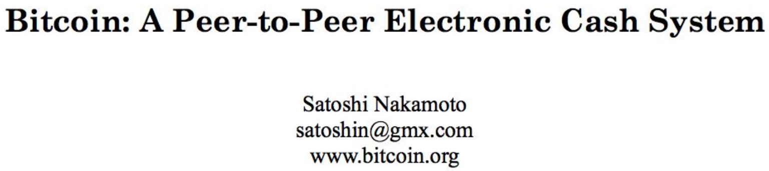
A Technical Primer on Blockchain

Dhruv Luthra

What is Bitcoin?



Bitcoin: A Peer-to-Peer Electronic Cash System

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

- A digital/crypto/network currency
- Exchange value without a centralized institution

But what is it really?

“A cryptographically secured network currency enabled by a blockchain”

What is a blockchain?

It’s in the name: a chain of blocks that contain **information**

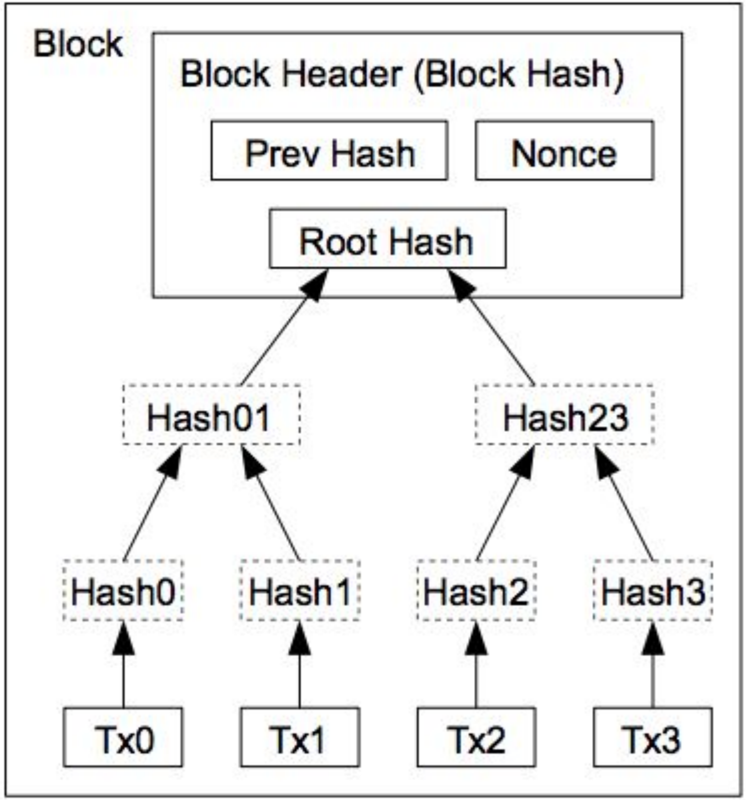
The information: sets of **transactions**

Often described as **a decentralized**, **immutable digital ledger**

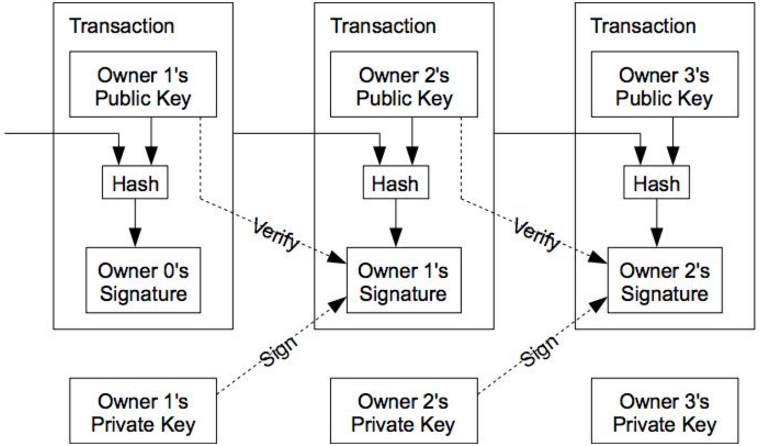
What’s in a block?

- The hash of the previous block
- A nonce
- The transactions to be included in the block

We’ll talk more about what each of these mean and why they’re important!



What’s in a transaction?



