BISTEC GLOBAL

BISTEC
Hearts Academy

first part

Road to Web3.0

Let’s build an eKYC application using blockchain.

Gayashan Wagachchige

BISTEC
Hearts Academy

HEARTS ACADEMY

Help our Hearts to improve their skills.

BISTEC
Hearts Academy

First part

Core Concepts of Blockchain

Second part

Ethereum Development

Third part

Build eKYC Application using blockchain

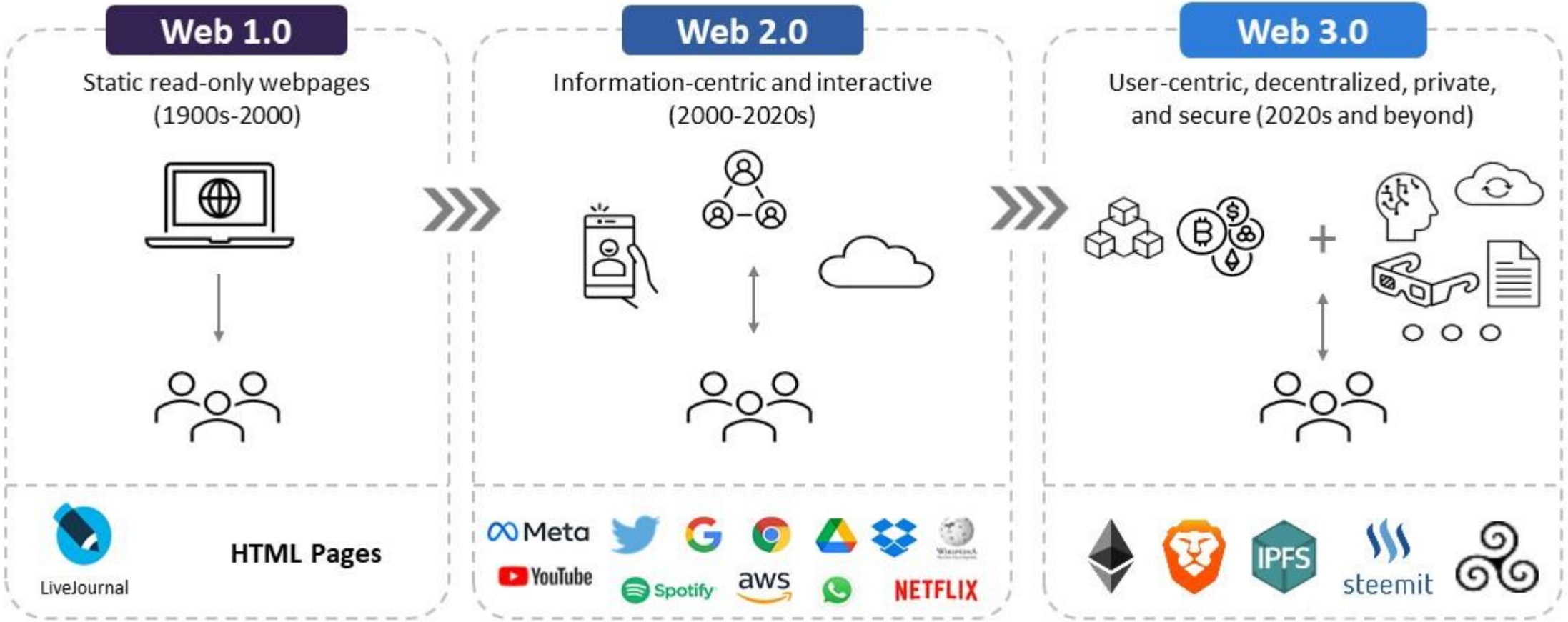
BISTEC
Hearts Academy

What will you learn ?

- A bit about Web 3.0
- Cryptocurrency & Crypto wallets
- Core Concepts of Blockchain
- How to write a smart contract with Remix IDE

BISTEC
Hearts Academy

The Future is Web 3.0



BISTEC
Hearts Academy

Cryptocurrency

Users Perspective of Blockchain.

Bitcoin

Who is Satoshi Nakamoto?

- **Bitcoin Whitepaper**
  Bitcoin : A peer-to-peer electronic cash system (2008)
- Who is **Satoshi Nakamoto** ?
- Bitcoin launched in January 2009 as world's first cryptocurrency
- Bitcoin market cap:
  as 2013, 1 Billion USD
  as 2021, 1100 billion USD
- Cryptocurrency is **the single disruptive force** in recent financial history.

