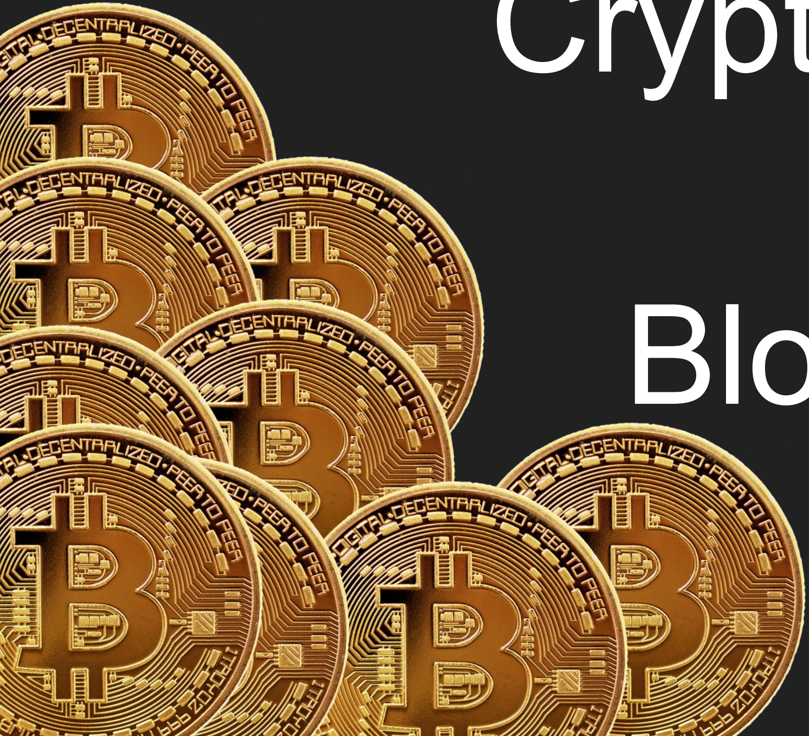
Cryptocurrency and Blockchain



Objective

To get a basic understanding of how blockchain, specifically bitcoin works and explore the mathematics/cryptography behind it.

Overview

1. Introduction: What is cryptocurrency?
2. Overview of how Bitcoin works
3. Cryptography and the blockchain
4. Alternatives and broader applications

Speakers

- Wasee Malik
- Kindeep Singh Kargil

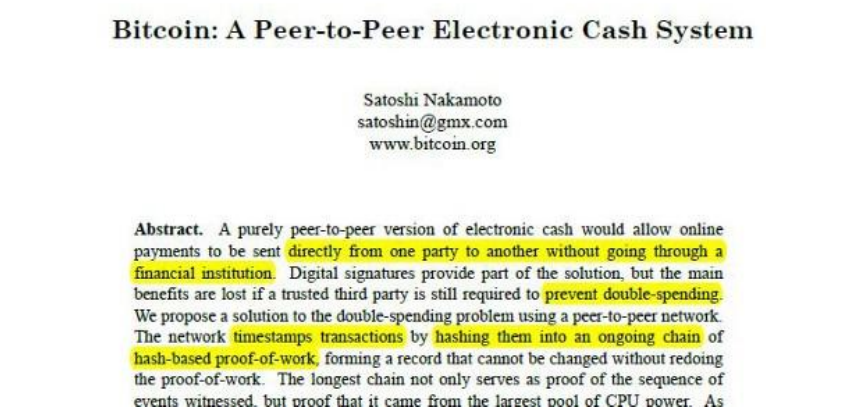
Introduction: What is cryptocurrency?

Reasoning about cryptocurrency

- Currency represents a monetary system in specific units (dollars, euros, yen, etc.) that hold international value which can be traded for any good or service which adopts it
- Governments produce a scarce amount of currency which is very difficult to counterfeit, and because of that there's trust that a currency holds real value
- Similarly, cryptocurrencies represent a monetary system that holds value for anything which adopts it
- Cryptocurrencies are also scarce

Bitcoin: the most popular form of cryptocurrency

- The most popular cryptocurrency today is Bitcoin, created by Satoshi Nakamoto in 2008
- Today, there are many different cryptocurrencies for broader applications, but the creation of Bitcoin and blockchain by Satoshi Nakamoto kickstarted the movement



