**Blockchain**

Hash function-

Process of converting input of any length into a fixed size string of text using mathematical function.

So any text can be converted into an array of numbers and letters, with an algorithm.

The message to be hashed is input, the algorithm used to do so is called hash function output is hash value.

A cryptographic hash function requisites... each hash value has to be unique (impossible to produce same hash value when

entering different inputs so same message should always produce the same hash value), hashing speed is

important- function should be quick to produce a hash value and a hash function needs to be secure- needs to be impossible

or at least extremely difficult to determine input based on the hash value while a slightest change to an input should

generate a hugely different hash to be useful

Hashes are used to represent the current state of a blockchain and ensure its immutability.

Every transaction has certain bits of information: amount sent, sending and receiving addresses, timestamp...

All this is combined in the formula to produce a hash called- transaction id: this is a hash value that can be used to

identify and confirm that a transaction has happened.

First block in a blockchain called a Genesis Block contains transactions that when combined create a unique hash when the

second block is created the hash of Genesis Block is added to all of the new transactions in the new (second) block; this

combination is used to create its respective hash and this is completed with all the new blocks being added to a blockchain

always taking previous hashes to generate the newer ones creating an unbreakable dependency, this way each block links back

to its previous block through its hash forming a chain back to the Genesis Block.

Blockchain is a secure, immutable and transparent network for money transfer.

Nodes-

A connection point between branches in a system, a place where things meet.

Computers working together to verify a transaction and update a common database.

Nodes are places in a network where information is received and sent out elsewhere- essentially every computer in the network is a node.

Block: structure of a Block in Blockchain.

Basic structure- there are four sections

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|Block size | Size of block in bytes

|Block header | Where meat of the block is- several fields

|Transaction counter | How many transactions on block

|Transactions | All the transactions being processed inside block

Wallets, Digital signatures and Protocols-

A Wallet is a tool you can use to interact with a blockchain network. There are

three main groups: Software(hot wallet), Hardware(cold wallet) and Paper(cold wallet).

Crypto wallets work as a gateway giving you the tools you need to communicate with a blockchain- these can generate all the information you need to use cryptocurrencies.

When creating a wallet, for a person or business, the program generates multiple pairs of public and private keys + several blockchain addresses.

When sending money the program calculates the pair of keys one public and one private. The public key is used to generate a unique BTC address, this is the address the sender needs to send BTC from his wallet to the receiver's wallet.

The coins never leave the blockchain, they are just transferred from one address to another. One should never give out their private key but can give a BTC address of course.

Private key is used for signing new transactions and gives one access to their funds. So even if Alice loses access to her computer or phone she can use the private key to access her coins on any device. If anyone gets to know her PK they can steal her funds. She can also use her private key to recover public key and BTC addresses- it precedes all other components and is the most important element of a crypto wallet.

Most modern wallets use a: Seed phrase- these allow one to make multiple PK so instead of making a backup of each PK she only needs to backup the seed phrase. This works like a root key giving access to all keys and addresses in Alice's wallet.

Types, aforementioned, named based on how they operate:

Hot wallets- any wallet connected somehow to the Internet: *Software wallet*

*These come in Web, Desktop (with program) and Mobile wallets (apps on phone) allow you to interact with blockchain via these different mediums.*

Cold wallets- much safer, having no connection to the Internet, they use a physical medium to store the keys offline so they are very resistant to hackers aka Cold storage particularly suitable for the long term investor: *Hardware wallet*

*Physical electronic devices that use rng to generate public and private key they are stored in the device itself with no Internet but less accessible for the frequent user, Paper wallet-*

*A piece of paper that blockchain address and its private key are physically printed out usually as QR codes, so one can generate and have a paper wallet and send funds via the QR codes, their use is now discouraged as they are not suitable for sending funds partially only the entire balance is sent all at once.*

*Should back up Wallet data file and Seed phrases for security*

Some notes on public, private key, signatures and addresses-

In simple words, the Bitcoin address is a hash of the public key. A hash is just a certain value. The public key is known when you make a transaction - it is derived from the private key. Hashes are used as a security measure to prevent potential theft.

Private keys can decrypt a public key, one can encrypt things to their public key.

Public key isn’t known until money is spent, people can encrypt things to your public key for decryption with your private key e.g. messages.

A second feature of private/public keys is digital signatures. A signature is something that can only be created by your private key, but which your public key can be used to verify that the signature indeed must have been created with your private key.

Address is a hash of a public key

When send money to an address, a hash of public key is only revealed when you spend money as it is necessary to prove the digital signature came from your private key and the way it is verified of validity is a program checks the signature with the public key

Public key is for encryption and private key is for decryption.