BISTEC
Hearts Academy

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 long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Ethereum ETH

USD Coin USDC

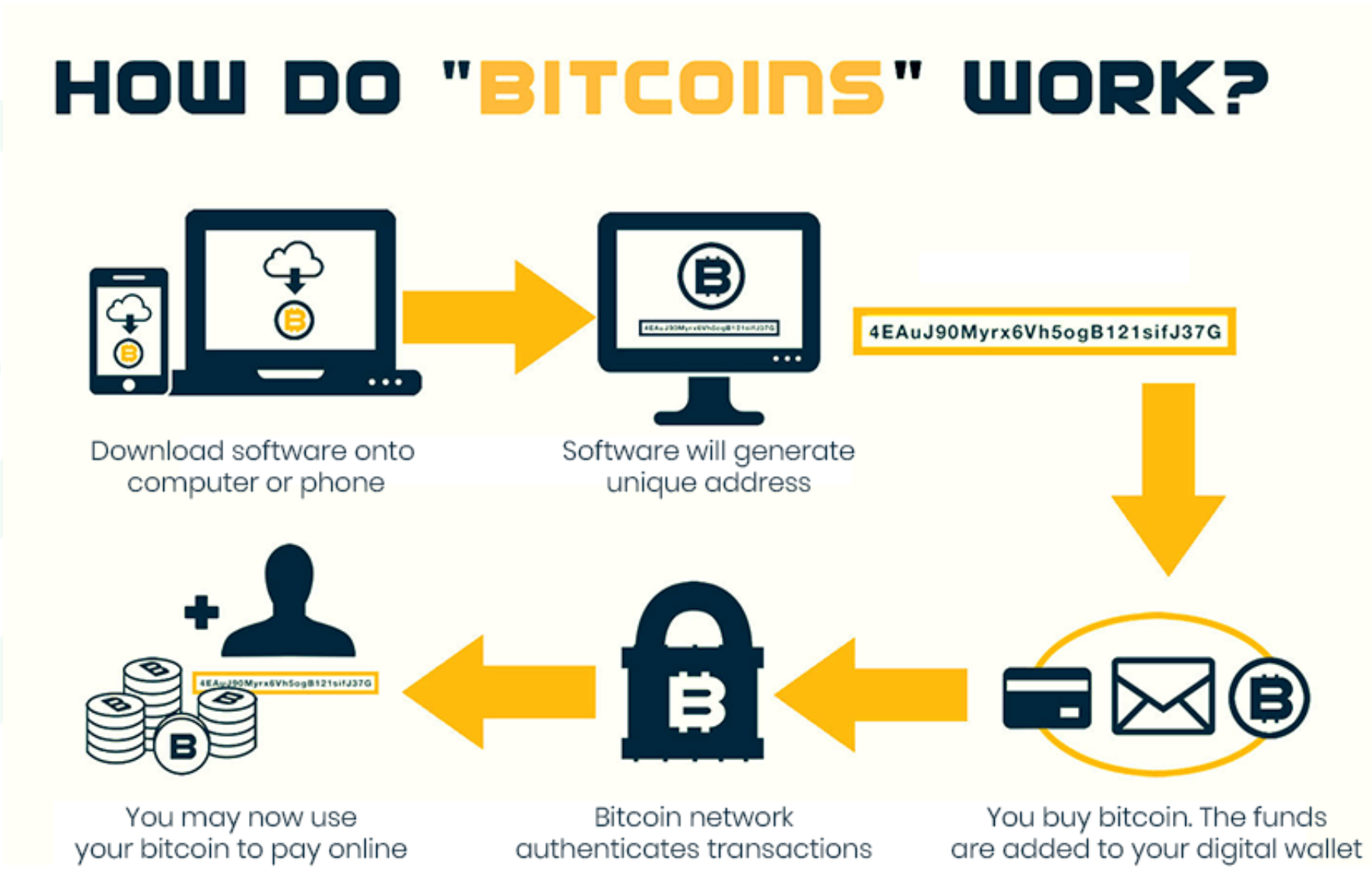
Litecoin LTC

Tether USDT

Dogecoin DOGE

Terra LUNA

HOW DO "BITCOINS" WORK?



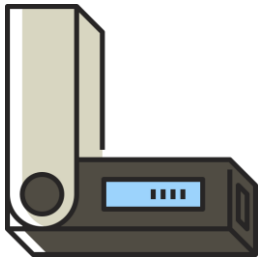
BISTEC
Hearts Academy

Let’s interact with cryptocurrency.

