

How Cryptography & Hashing keeps a blockchain secure

Group 1

Parikha Goyanka

Anushka Saxena

Aman Bahuguna



Summer Internship 2020, Internity Foundation

What is a blockchain?



- Blockchain is a **record of transactions** similar to a **traditional ledger**.
- Blockchains aren't on display on public , anyone who wants to can store a copy of a blockchain on their computer.
- Blockchains use **cryptography**, **computers** and **electricity** to build the blocks.
- This technology has the potential to be used in vast range of applications.



The uses of blockchain

- Cryptocurrencies
- Decentralised apps & Smart Contracts
- Supply - chain management
- Financial Transactions



Uses of blockchain contd.

- **IBM Food Trust** uses this technology to manage food supply logistics.
- Banks such as **UBS** are adapting blockchains for financial settlements.
- **Australian Stock Exchange(ASX)** aiming to adopt this technology.
- Blockchains are yet to be fruitful as many have hoped.



Bitcoin : Transaction in blockchain

- Bitcoin is **cryptography based currency** that could avoid the downsides of having a financial system controlled by central institutions.
- The basic intuition is **transferring value through a chain of digital signatures**



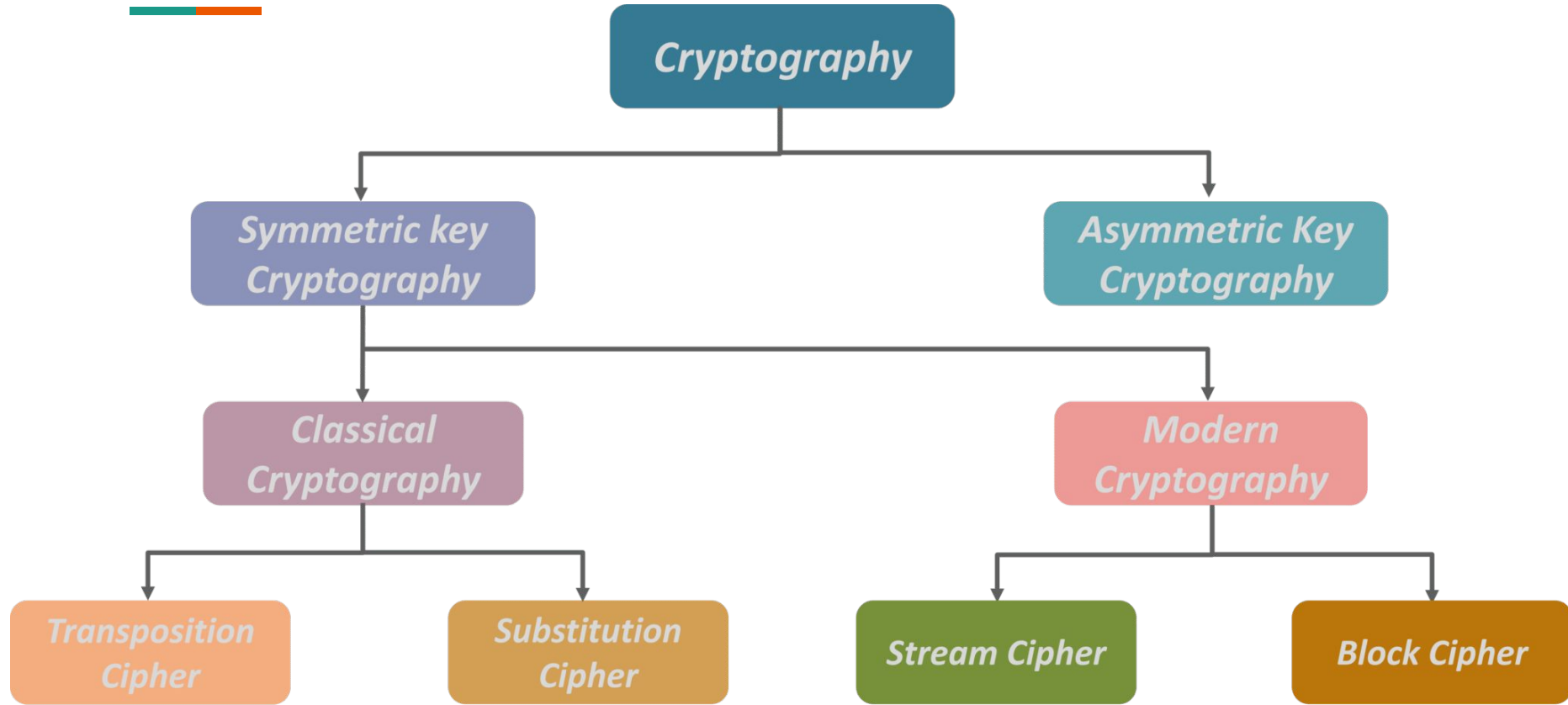
What is cryptography?