Bitcoin: A Peer-to-Peer Electronic Cash System

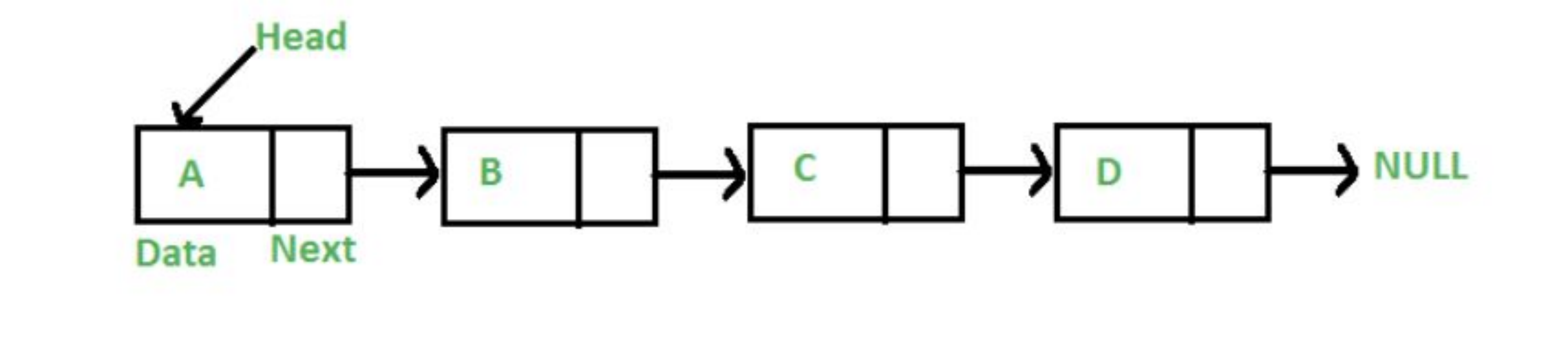
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As