- Install Metamask.
- Get some ‘fake’ crypto.
- Perform transactions.
- Track transactions in a block-explorer.

Crypto-wallets

Software wallets



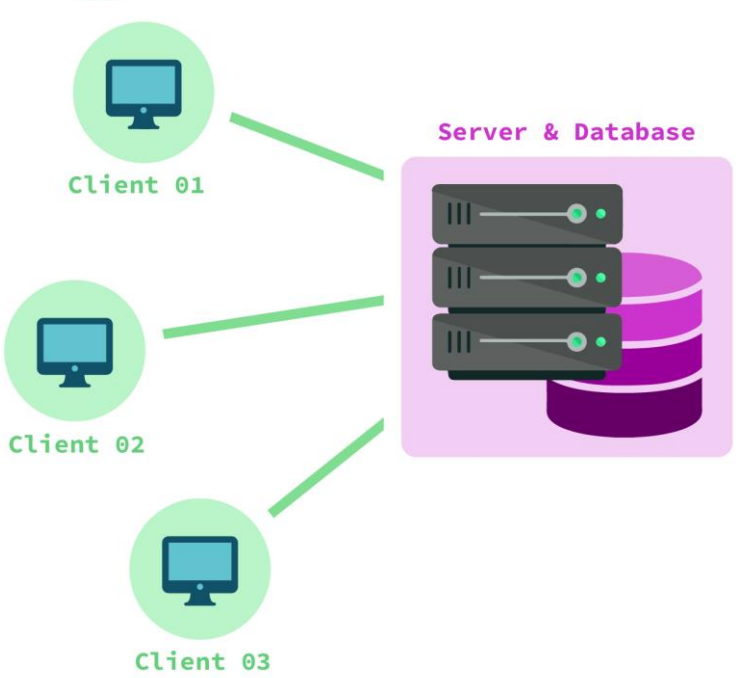
Hardware wallets

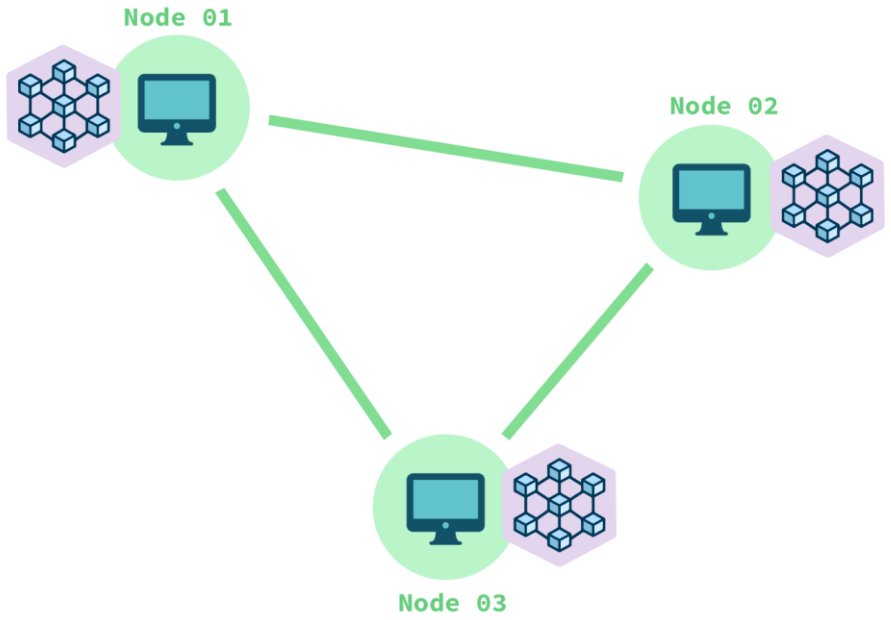
Piece of paper

- A wallet **generates and stores** private key, public key, address.
- You interact with the blockchain via the wallet.

Traditional transaction vs Crypto transaction

BISTEC
Hearts Academy





Data is in a **database**.

Data is **private**.

Centralized system.

Client-server system.

Bank is the trusted third party.

Data is in a **blockchain**.

Data is **public**.