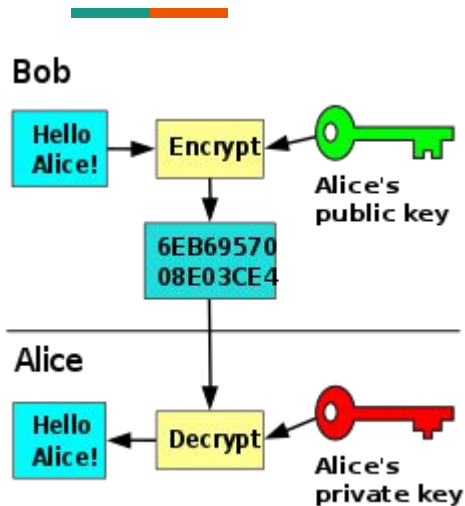
Cryptography



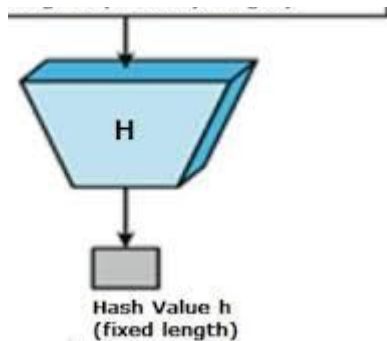
Types of Cryptography



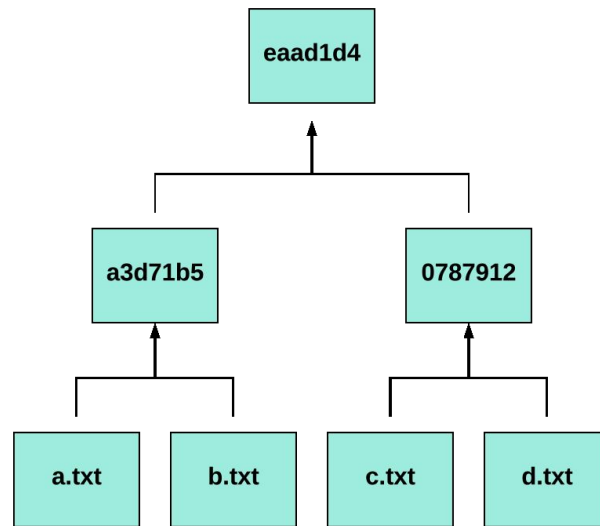
Cryptography in Blockchain



Public-key Cryptography



Cryptographic Hashing



Merkle Tree

Cryptography in blockchain

Helps manage:

- Wallets
- Transactions
- Security



Why Cryptography in Blockchain?

- Confidentiality
- Authentication
- Integrity
- Non- Repudiation



Hashing

What is hashing ?




- ❖ Hashing is the process of sending data through a hash function to produce a specific, essentially unique hash of a fixed length.
- ❖ The most used cryptographic hash functions is SHA-256.

WHY Cryptographic hash functions?

- They are deterministic.
- They are one way functions.
- Hashes can be computed quickly.
- A slight change in the input results in a significantly different output.

Where hashing is used ?

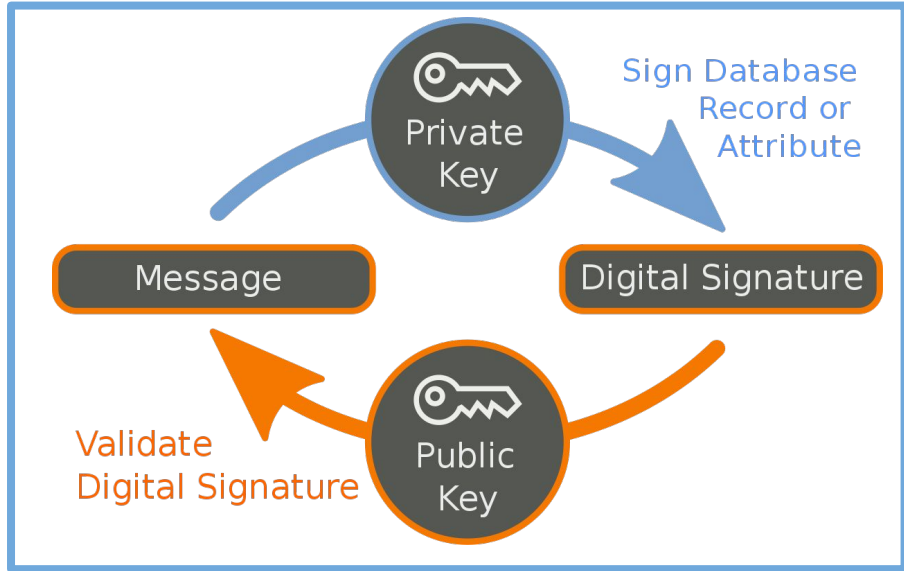
Hashing is mainly used in digital signature.