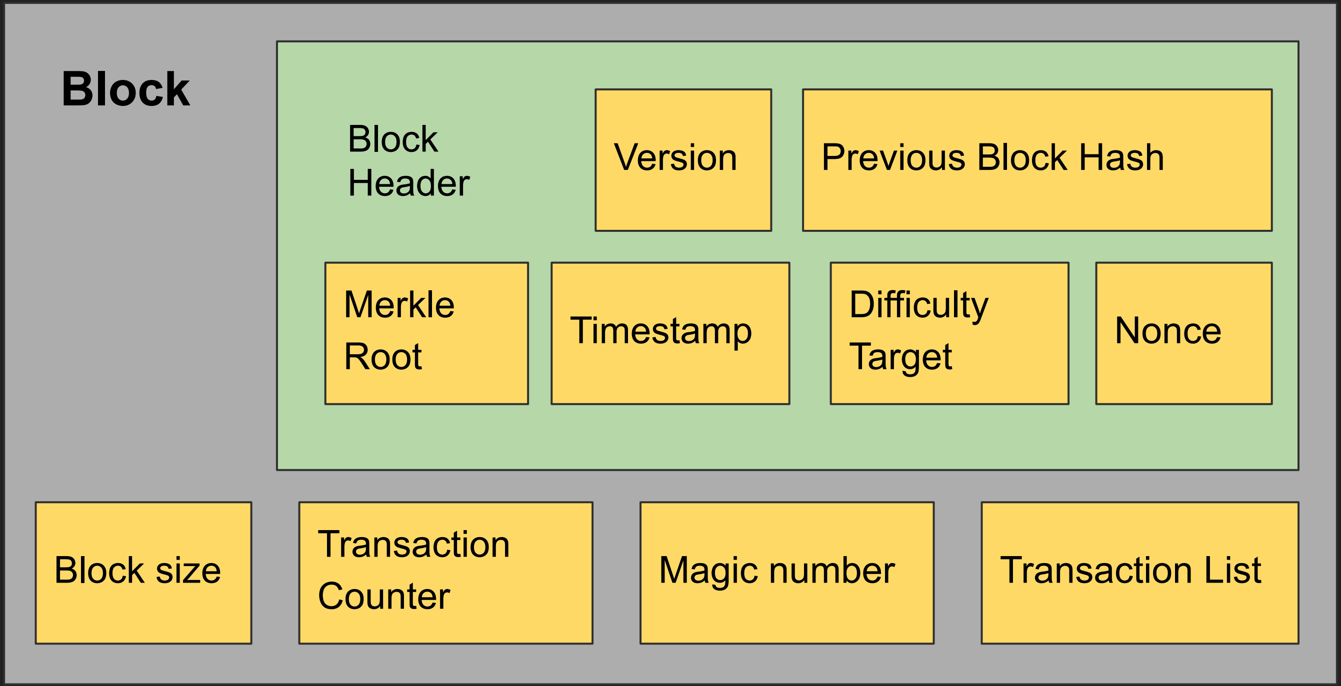
Overview of how Bitcoin works

Blockchain

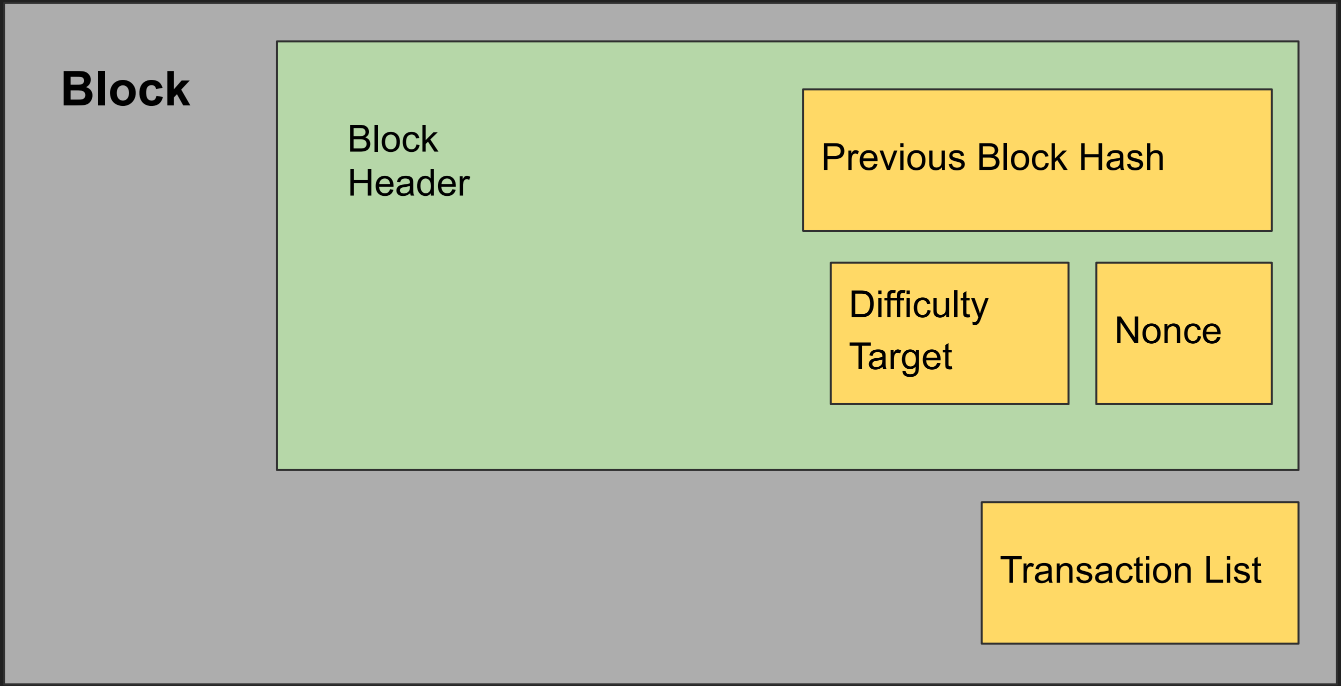
- What is a blockchain?
  - Let’s just call it a chain of blocks.
  - It’s essentially a linked list.