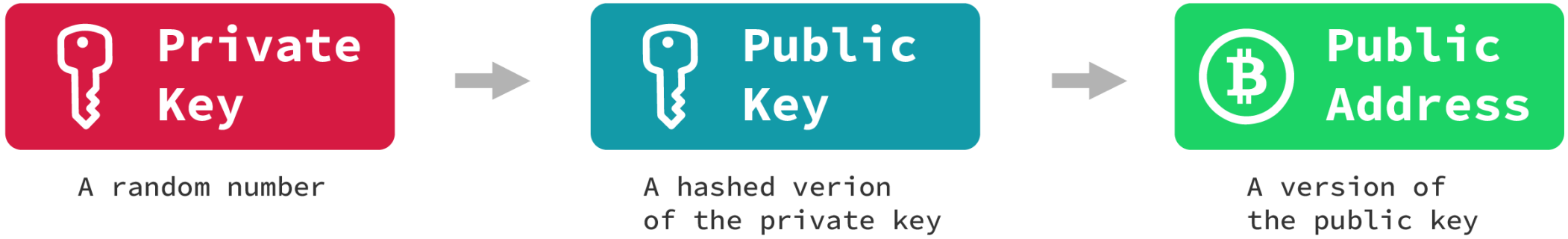
Decentralized System.

Peer-to-peer network.

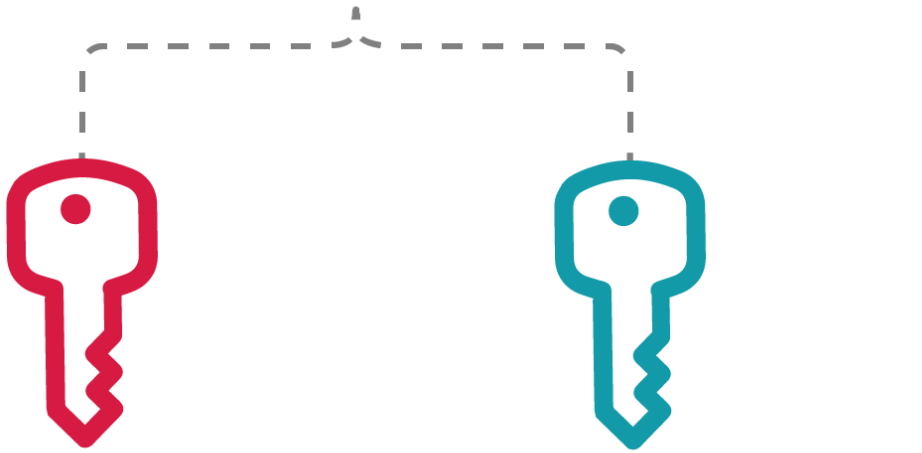
No trusted third party.