- The sender of the Bitcoin (Person A)
- The receiver of the Bitcoin (Person B)
- A signature validating that Person A is sending the Bitcoin to Person B

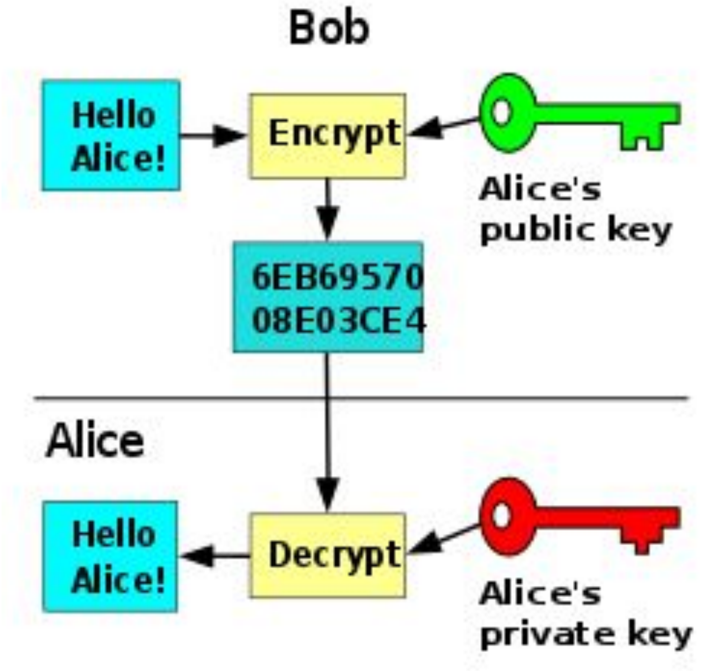
Private-Public Key Cryptography

Two related keys for encrypting and decrypting data

- Private Key: Used to decryption
- Public Key: Used for encryption
- Public key is easy to figure out from private key, but the reverse is very difficult

Together, enable us to receive private messages

An example...



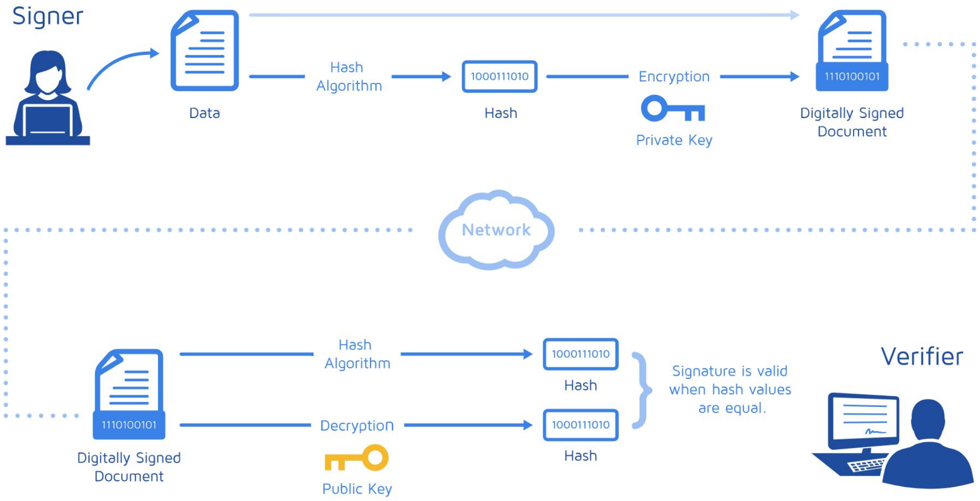
- Bob wants to send a message to Alice
- Bob encrypts the message using Alice’s public key
- Alice uses her private key (which only she has!) to decrypt the message

So now… Bob has a (public) message he wants to send to Alice. Alice needs to make sure the message was sent from Bob and not changed. How do we do this?

Digital Signatures

Leverages the assymetry of Private-Public Key cryptography to ensure 3 critical properties of messages:

- Authenticity
- Non-repudiation
- Integrity



How does this work?

1) Key generation algorithm: Public and private key pair generated
2) Signature algorithm: Uses the message being sent and the private key to create a digital signature
3) Verification algorithm: Determines if a message is valid when given a message, a public key, and a digital signature

What does this have to do with Bitcoin?

A Bitcoin address is just a **public key.**

The private key is stored in your wallet.

The blockchain is just a **ledger of addresses** with the amount of Bitcoin stored at each address.

To say you want to send 1 Bitcoin from Address A to Address B, Address A needs to sign the transaction with the associated **private key**

So what is a transaction...

A message: Bob is sending 1 Bitcoin to Alice

A signature: Bob signs the transaction (AKA message) with his private key

Alice can check the transaction using Bob’s public key (i.e. the address the money is coming from)

BUT ALSO: Anyone in the network can check the transaction because Bob’s address is public-> **they have the public key**

So now… we have transactions, and we know they’re organized in blocks as a ledger. This isn’t new… what makes Bitcoin different?

