 88) or on external storage media

Private Key (WIF)	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn
Passphrase	MyTestPassphrase
Encrypted Key (BIP-38)	6PRTHL6mWa48xSopbU1cKrVjpKbBZxcLRRCdctLJ3z5yxE87MobKoXdTsJ

BIP-38 proposes a common standard for encrypting private keys with a passphrase and encoding them with Base58Check so that they can be stored securely on backup media, transported securely between wallets, or kept in any other conditions where the key might be exposed.

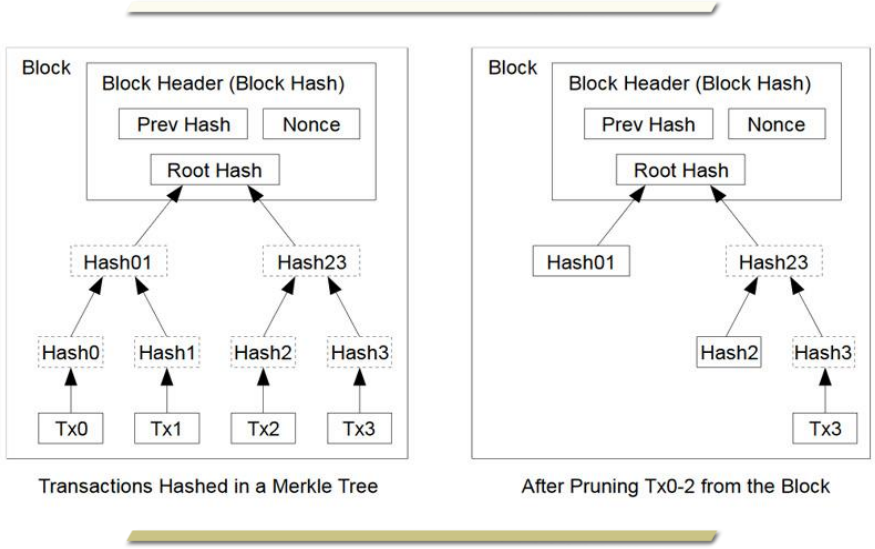
A BIP-38 encryption scheme takes as input a bitcoin private key, usually encoded in the WIF, as a Base58Check string with the prefix of “5.”

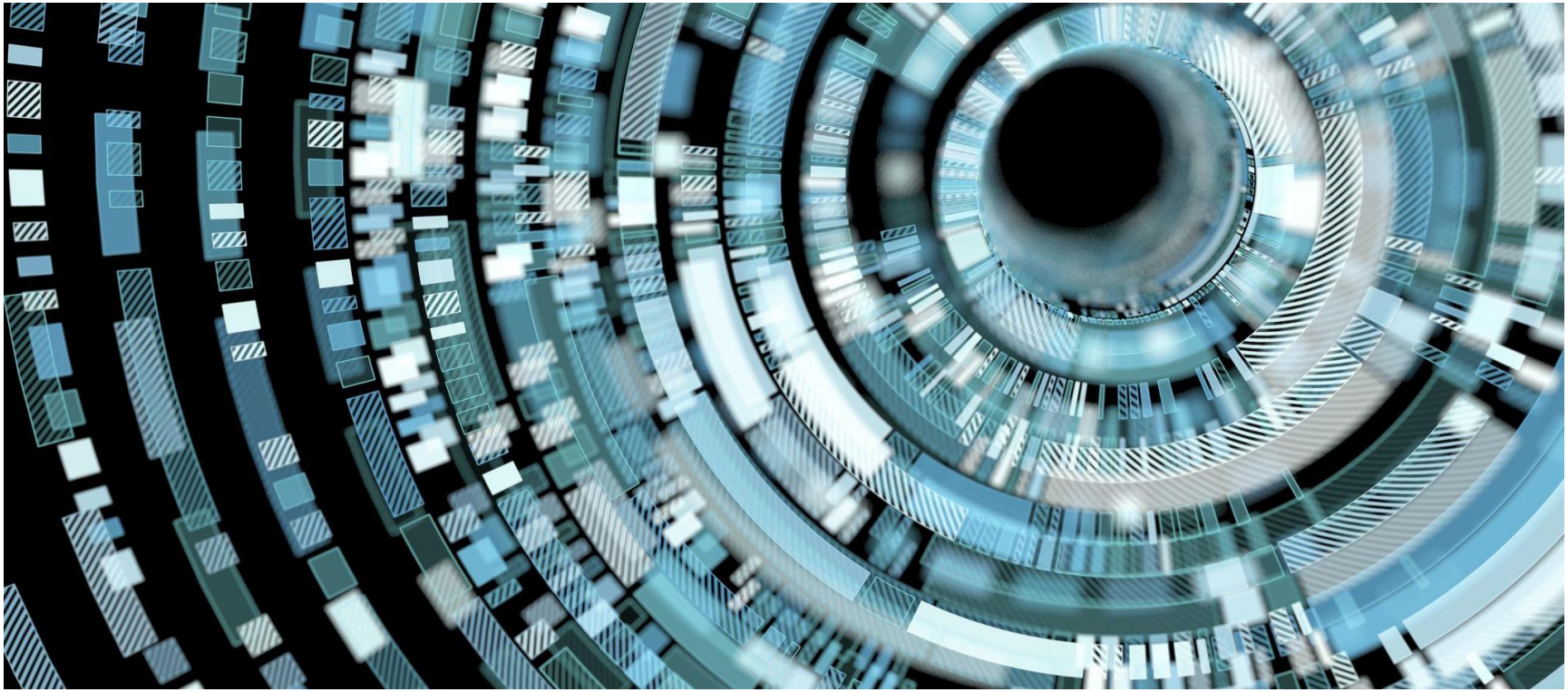
Result of the BIP-38 encryption scheme is a Base58Check-encoded encrypted private key that begins with the prefix 6P. If you see a key that starts with 6P, it is encrypted and requires a

What's within the block header

Within that block as well as the block header which consists of:

- Block Version Number
- Previous Block Hash
- Timestamp
- Mining Difficulty Target
- Nonce
- Merkle Root Hash





Crypto Mining

What is the purpose of Mining?