BISTEC
Hearts Academy

Public-private key pair

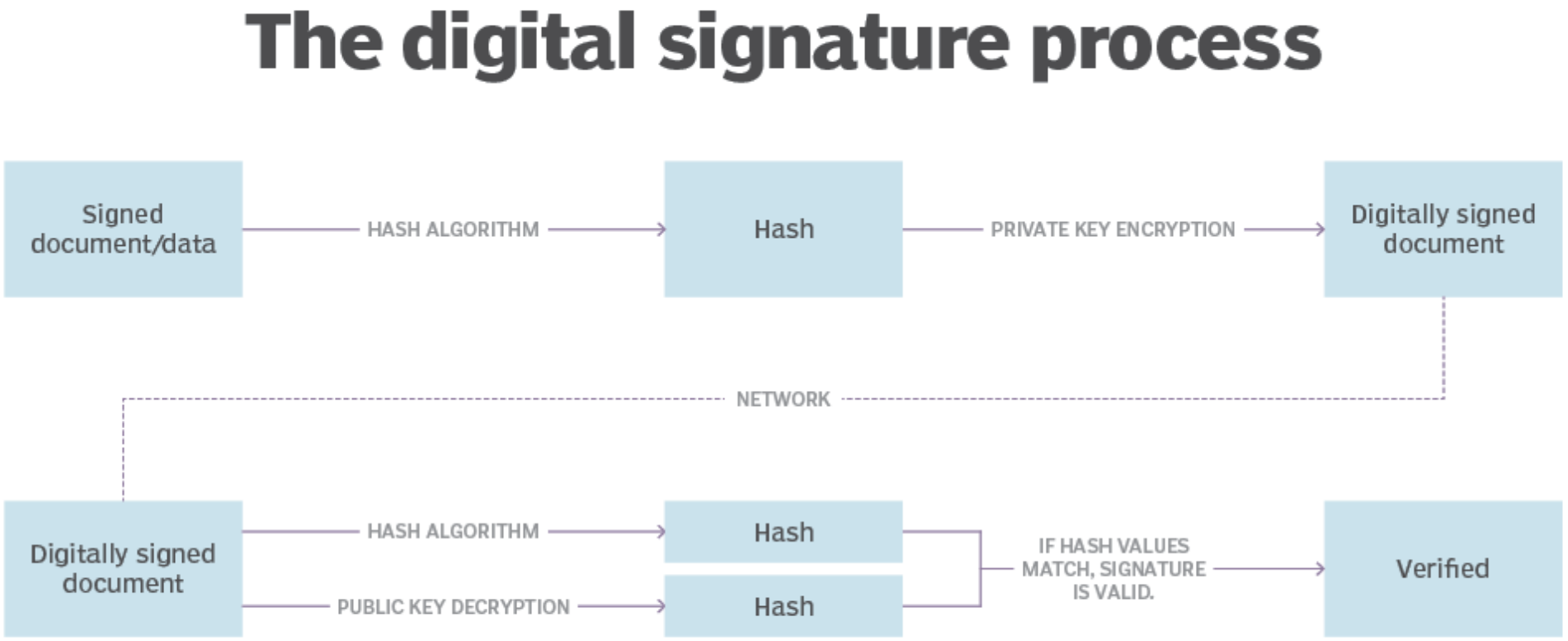


- Private key is **the fundamental part**.
- Public key and Public Address are created using private key.
- Private key **must be secret and secured.**
- Private key **cannot be recovered**.
- **If private key is lost, your crypto is lost.**



Digital Signature

BISTEC
Hearts Academy



Data is signed with private key, Verified with public key.

BISTEC
Hearts Academy

Let’s dig deep.

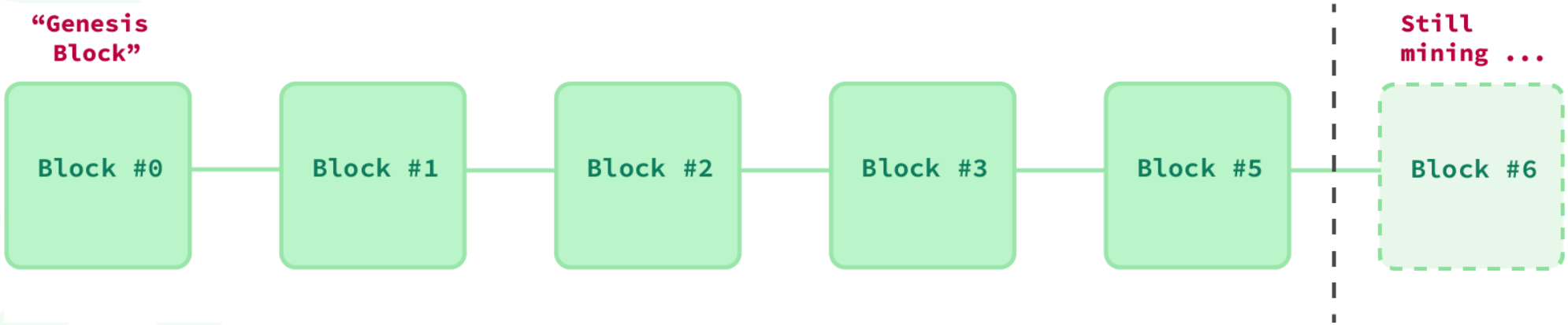
BISTEC
Hearts Academy

Core Concepts of Blockchain

Developer’s perspective of Blockchain.

What is Blockchain?