A single block in a blockchain



A (stripped down) single block in a blockchain

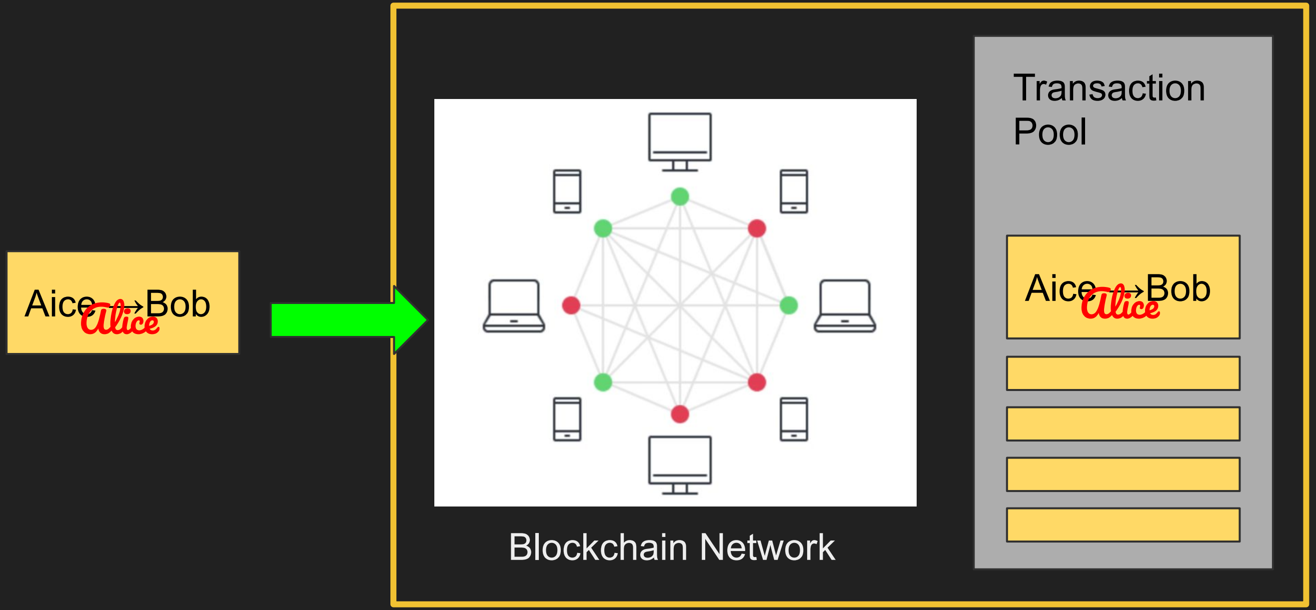


Transactions

- Let’s say you’re Alice, you wanted to make a transaction. You will need the public key of who you’re sending it to. Let’s call him Bob.
- You generate a transaction like [Public key(Alice) -> Public key(Bob)] and use a digital signature to sign it with your private key.

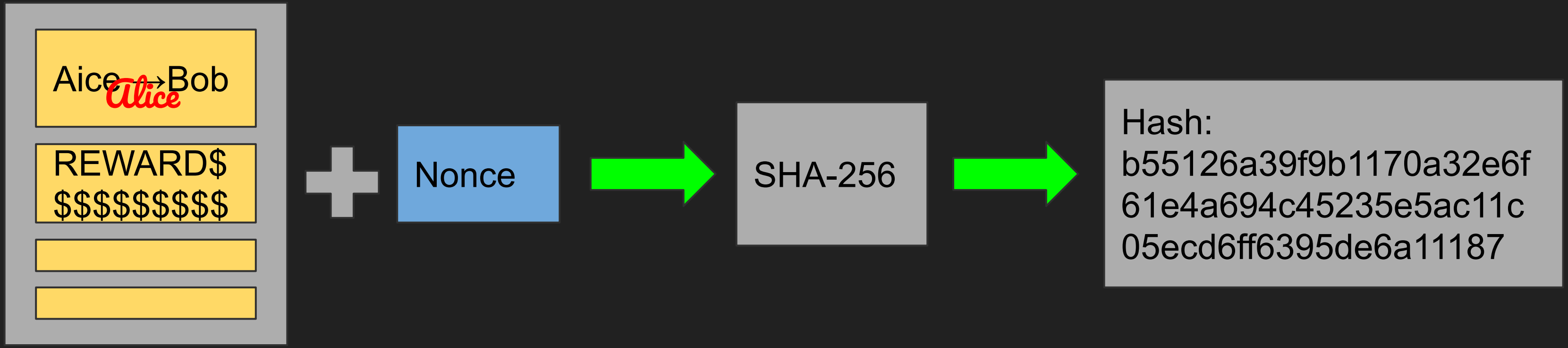
Transaction Pool

- Broadcast this transaction to the blockchain network.
- The transaction gets added to the transaction pool.



Mining

- There is a monetary reward for processing transactions.
- Miners collect a list of transactions from the transaction pool along with a transaction with their monetary reward and verify each transaction.
- These transactions are bundled up into a Block along with other block info like the nonce. This bundle is run through SHA-256 to calculate a ‘hash’.