Crypto mining is the process by which transactions are verified and added to the public ledger, also known as the blockchain, and also the means through which new Bitcoin are released

Miners must compete with other miners to find a correct hash for each hash function

In exchange for solving the puzzle, miners are rewarded with Bitcoin and is otherwise known as a block reward.

Miners must compete with other miners to find a correct hash for each hash function

Bitcoin mining

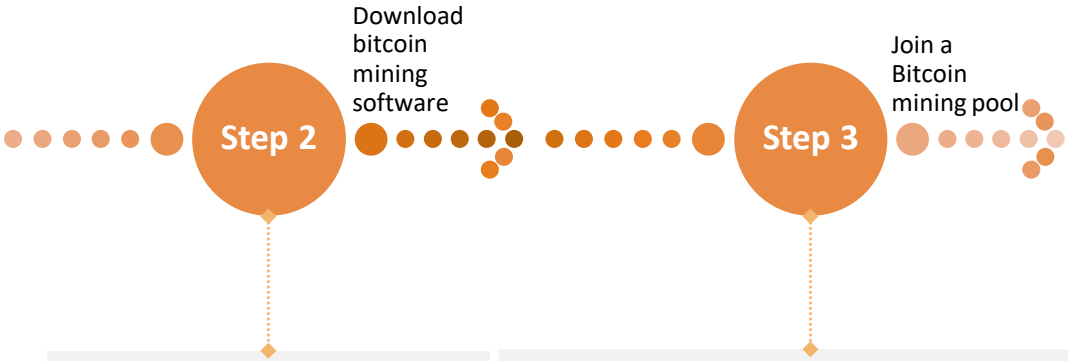
Bitcoin mining is legal and is accomplished by running SHA256 double round hash verification processes in order to validate Bitcoin transactions and provide the requisite security for the public ledger of the Bitcoin network.

The speed at which you mine Bitcoins is measured in hashes per second.

Bitcoin mining services

Bitcoin Mining Hardware

Bitcoin mining



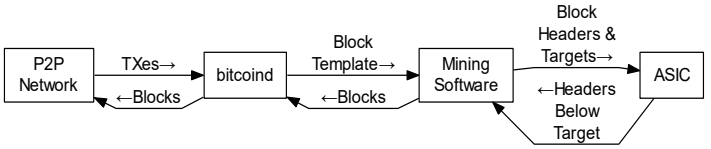
- CGminer, BFGminer
- More can be found in https://www.bitcoinmining.com/bitcoin-mining-software/

- Bitcoin mining pools are groups of Bitcoin miners working together to solve a block and share in its rewards.
- Without a Bitcoin mining pool, sole miner may need over a year and never earn any bitcoins.
- http://p2pool.in

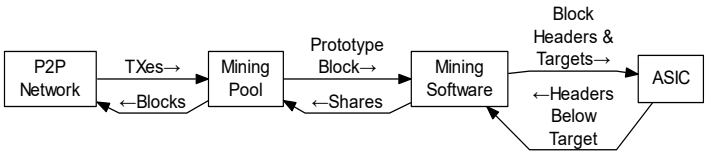
Sole Mining and Pool Mining

Solo mining, where the miner attempts to generate new blocks on his own, with the proceeds from the block reward and transaction fees going entirely to himself, allowing him to receive large payments with a higher variance (longer time between payments)

Pooled mining, where the miner pools resources with other miners to find blocks more often, with the proceeds being shared among the pool miners in rough correlation to the amount of hashing power they each contributed, allowing the miner to receive small payments with a lower variance (shorter time between payments).



Solo Bitcoin Mining Workflow



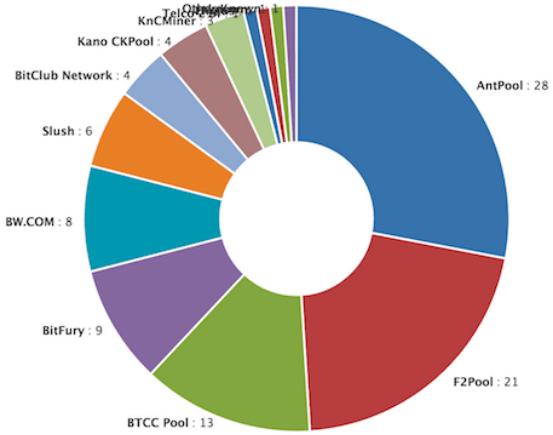
Pool-Based Bitcoin Mining Workflow

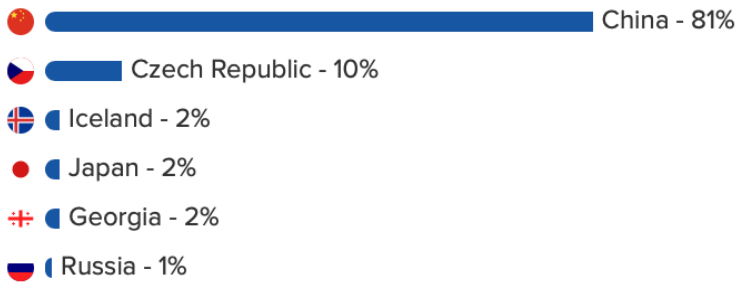
Bitcoin Mining Pools

Bitcoin mining pools are a way for Bitcoin miners to pool their resources together and share their hashing power while splitting the reward equally according to the amount of shares they contributed to solving a block.