The Problems Bitcoin Solved

Two critical issues:

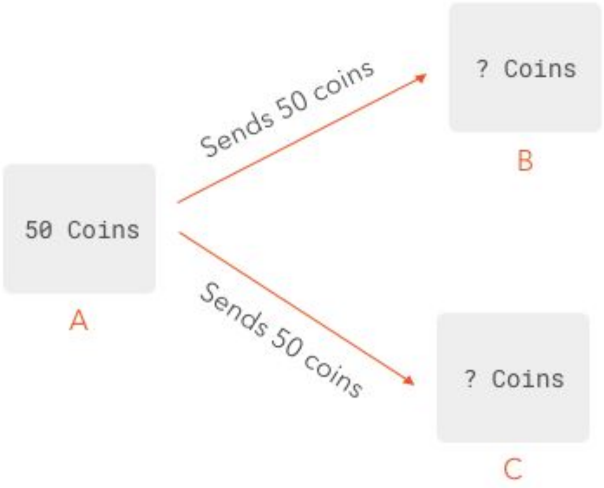
- The Double Spend Problem
- The Byzantine General’s Problem

The Double Spend Problem

Bob has 12 BTC.

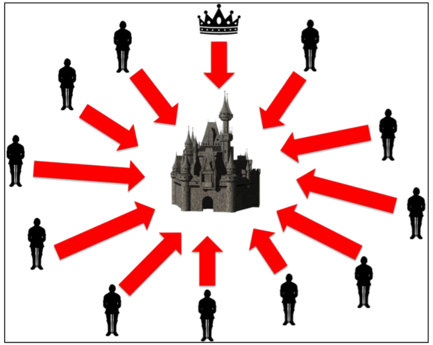
How do we stop him from sending 12 BTC to both Alice and Alice's sister?

This can't happen with fiat… and there are many institutions that stop you from doing so.

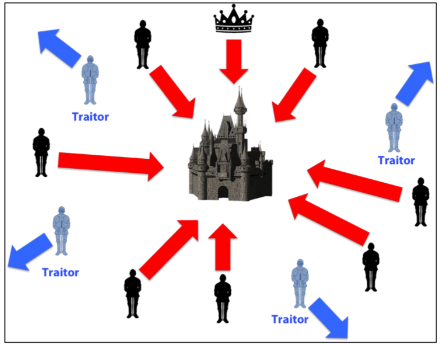


Byzantine General's Problem as Applied to Blockchain

In a system where you don't know who to trust… how can you prevent malicious outcomes?



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

A Byzantine Fault Tolerant system is a system that prevents negative outcomes, even when there are traitorous generals.

Consensus Mechanisms

In the context of blockchains:

Consensus mechanisms determine what the next block should be.

We want each block to contain valid transactions.

Therefore, our consensus mechanism **must solve the double spend problem and by Byzantine Fault Tolerant.**

Proof-of-Work

General Idea: Nodes must solve a particular computationally difficult problem to ‘mine’ the next block

How do we get people to spend resources?

Reward the solver of the problem with some amount of Bitcoin (or other cryptocurrency)

Introducing a new player: The Miner

Their job: determine the next valid block

Pick from a pool of transactions sorted by transaction fee

These transactions become a part of the problem that needs to be solved

So what is this problem I keep talking about?

A Hashing Problem: Hard to solve, Easy to verify

Remember what is in each block:

- Hash of previous block
- Set of transactions in the block
- **The nonce**

Looking for a specific hash of this set of information

Once a miner solves the problem...

Miner broadcasts the solution

Every other node can easily verify the solution

Once 51% of miners agree that the new block is valid, **consensus has been reached,** the block is added to the chain, and miners move on to solving the next problem

Immutability is a Result of Proof-of-Work

To change a transaction, you would have to resolve the proof-of-work for the block.

Because the block is connected to the previous ones, you’d have to resolve the hashing problem for the previous block… and the one before that… and the one before that… and every block from the start

Criticisms of Proof-of-Work

Scalability -> there is a limit on block size, so only so many transactions can be included every block

Centralization of Mining: ASICs have enabled some large organizations to control a significant amount of the mining power (i.e. China)

Energy Consumption: The energy used for mining farms is horrendous and mainly comes from fossil fuels

Proof-of-Work isn’t the only consensus mechanism

Proof-of-Stake

Important for Ethereum

Block validators deposit some cryptocurrency into an account. One of them is randomly chose to generate the next block.

Once the block creator generates the block, the other validators check to see if it is valid.

If you propose invalid blocks, you lose your deposit.

Practical Byzantine Fault Tolerant Mechanisms

The main value of Proof-of-Work and Proof-of-Stake is that they do not **require any trust between parties in the network**.

They are also public: any node can see any transaction

There are other consensus mechanisms… they enable privacy, but you have to assume some information

Ex: The Tendermint proposal assumes ⅓ of nodes are trustworthy

So where does that leave us?

A blockchain is an immutable, decentralized digital ledger of transactions

Each block in the chain contains a set of valid transactions.

Each transaction is signed by the sending party using cryptography (digital signatures)

A consensus mechanism is used to determine the next valid block of transactions.

To stay involved and learn more: Chat with us after, sign up for the DBL list serve on the website, fill out the interest form