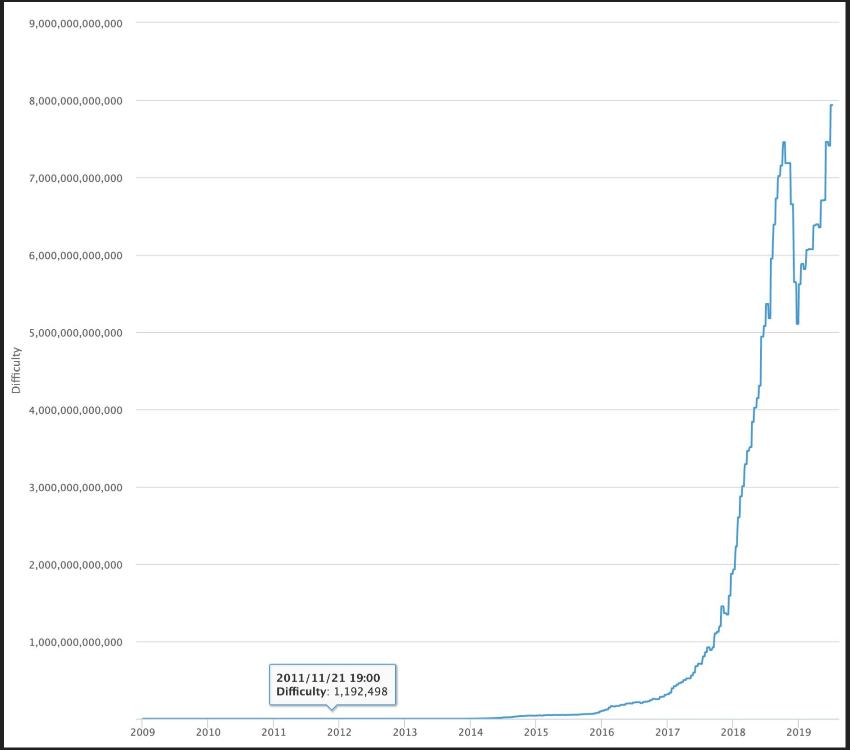
Mining

- Nonce is set to zero initially, and the miner keeps increasing it until it finds a hash value with a number of preceding zeros specified by the difficulty level.
- More the zeros, more the difficulty level.
- Let’s go through an example:-
  nonce + prevhashalicetobob

Mining - Proof of Work

- As we saw, this takes time, and requires computing power. This time keeps increasing as we increase the difficulty, i.e. the required number of preceding zeros.
- For bitcoin, this time is always kept constant at 10 min and the difficulty is increased if the time starts decreasing.
- Now this block is added to the blockchain and is broadcasted to the network.
- Other nodes in the network will verify the validity of the block, and just reject the block if invalid.
- The first node to complete this process gets the monetary reward.

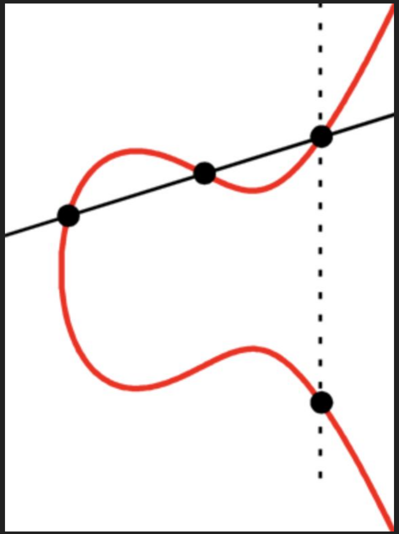
Proof of work



Cryptography and the blockchain

Digital signatures

- Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA)
- We will ignore its existence.
- Instead, let’s look at RSA digital signatures, which works in a similar way.



Digital signatures with RSA - signing

- In order for Bob to sign a message m, he raises m to his private decryption exponent mod n. This is the signature algorithm.
- The verifier must know the message m in order to be sure that this is the message that Bob signed, so in this application Bob must send the ordered pair (m, md mod n).

$$n = p \cdot q$$
$$\text{Choose random e s.t. } (e, \phi(n)) = 1$$
$$e \cdot d = 1 (mod \phi(n))$$
$$\text{message} = \text{m}$$
$$\text{Signed message} = m^d mod(n)$$
$$\text{Broadcasted message} = (m, m^d mod(n), e, n)$$