Bitcoin Mining Pool

- Antpool
- F2Pool
- BTCC
- Slush Pool
- Eligius
- …





Antpool

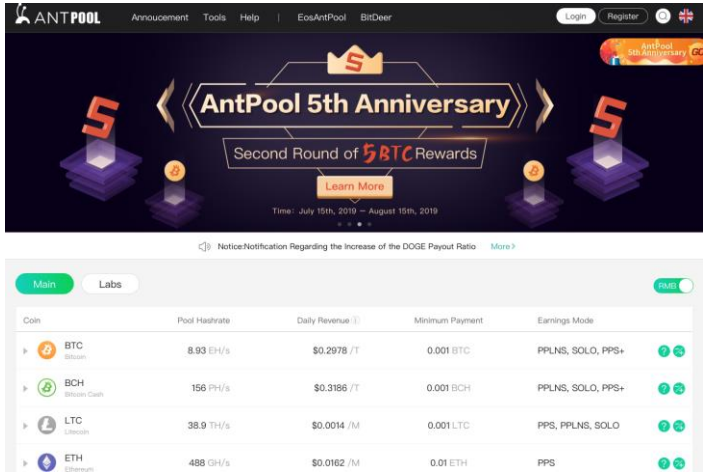
Antpool mined its first block in March 2014, meaning that it emerged roughly four years after the first mining pool; Slushpool.

Antpool is run by Bitmain Technologies Ltd., the world's largest Bitcoin mining hardware manufacturer, and a large portion of their pool is run on Bitmain's own mining rigs.

Antpool supports p2pool and stratum mining modes with nodes that are spread all over the world to ensure stability (US, Germany, China etc.).

Currently, every Bitcoin block has a 12.5 BTC reward which Antpool does share with you when it finds a block.

Lately, however, Bitcoin transaction fees have been rising and an additional 1-2 bitcoins are collected per block by pools.

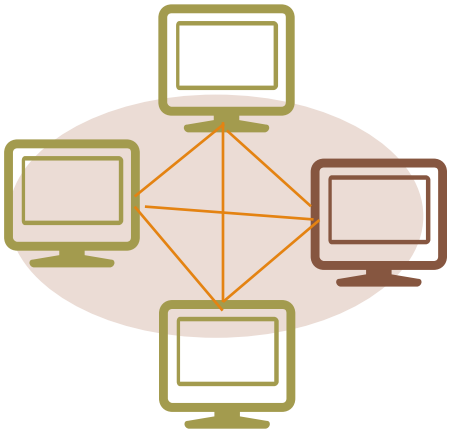


Miners – Mining Node

In Bitcoin network, data is shared among nodes.

When a new node added and connected to the Bitcoin network, it would download the transactions.

Now, the whole block of transaction is about 128G in size.

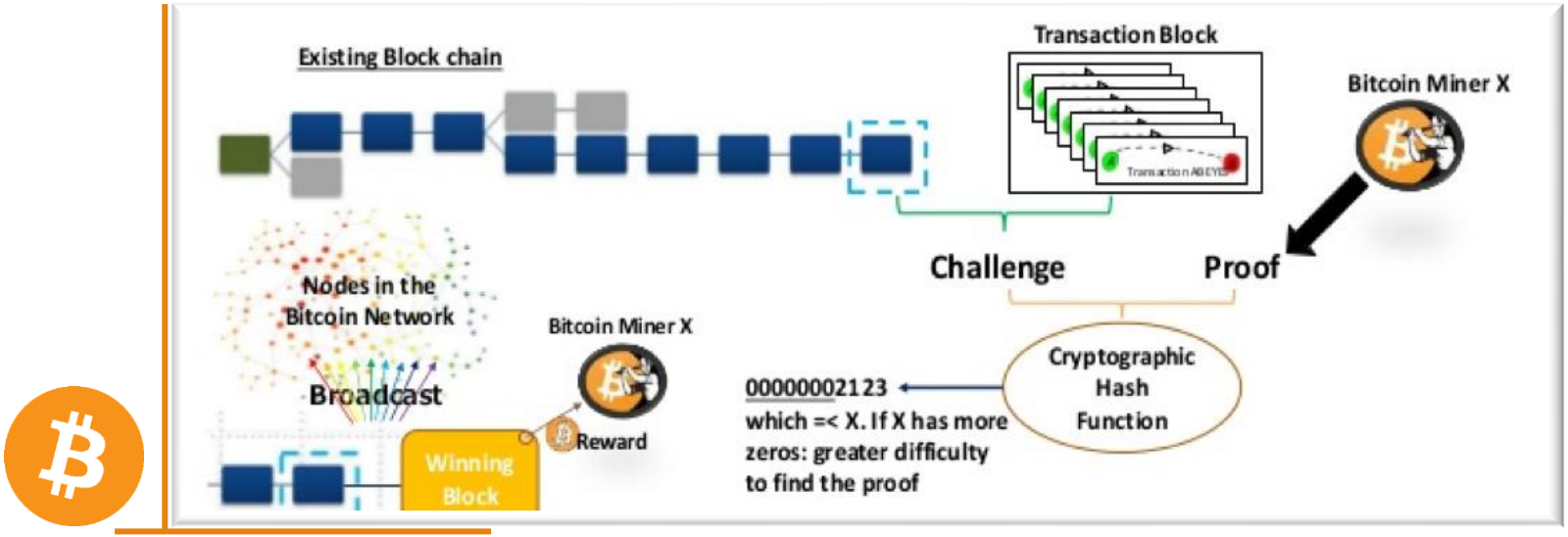


Some nodes are mining nodes and they perform the following:

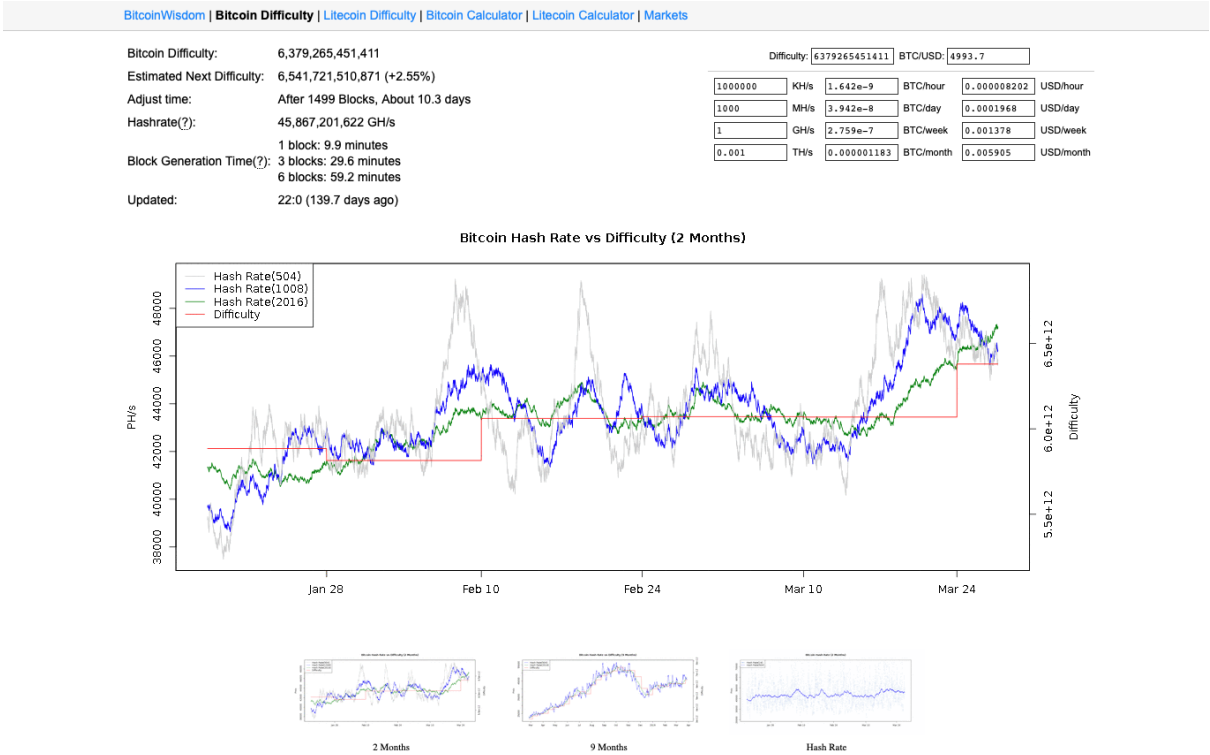
1. Group the outstanding txn into block
2. Solving a complex math puzzle as part of the bitcoin program.
3. The miner who solve the problem first, include the answer into the block and announce to the network.
4. The winner will be rewarded with new bitcoin.

https://charts.bitcoin.com/bch/chart/blockchain-size

What is the math puzzle?



How complex is the puzzle?



https://bitcoinwisdom.com/bitcoin/difficulty

Mining in Bitcoin

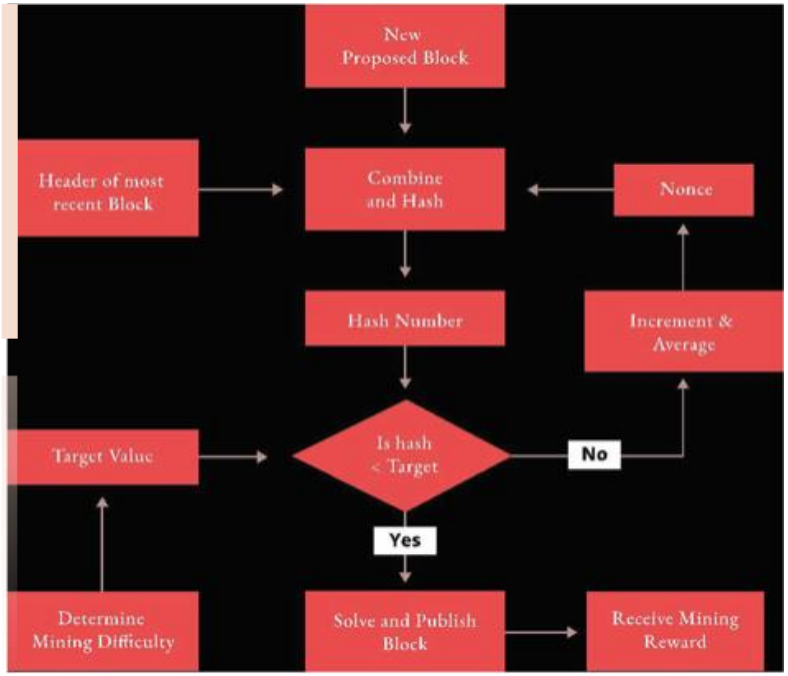
Any small change in the string will have a substantial change in the value of the Hash.

The Hash value starts with a particular format starting with four zeros "0000," which is very uncommon and more difficult to arrive at."