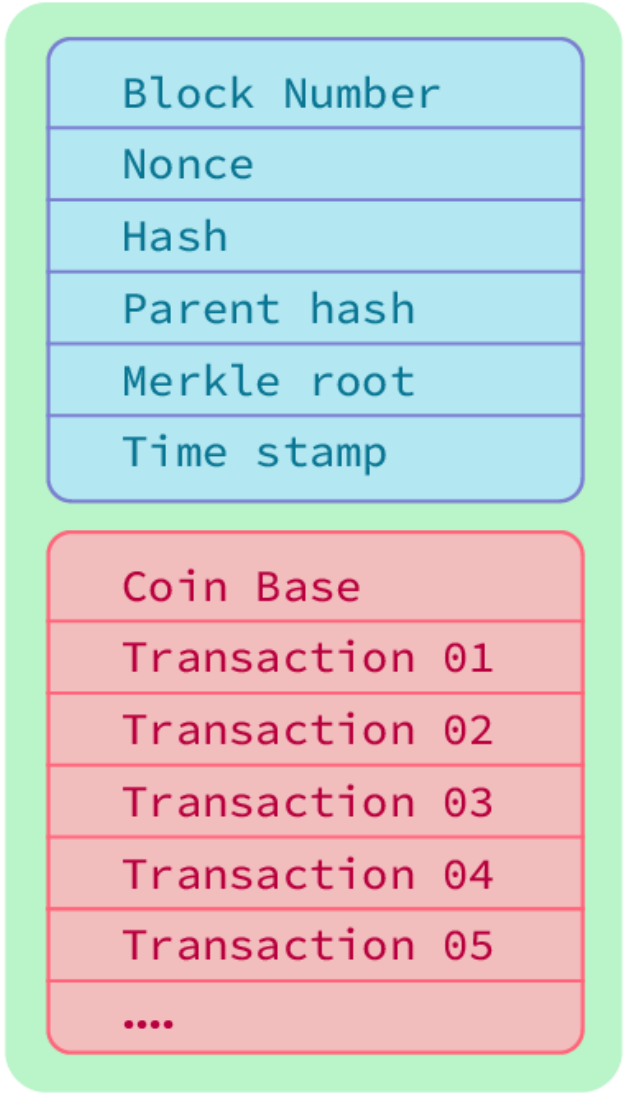
BISTEC
Hearts Academy



- **Immutable** – Create / Read only. Cannot update / delete data.
- **Distributed** – Data is distributed among everybody, equally.
- **Decentralized** – No central authority.
- **Uses cryptography** – To sign and verify data. Blocks are linked cryptographically.

Cryptographic Hash Function

- A hash function is a **one-way mathematical function**.
- Almost impossible to reconstruct initial data.
- A minor change to the original data alters hash value drastically. (Avalanche effect)
- Having same hash for two different inputs is extremely unlikely.

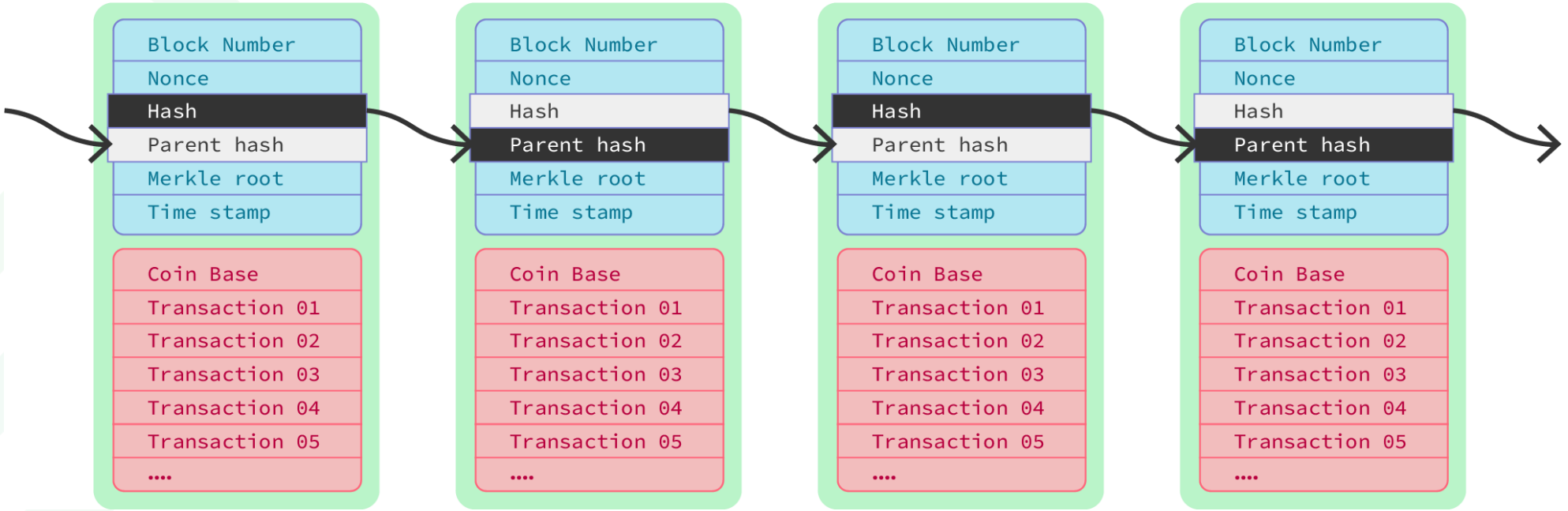


Block

- A block consists of **header and a long list of Transactions**.
- Each block within the blockchain is identified by a **hash**.
- First block of the blockchain is called **“genesis block”**.