- 
- When a new transaction is made, **the data is also hashed to form a transaction ID (txid)**, which is an identifier that can be used to locate the transaction details on the blockchain.
 - When a transaction is being made, **data from previous transactions is hashed** and included in the present transaction.
 - **A hash of the public key is used as the address** where users can send funds. This makes the addresses shorter and more convenient, as well as providing some security benefits.

Digital Signatures

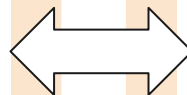
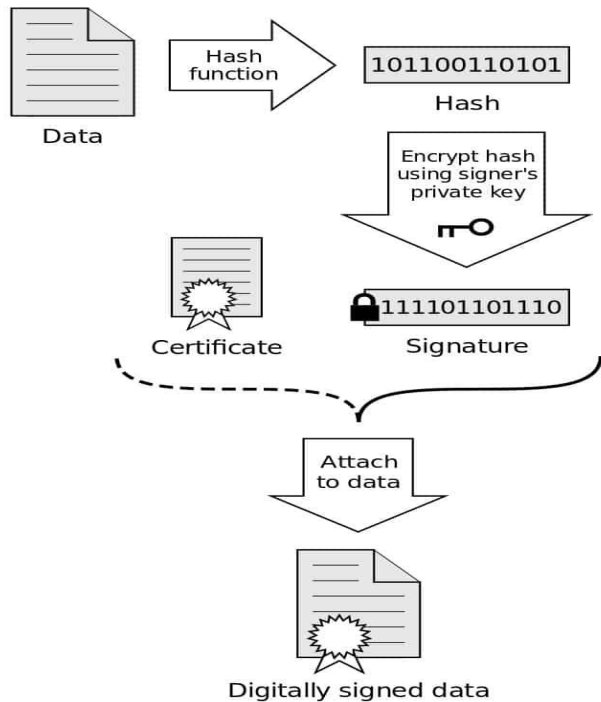
What is a digital signature ?

- A digital signature is a cryptographic means which allow an individual to prove their ownership (of private key without revealing it to other party).
- D.S. are used to validate the authenticity and integrity of data or message at the same time by assuring repudiability of it.
- It is based on Public Key Cryptography.
- In bitcoin and other blockchains, digital signatures are mainly used in the transaction process as a way for someone to prove their ownership, without having to reveal their private key.
- Some of the most common digital signature schemes include RSA, DSA, EcDSA and EdDSA.

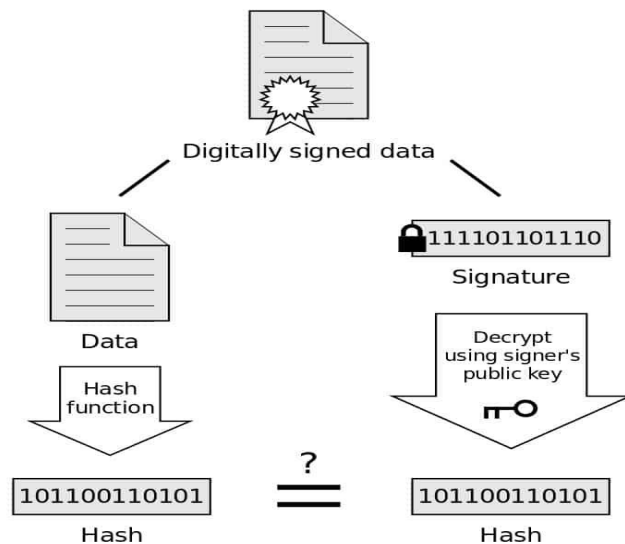


How it works?

Signing



Verification



If the hashes are equal, the signature is valid.

Proof of security

➤ Digital Signature security unit

- Data signed with a private key is verified with the same individual's matching public key.

If (it matches)
then transaction will move forward
Else
it get terminated

- It should be essentially impossible (using current technology and techniques) to forge a valid signature without knowing the individual's private key.

➤ To prevent double spending



- The bitcoin protocol uses a concept known as proof-of-work to validate its transactions. This proof-of-work system is based on the **SHA-256 algorithm**.
- Moreover it uses a peer to peer verification process(mining) using nodes and minors to prevent double spending, as it is considered that its relatively difficult to compute the solution, but easy to verify it.