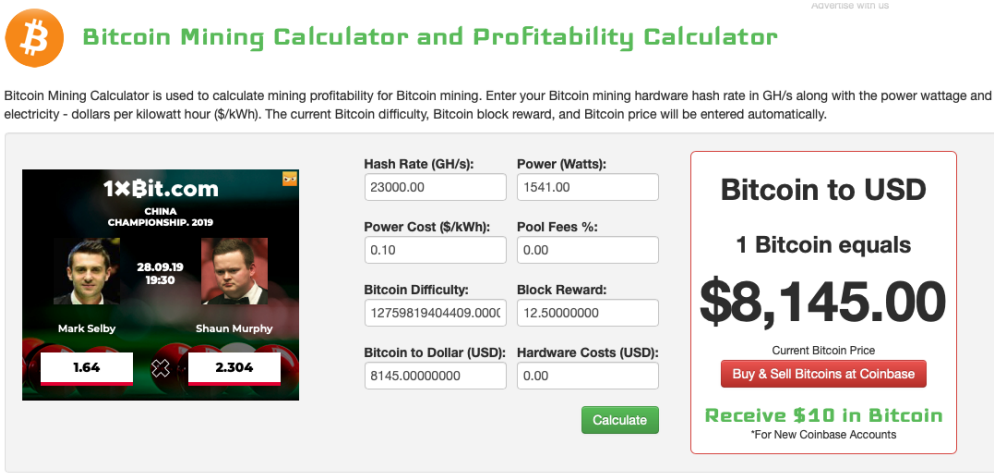
Miners have to determine the value of the random number called the Nonce which when combined with the transaction data will result in the hash that has the patter on four leading zeros.

When this hash is produced the block is considered signed. When a miner successfully signs the block before any other miner does, he or she receives the block reward and the block is added to the blockchain.

Excerpt From: Sarah Swammy. "Crypto Uncovered". Apple Books.



Bitcoin Mining Earning



Time Frame	BTC Coins	USD	Power Cost (in USD)	Pool Fees (in USD)	Profit (in USD)
Hourly	0.00001889	$0.15	$0.15	$0.00	$0.00
Daily	0.00045326	$3.69	$3.70	$0.00	($0.01)
Weekly	0.00317282	$25.84	$25.89	$0.00	($0.05)
Monthly	0.01359779	$110.75	$110.95	$0.00	($0.20)
Annually	0.16543983	$1,347.51	$1,349.92	$0.00	($2.41)

Proof of Work and Mining

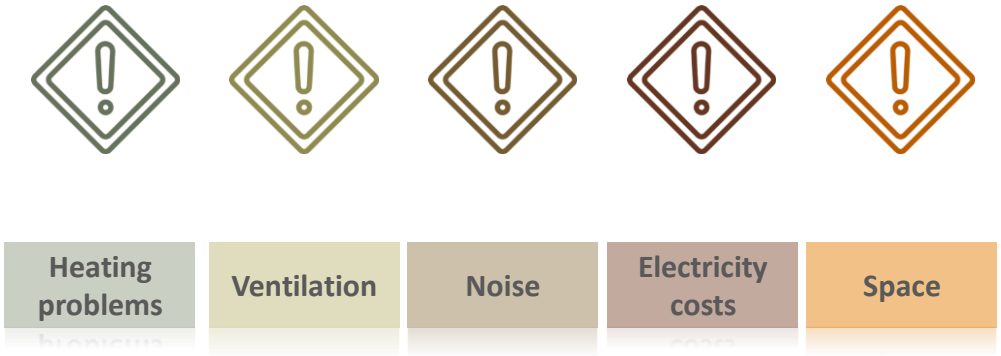
Finding such a solution, in blockchain terms “Proof of Work,” requires millions of hashing operations per second, across the entire Bitcoin network.

The algorithm for Proof of Work involves hashing the header of the block and a random number with the SHA256 cryptographic algorithm, until a solution matching a predetermined pattern emerges.

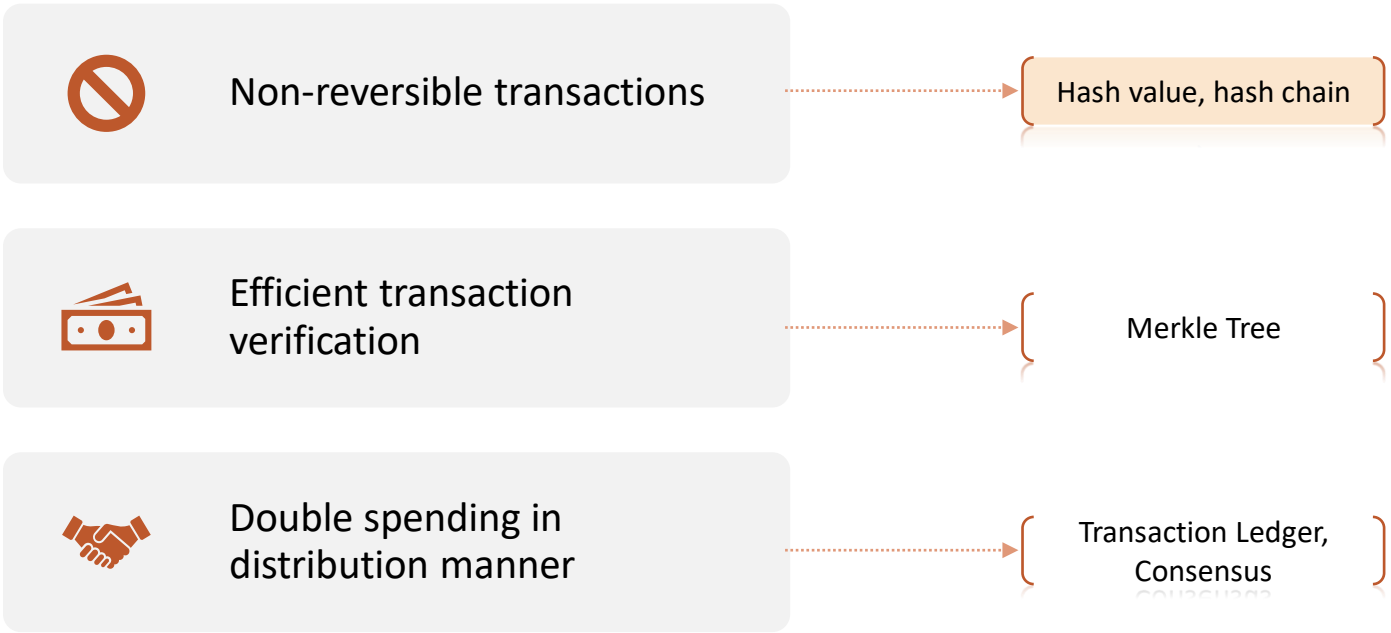
The first miner who finds such a solution wins the round of competition and publishes that block into the blockchain.