Digital signatures with RSA - verification

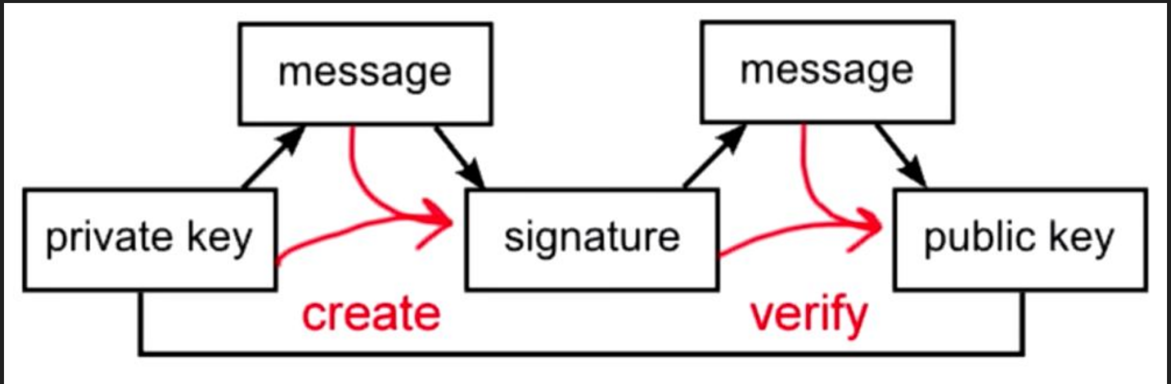
- Anyone can verify this signature by raising m^d to Bob's public encryption exponent mod n. This is the verification algorithm.
- Application of the verification algorithm to a valid signature yields the message m.

$$\text{Broadcasted message} = (m, m^d mod(n), e, n)$$

$$m^{d \cdot e}(mod(n)) = m(mod(n))$$

Making a transaction

- Through the Elliptic Curve Digital Signature Algorithm (ECDSA) method, one can use the private key and message to create the digital signature of the transaction
- The transaction can be verified by anyone in the network by using the person's public key