BISTEC
Hearts Academy

How are blocks linked?



- Blocks are **linked by the block hash**. These are cryptographic links.
- Blockchain is **append-only**. Blocks are appended in a chronological order.

Mining / Difficulty

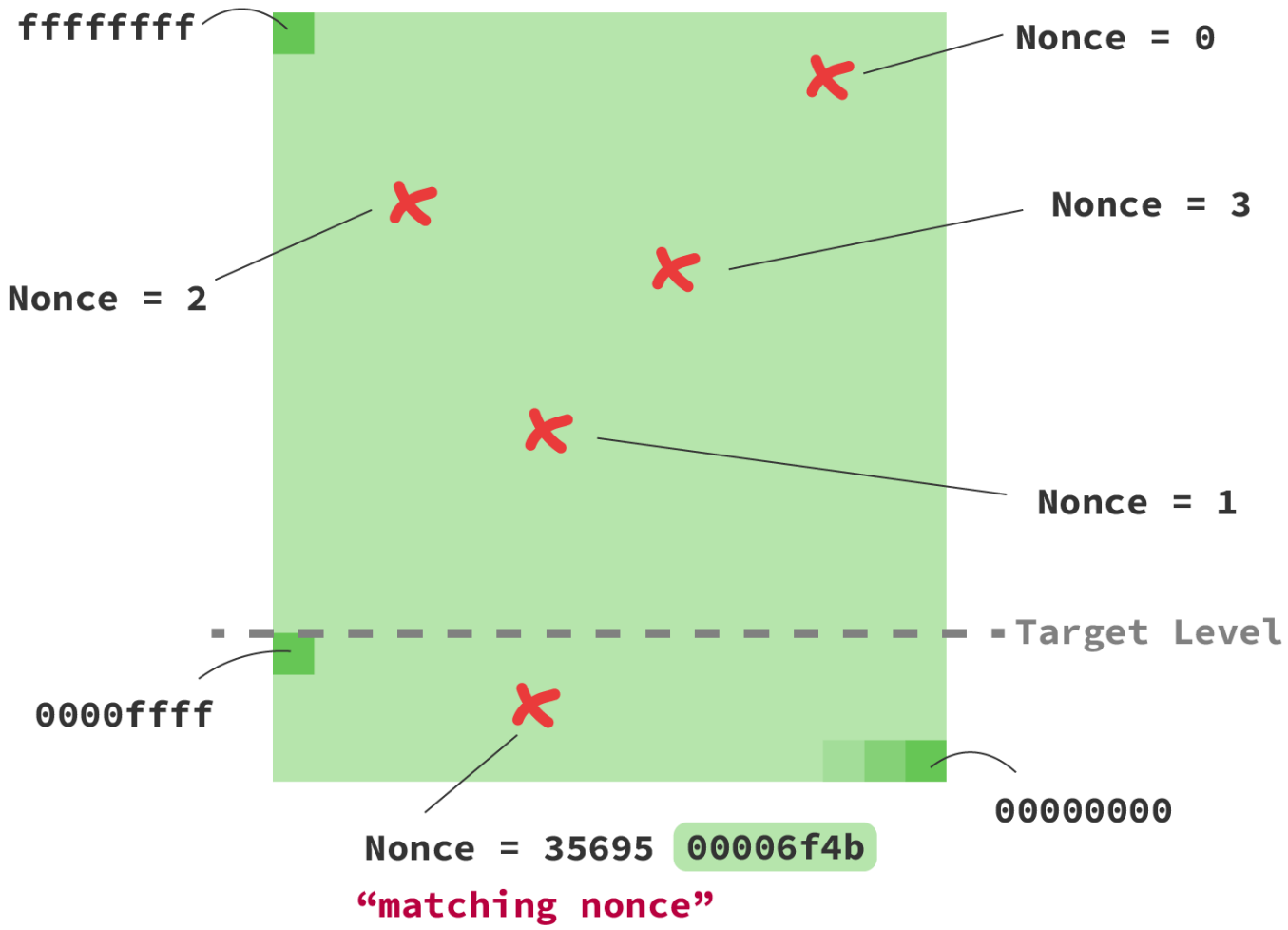
BISTEC
Hearts Academy

```
hash("Satan, prince of this world" + "some nonce") = 99e9ba071ac7040f04ea8d8f303b1a3c349a6e0b

hash("Satan, prince of this world" + "other nonce") = 278ceb29e11cb9e9c8d37af74730fb6faa185757

hash("Satan, prince of this world" + ????????) < 00000000000000000000000001231231 # Very difficult
```

- **Solving cryptographic puzzle** to create a new block is called “Mining”.
- **Nonce = Number only used Once**
- The nonce is the number which miners are solving for.
- Difficulty level is determined by **leading zeros**.
- Difficulty is **increased exponentially** with the number of leading zeroes.