Every ten minutes, miners produce a new block, which comprises all the transactions since the last block.”

Issues of Mining



Problems and Solutions



What is Merkle Tree

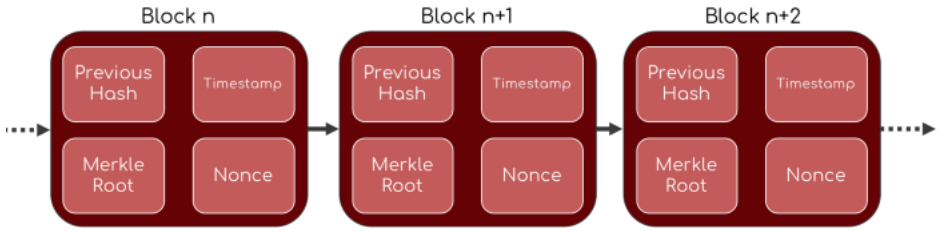
In 1979, Ralph Merkle described an efficient method of creating proofs via Merkle Trees which was described in his paper “A Certified Digital Signature”, https://www.researchgate.net/profile/Ralph_Merkle/publication/221355342_A_Certified_Digital_Signature/links/0f31753a3305a7c9f5000000/A-Certified-Digital-Signature.pdf

A Merkle tree, or binary hash tree, involves taking large amounts data and making it more manageable to process.

Merkle trees are structures used to validate large amounts of data in an efficient manner.

They are able to not only verify that the data received from other peers in a peer-to-peer network like Bitcoin or Ethereum are unaltered but also that the blocks being sent are legitimate.

Merkle roots, however, can be understood as the signature of all the transactions included within a single block



What is Merkle Tree

In the case of blockchain technology, merkle trees are used to organize regular transactions such as: “Alice sent Bob 5 Bitcoins”, in a way that utilizes fewer resources.

Each transaction on a blockchain has its own unique transaction ID. With most blockchains, each transaction ID is a 64-character code that takes up 256 bits (32 bytes) of memory.

Merkle Trees take a huge number of transaction IDs and put them through a mathematical process that results in a single, 64-character code.

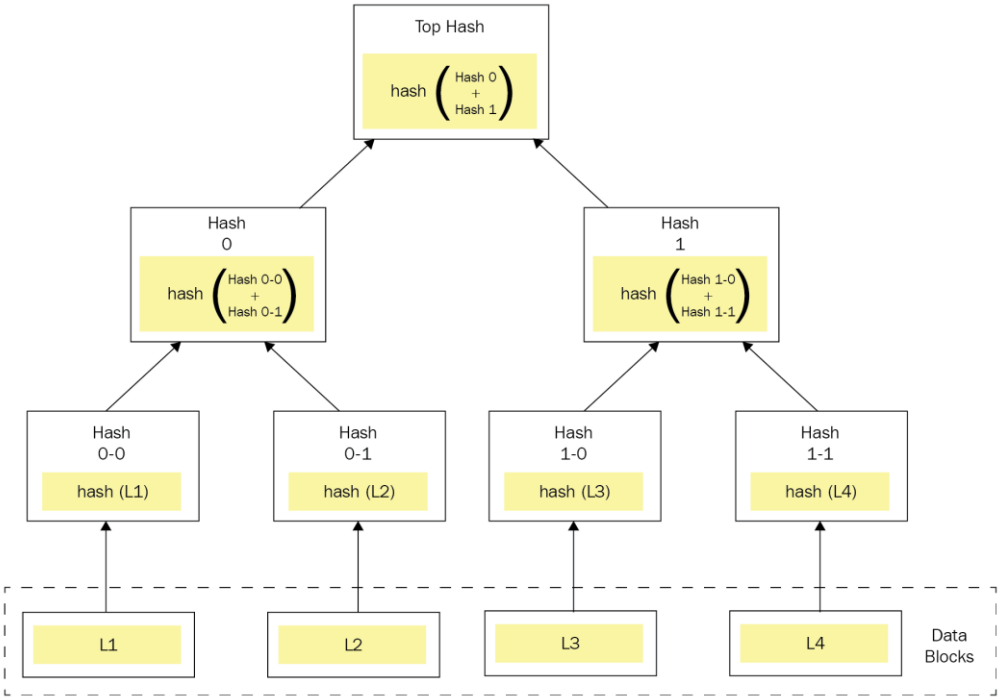
Merkle Root is a crucial piece of data because it allows computers to verify information with incredible speed and efficiency.

If there is an odd number of inputs, the last input is copied and then paired with itself. This holds true for all the transaction IDs written onto a block of a blockchain.

For instance, a single block contains a total of 512 transactions. The Merkle Tree would begin by grouping those 512 transactions IDs into 256 pairs.

https://www.youtube.com/watch?v=fB41w3JcR7U

What is Merkle Tree



From Hands-on Cybersecurity with Blockchain

What is Merkle Proofs

Allow us to compress large data sets by removing all superfluous branches while keeping only the ones we need to establish our proof.