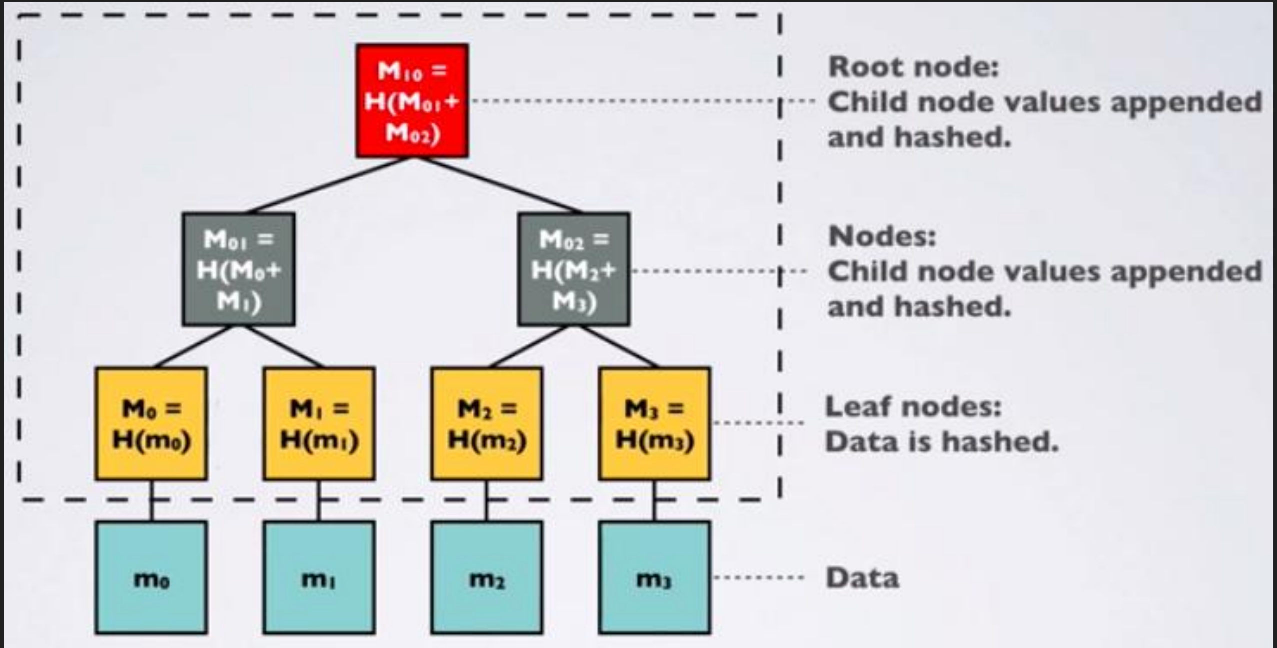


The SHA256 hash function

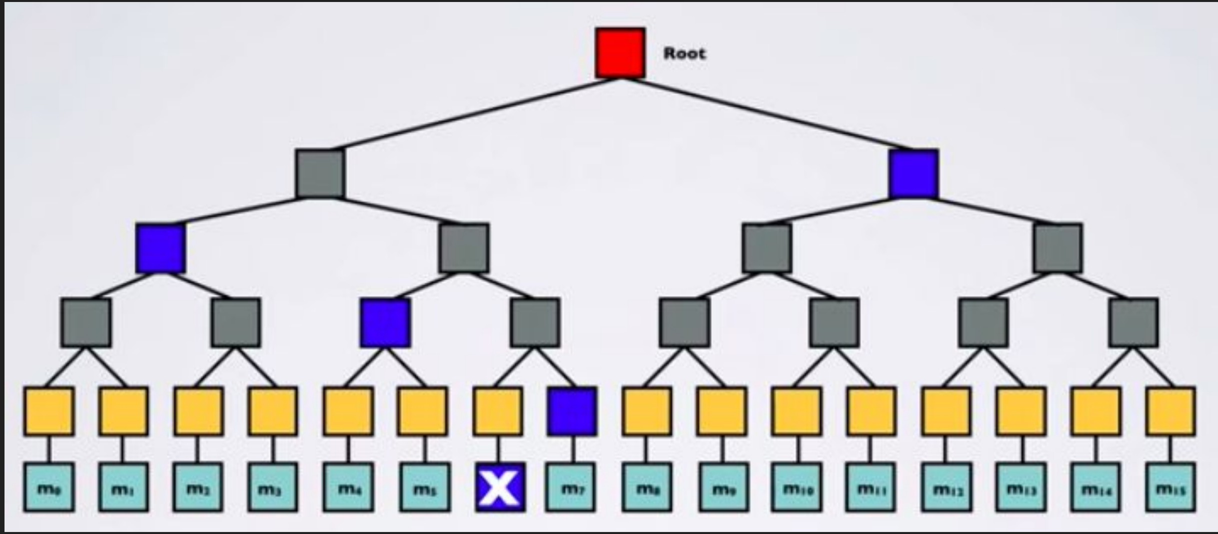
- A *hash function* is any function that can be used to map data of arbitrary size onto data of a fixed size.
- In cryptography, a hash function is a one way function
- The SHA256 hash function is developed by the NSA, and from a given input, produces an output which can be represented by 256 bits
- Hash functions can produce the same index for different keys and they do not have a random output
- The SHA256 hash function is not random, but is *very close* to randomly producing a number represented by 256 bits
- 256 bits → 1.16*10^77 possible numbers

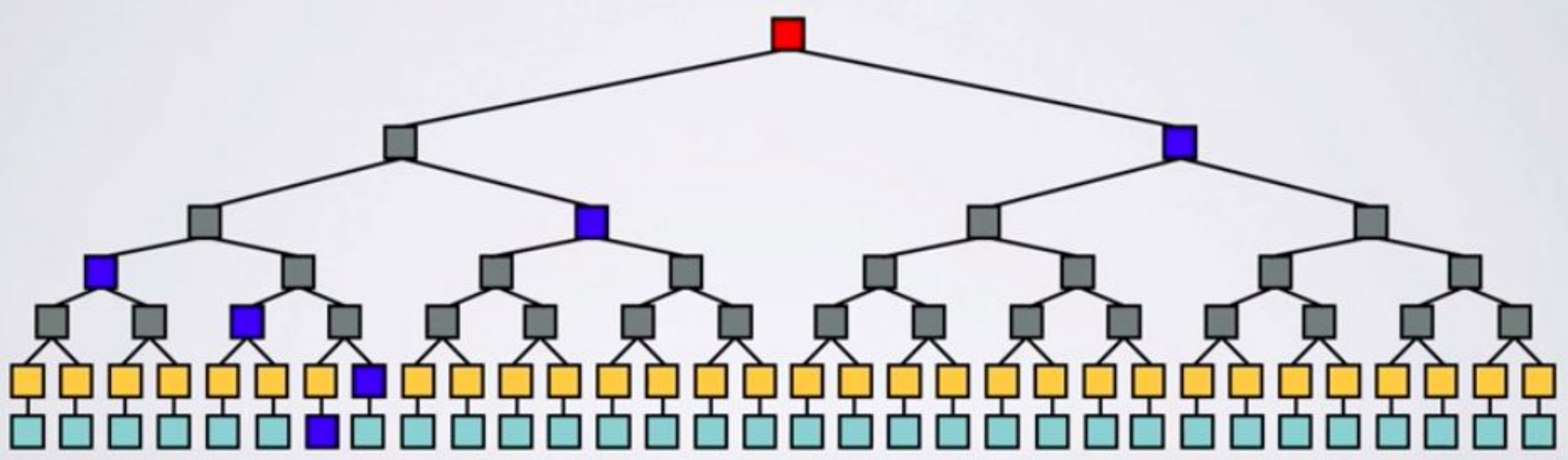
Using a Merkle tree to represent transactions

- A *Merkle tree* in which every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes.
- Merkle trees are inverted in that they start from the leaf nodes and propagate up in pairs until there is only one (root) node.



