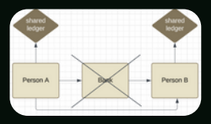
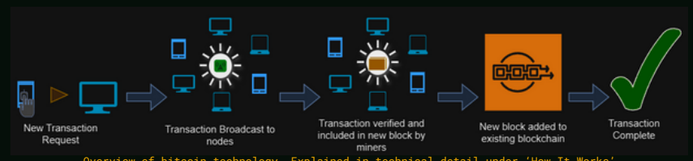
Bitcoin - A Peer-to-Peer Electronic Cash System

Introduction

- bitcoin is a cryptocurrency developed to eliminate the double spending problem (when the same unit of currency is spent more than once) within a peer-to-peer electronic cash system network
- (A Ledger - Trust factor) + Cryptography = Cryptocurrency
- Most forms of cashless payments nowadays rely on third-party institutions, like banks or governments, to track transactions. This system is based on trust in these institutions to be accurate and fair. Bitcoin eliminates the need for a middleman as it operates as a decentralised shared public ledger
- Electronic cashless payments increase -> Number of disputes increase -> Cost increase. This results in transaction fees and other charges from banks. We can solve this problem as well as there is no intermediary (peer-to-peer)



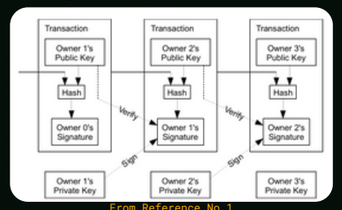


Overview of bitcoin technology. Explained in technical detail under 'How It Works'

How It Works

Digital Signature

- Each person who uses the Bitcoin network has a public key (pk) and a private/secret key (sk). pk is the only ID, otherwise anonymous (pseudonymous)
- A digital signature is designed to be different for each transaction to ensure it cannot be forged
- A hash function takes the transaction and your sk and outputs a string of 1s and 0s (256 bits): h(transaction, sk) = 256 bit hash -> digital signature
- Another function is used to verify the transaction by checking against your pk to make sure the transaction is made by the owner of the pk/sk pair: v(transaction, digital signature, pk) = True/ False



From Reference No.1

References

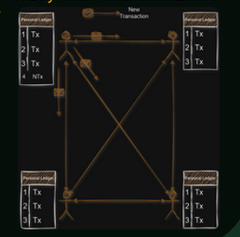
- *Bitcoin: A Peer-to-Peer Electronic Cash System* - Satoshi Nakamoto (Founder)
- *Blockchain Technology Overview* - Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone
- *But how does bitcoin actually work* - 3Blue1Brown (Youtube Video)
- *How bitcoins work under the hood* - CuriousInventor (Youtube Video)

Ledger History = Currency!

- It is computationally infeasible (currently) to crack someone's sk by brute-force methods
- Each transaction has a unique ID as well to avoid duplicate transactions. Therefore, duplicate transactions would also have a different signature
- These requirements make it very hard to make fraudulent transactions
- To avoid people from overspending or double spending, the only way for everyone to know if you can make a valid transaction is by knowing the whole history of transactions
- This means that the ledger history is the currency! (since that is the only proof of how much you have)
- This also means that a bitcoin is it's own independent currency!

Decentralised Ledger

- Now that we have no middleman (banks/governments) to keep track of the transactions, the transactions are recorded in a public ledger
- But if there is only one public ledger it becomes centralised again - Where is it hosted? Who decides what transactions go on the ledger?
- To remove this problem, each person gets a copy of the ledger to keep in their system -> A shared public ledger -> A distributed timestamp server (records time and order of transactions)
- Every transaction is broadcast so that each person can update their version of the ledger. Some systems in this network called nodes verify the transactions.
- How do we all agree on the same version of the ledger?



Misuses

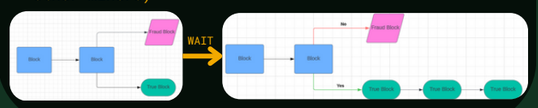
- bitcoin's pseudonymous nature (every person has a pk and no other personal details), facilitates its use in illegal purchases and tax evasion
- Easy remit without intermediaries makes it easy for users to obfuscate transaction trails, aiding money laundering
- The proof of work mining process demands significant energy and raises environmental impact concerns
- Emergence of quantum computing poses a potential risk to the Bitcoin network, as its fast decryption capabilities could render current security measures vulnerable to cyberattacks.

Uses

- The most significant advantage of using bitcoin is that digital transactions and payments can be conducted globally without relying on any traditional banking systems
- This system provides quick and cost-effective remittances even internationally
- People invest in bitcoins due to its limited supply, which enhances its value as a resource
- You just need a mobile phone and access to the internet to send and receive bitcoins (easy to set up and user-friendly)

Conflict Resolution

- The Bitcoin protocol relies on the blockchain with the highest amount of computational work invested in it
- When there are two conflicting blocks, the network waits for additional blocks to be added. The longer blockchain is then recognized as the correct ledger history
- If someone were to create a block with a fraudulent transaction, a tremendous amount of computational work would be required to sustain that chain (more than 50% of the total computational power of all other miners)

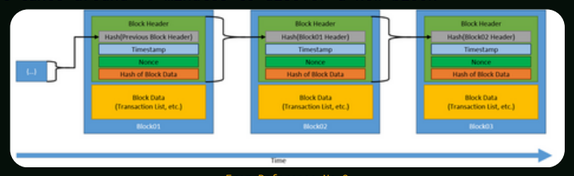


New bitcoin

- How does new money enter the system? People who perform computational work to find the specific number that generates the required hash are called miners (data miners)
- Data mining is incentivized, which means they are rewarded with bitcoins for the computational work they undertake to discover the nonce
- Initially, the reward for successfully mining a block was 50 BTC, but approximately every 210,000 blocks (roughly 4 years) the reward gets cut in half (Currently set at 6.25 BTC)
- As a result, the total supply of bitcoins is capped at 21 million, mimicking the scarcity of precious substances like gold (BTC -> Digital Gold)
- All new money entering the Bitcoin network comes through Proof of Work rewards
- Additionally, miners can earn money from transaction fees (optional) included by senders to incentivize miners to incorporate their transactions into their block
- Each block is limited to around 2400 transactions.

Blockchain Technology

- So instead of a ledger, this becomes analogous to a linked list, a chain of blocks of transactions -> Blockchain
- To optimize space, transactions are stored in the form of a Merkle tree. As a result, a block will contain the hash of the previous block, the nonce, the hash of the current block, and the root hash of the transaction list stored within the Merkle tree
- The Bitcoin protocol employs the SHA-256 cryptographic function and periodically adjusts the number of leading zeroes approximately every 2020 block, to ensure on average it takes around 10 minutes to disover a new block



From Reference No.2

Proof of Work Consensus

- A cryptographic hash function is a function that takes a list of transactions and returns a 256-bit hash called a digest. chf(list of transactions) = digest (256-bit hash)
- The principle is similar to a digital signature in the sense that it is designed to be computationally infeasible to find the input from the digest
- The idea is to find a number called a nonce (number used once), when added to the end of a list of verified transactions will give a digest that satisfies a certain condition, e.g., the hash starts with 10 0s (depending on the protocol)
- Finding the nonce of a list of transactions takes a considerable amount of computational work since only brute-force methods work
- The nonce is the Proof of Work and can be easily verified by putting it through the cryptographic hash function
- List of verified transactions + nonce + previous hash (digest) = block. The previous block's hash is included in a block so that any alteration to a prior block will result in a different hash for that block, which in turn changes the hashes of all subsequent blocks, effectively preventing fraud