Merkle proofs are used to decide upon the following factors:

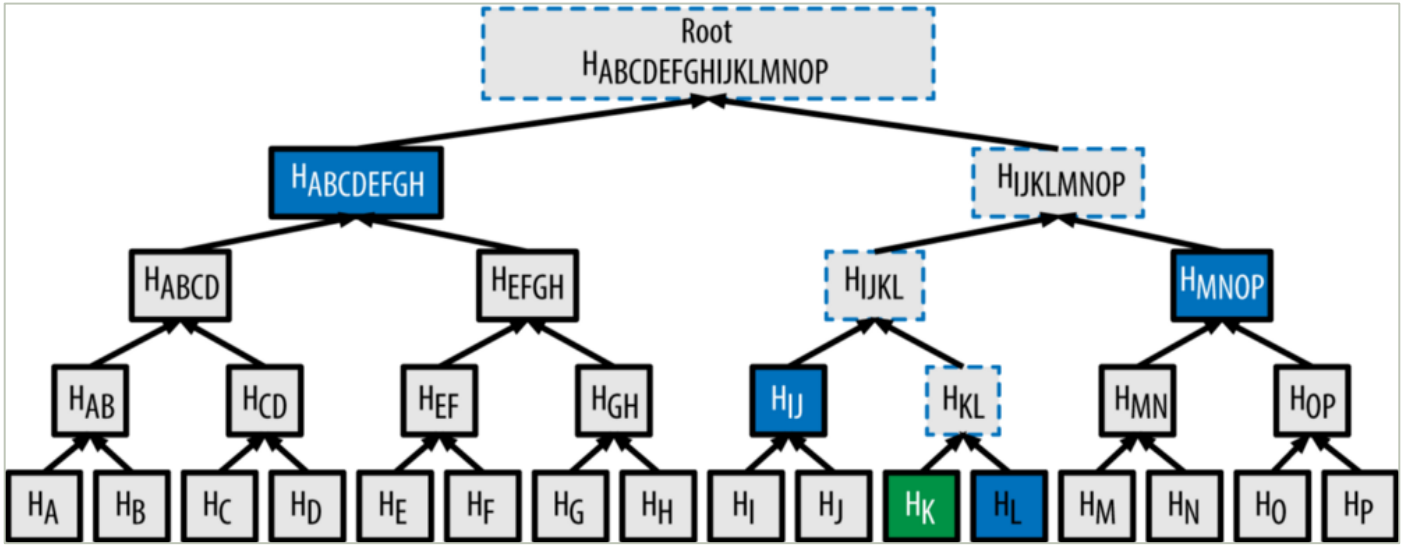
- If the data belongs in the merkle tree
- To concisely prove the validity of data being part of a dataset without storing the whole data set
- To ensure the validity of a certain data set being inclusive in a larger data set without revealing either the complete data set or its subset.

Function of Merkle proofs

- Ability to verify whether a transaction is included in a block
- Light-clients (since we don't have to download the entire chain)
- Overall performance and scalability
- Simplified Payment Verification or (SPV)
- Will be used for proofing a transaction is within the transaction list within a block

The Benefits Of Merkle Trees

Can verify the transaction code through the use of hash in smaller number of operations



In order to obtain a merkle proof of H, we need H(L), H(IJ), H(MNOP) and H(ABCDEFGH) with which we can together obtain H(ABCDEFHGIJKLMNOP) hence proving that H(K) was part of the merkle tree

Benefits of Merkle Tree

1. They provide a means to prove the integrity and validity of data

2. They require little memory or disk space as the proofs are computationally easy and fast (Compress)

3. Their proofs and management only require tiny amounts of information to be transmitted across networks

4. Supports the use of Simplified Payment Verification (SPV) – a way of verifying transactions in a block without downloading an entire block.

Beyond Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Paper

"Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."

By Apr 2018, Bitcoin's (BTC) blockchain hit a unique milestone in April as the 17 millionth BTC was mined.

Bitcoin's blockchain protocol makes mining more difficult as more miners join the pool, and the Bitcoin reward for mining a block also halves every 210,000 blocks.

Miners receive a 12.5 BTC reward for unlocking a new block. The next reward halving will happen in May 2020 - reducing the reward to 6.25 coins.

Assuming that there are no changes to the protocol, the Bitcoin cap will be reached by 2140

When the day comes that the 21 million BTC cap is hit (by 2140), there will be no more BTC rewards for miners. Miners will only benefit from transaction fees.

Transactions can still be validated and stored on blocks in the blockchain

Beyond Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Paper

In 2010, Nakamoto implemented a 1MB size limit for blocks in order to stop miners producing bigger blocks that were likely to be rejected by the network - which could have caused the blockchain to split.

SegWit's implementation also laid the foundation for second layer solutions to further improve Bitcoin's network.

The most anticipated is the Lightning Network, which will essentially do what SegWit has done but on a grander scale.

If the Lightning Network is full integrated by this time, there could be far less transactions being recorded on a daily basis. This could potentially affect the amount of money miners will be making from transactions.

One of the reasons was the need to keep the number of Satoshis within the limits of 64-bit double floating numbers with a small margin for multiplication/division rounding. 64 bit floating gives 52 bits of explicit storage. Interestingly 2^{51} = 2,251,799,813,685,248 units. This is just enough to store 21 million coins times 108 divisions.

Beyond Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" Paper

The overall supply of a coin can be broken down into 3 main parts: Circulating Supply, Total Supply, & Maximum Supply.

As it is not entirely so important how many Bitcoins will exactly be mined. Satoshi could have easily chosen almost any number. He could just adjust block reward halving (210 000 blocks), reward sizes (50, 25, 12.5 …) etc. to match some particular number.

Nakamoto's protocol also requires that the mining reward is halved every 210,000 blocks or approximately four years.

Once miners have unlocked 21 million of Bitcoins, the planet's supply will essentially be tapped out, unless Bitcoin's protocol is changed to allow for a larger supply.

Relationship of Bitcoin and Satoshi

The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto.

Satoshi left the project in late 2010 without revealing much about himself.

Satoshi's influence was limited to the changes he made being adopted by others and therefore he did not control Bitcoin.

The community has since grown exponentially with many developers working on Bitcoin

The Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software

Bitcoin can only work correctly with a complete consensus among all users.