M10 = H(M01+ M02)
M01 = H(M0+ M1)
M02 = H(M2+ M3)
M0 = H(m0)
M1 = H(m1)
M2 = H(m2)
M3 = H(m3)
m0
m1
m2
m3
Root node:
Child node values appended and hashed.
Nodes:
Child node values appended and hashed.
Leaf nodes:
Data is hashed.
Data


Root
m0
m1
m2
m3
m4
m5
X
m7
m8
m9
m10
m11
m12
m13
m14
m15



Merkle tree code demonstration

Creating the hash for a block

- On the blockchain, each block is referred to by its hash value. Each block refers to the previous block and the next block by their hash value.
- The hash value for a block is created by passing the values in the block header to the hash function:
  - version - represents bitcoin consensus rules
  - hash of the previous block
  - hash of the Merkle root
  - current block timestamp
  - bits to set the target number
  - nonce - a random number which increments after each failed iteration
- If the hash function outputs a value lower than the target number, then the block can be appended to the end of the blockchain

Creating the hash for a block

The *maximum* target number is:

0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

- Probability of a single hash being below the target number (1/16)^8
- Target number changes after every 2016 blocks, by at most a factor of 4

Proof of work, but why?
Byzantine Generals’ problem

- Blockchains rely on a system of consensus
- All nodes in the network cannot be trusted.
- Bitcoin’s security relies on the assumption that at least 51% of the nodes in the network are ‘good’.
- All participating nodes have to agree upon every message that is transmitted between the nodes. If a group of nodes is corrupt or the message that they transmit is corrupt then still the network as a whole should not be affected by it and should resist this ‘Attack’. In short, the network in its entirety has to agree upon every message transmitted in the network.
- But messages of consensus can be altered, can’t rely on someone saying ‘yeah that's correct’

Solution

- The requirement for proof of work allows each node to individually verify that a new proposed block of transactions is currently mined.
- In general, the network picks the longest chain, i.e. the one that required the most amount of work to get to, which is a proof of the combined effort of most of the network.

Double Spending/ 51% attack

- Broadcast A → B.
- Secretly mine a branch with a conflicting transaction that pays A.
- Wait until confirmation from B and receiving product, while continuing to extend the secret blockchain.
- Broadcast secret chain to network. If the chain is longer than any other known by the network, it will be considered valid, and payment to B will be replaced by a payment to A.
- If a attacker controls 51% (>1/2) of the computing power for the network, he will always succeed in making a longer chain.
- Eventually the whole network can be de-incentivized from mining and A will have complete control of the network.

Alternatives and broader applications

Ethereum: platform for decentralized blockchain apps

- Ethereum allows users to write decentralized blockchain applications for more than just currency
- Scripting capabilities are much more robust in comparison to Bitcoin, which focuses on just currency
- Has capabilities for *smart contracts*, programs which execute based on the specific requirements of a clause:
  - ie. betting on the results of a race, and the winner would get a specified amount of Ether from the loser
- Blocks take ~15 seconds to process, compared to ~10 minutes for Bitcoin

Ripple: a payment protocol used by banks

- Ripple is a payment protocol that allows people to transfer and exchange currency
- Ripple is maintained and developed by Ripple Labs, and uses the XRP token as its method of cryptocurrency
- XRP is widely adopted at different banks worldwide, and transactions are processed within seconds through a network consensus
- XRP has the second largest market cap behind Bitcoin at 73 billion USD

Libra: a currency for Facebook

- Libra was announced in June 2019 as Facebook's own cryptocurrency, and is to be released in 2020
- Libra can be programmed to operate in smart contracts with its new scripting language, called Move
- Facebook has faced a large amount of backlash for saying that Libra is decentralized on the project site, but later admitting that it will only be decentralized it in the years to come
- Facebook has had issues with user privacy in the past

Cash

Or better yet...

Barter System