Miscellaneous of Bitcoin

Blockchain Terminology

Multisignature (multisig)

- Requiring more than one key to authorize a bitcoin transaction

Opcode

- Operation codes from the Bitcoin Script language which push data or perform functions within a pubkey script or signature script. Bitcoin uses a scripting system for transactions. Forth-like, Script is simple, stack-based, and processed from left to right. It is intentionally not Turing-complete, with no loops.

OP_RETURN

- An opcode used in one of the outputs in an OP_RETURN transaction.

OP_RETURN transaction

- A transaction type relayed and mined by default in Bitcoin Core 0.9.0 and later that adds arbitrary data to a provably unspendable pubkey script that full nodes don't have to store in their UTXO database.

Blockchain Terminology

P2PKH (Oldest Bitcoin address format)

- Transactions that pay a bitcoin address contain P2PKH or Pay To PubKey Hash scripts. An output locked by a P2PKH script can be unlocked (spent) by presenting a public key and a digital signature created by the corresponding private key. (starts with 1 – 26, 36 characters). E.g. 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

P2SH (Bitcoin address)

- P2SH or Pay-to-Script-Hash is a powerful new type of transaction that greatly simplifies the use of complex transaction scripts. With P2SH the complex script that details the conditions for spending the output (redeem script) is not presented in the locking script. Instead, only a hash of it is in the locking script. (starts with 3 instead of 1). E.g. 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

P2SH address

- P2SH addresses are Base58Check encodings of the 20-byte hash of a script, P2SH addresses use the version prefix “5”, which results in Base58Check-encoded addresses that start with a “3”. P2SH addresses hide all of the complexity, so that the person making a payment does not see the script.

Bech32 (Newest Bitcoin address)

- Bech32 aka “native segwit” is the newest Bitcoin address format. Addresses of this type start with “bc1” and are longer in length than P2PKH and P2SH addresses. (https://segwitaddress.org/). E.g. bc1q42lja79elem0anu8q8s3h2n687re9jax556pcc

P2WPKH

- The signature of a P2WPKH (Pay-to-Witness-Public-Key-Hash) contains the same information as a P2PKH spending, but is located in the witness field instead of the scriptSig field. The scriptPubKey is also modified.

P2WSH

- The difference between P2SH and P2WSH (Pay-to-Witness-Script-Hash) is about the cryptographic proof location change from the scriptSig field to the wit- ness field and the scriptPubKey that is also modified.

Blockchain Terminology

satoshi

- A satoshi is the smallest denomination of bitcoin that can be recorded on the blockchain. It is the equivalent of 0.00000001 bitcoin and is named after the creator of Bitcoin, Satoshi Nakamoto.

Bitcoin script

- the name of the Bitcoin protocol scripting system that processes and validates transactions.
- Script is a clever, stack-based instruction engine, and it makes all transactions from simple payments to overseen/complex oracle contracts possible.

ScriptPubKey (aka pubkey script)

- ScriptPubKey or pubkey script, is a script included in outputs which sets the conditions that must be fulfilled for those satoshis to be spent. Data for fulfilling the conditions can be provided in a signature script.

ScriptSig (aka signature script)

- ScriptSig or signature script, is the data generated by a spender which is almost always used as variables to satisfy a pubkey script.

Wallet Import Format (WIF)

- WIF or Wallet Import Format is a data interchange format designed to allow exporting and importing a single private key with a flag indicating whether or not it uses a compressed public key.

Bitcoin variations

Variations	Characteristics
Bitcoin Segregated Witness (SegWit)	Among these are increased block size and transaction malleability protection. The current block size limit of 1 Megabyte will be increased with Segregated Witness. The proposal introduces the SegWit concept and a new structure called “witness” for storing signatures and relevant scripts
Bitcoin Unlimited	Bitcoin Unlimited makes a small change to the consensus in the Bitcoin core, so that the consensus no longer enforces a hardcoded block size limit. The maximum size of a block is freely adjustable by miners, who then engage in Emergent Consensus (EC) to set the maximum block size.
Bitcoin Cash	Bitcoin Cash (BCC) takes another approach and provides an immediate increase of the block size limit to 8 Megabytes. Bitcoin Cash also introduces other changes such as Replay Protection and Wipeout Protection

Bitcoin UTXO is Token?

In Bitcoin transaction, transaction record and unspent transaction will be kept.

Storing a receipt of the transaction where someone sent you a Bitcoin. These receipts are called unspent transaction outputs (UTXOs).

Every Bitcoin only exists as a chain of receipts leading back to the valid block where that Bitcoin was originally mined and awarded as part of the block reward

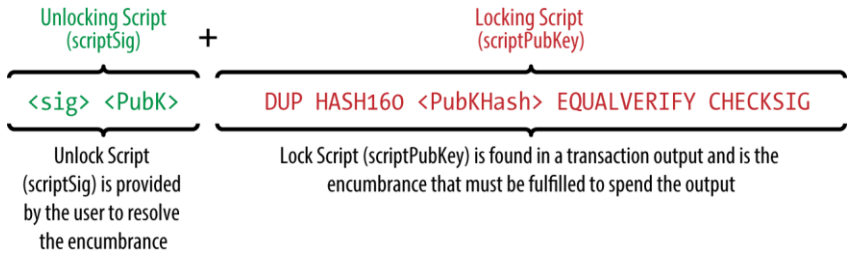
Bitcoin transaction script language

The bitcoin transaction script language, called Script, is a Forth-like reverse-polish notation stack-based execution language.

Script is a very simple language that was designed to be limited in scope and executable on a range of hardware, perhaps as simple as an embedded device.

A script will predictably execute the same way on any system. If your system verifies a script, you can be sure that every other system in the bitcoin network will also verify the script, meaning that a valid transaction is valid for everyone and everyone knows this.

Example of the unlocking and locking scripts



Bitcoin's script validation doing simple math