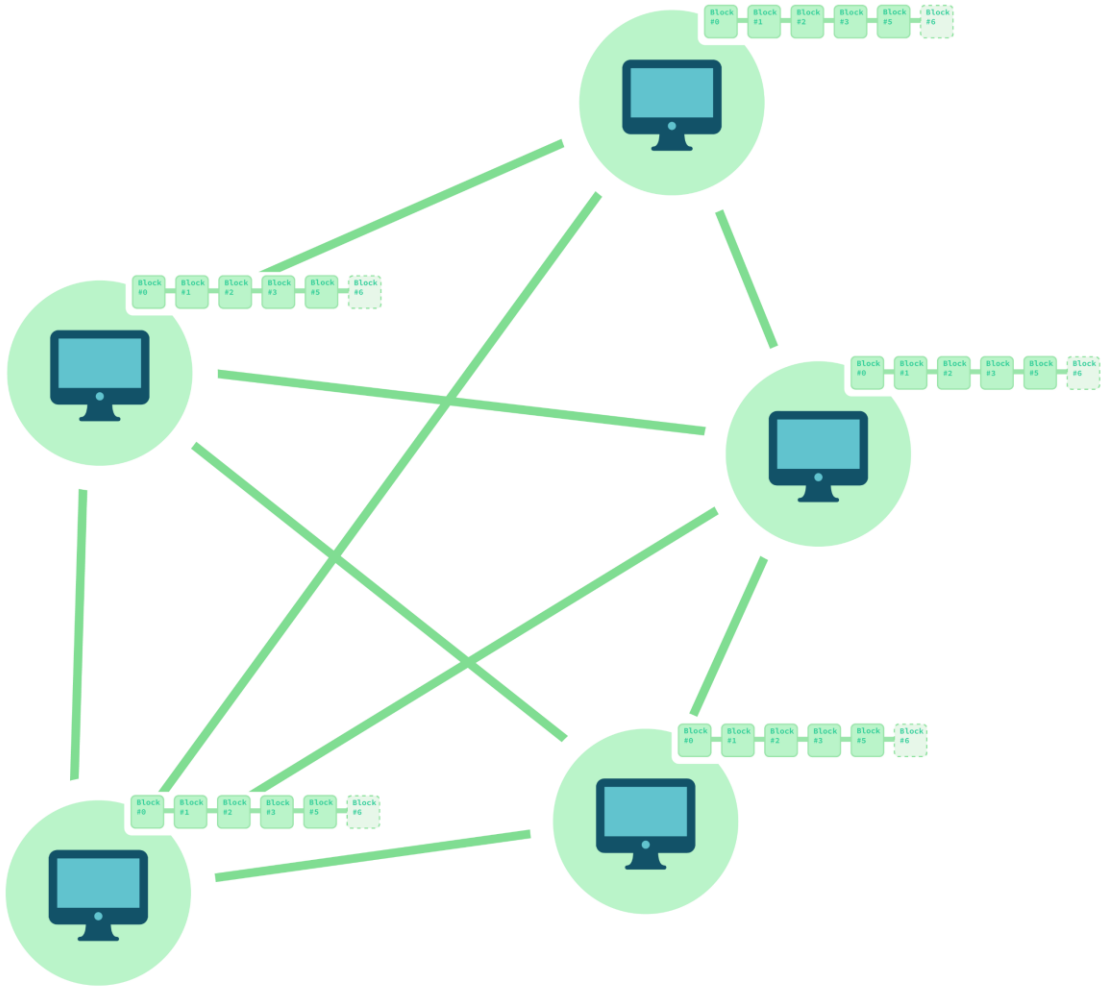
ffffffff = 4’294’967’295

0000ffff = 65’535

$$\frac{\texttt{ffffffff}}{\texttt{0000ffff}} = 0.000015$$

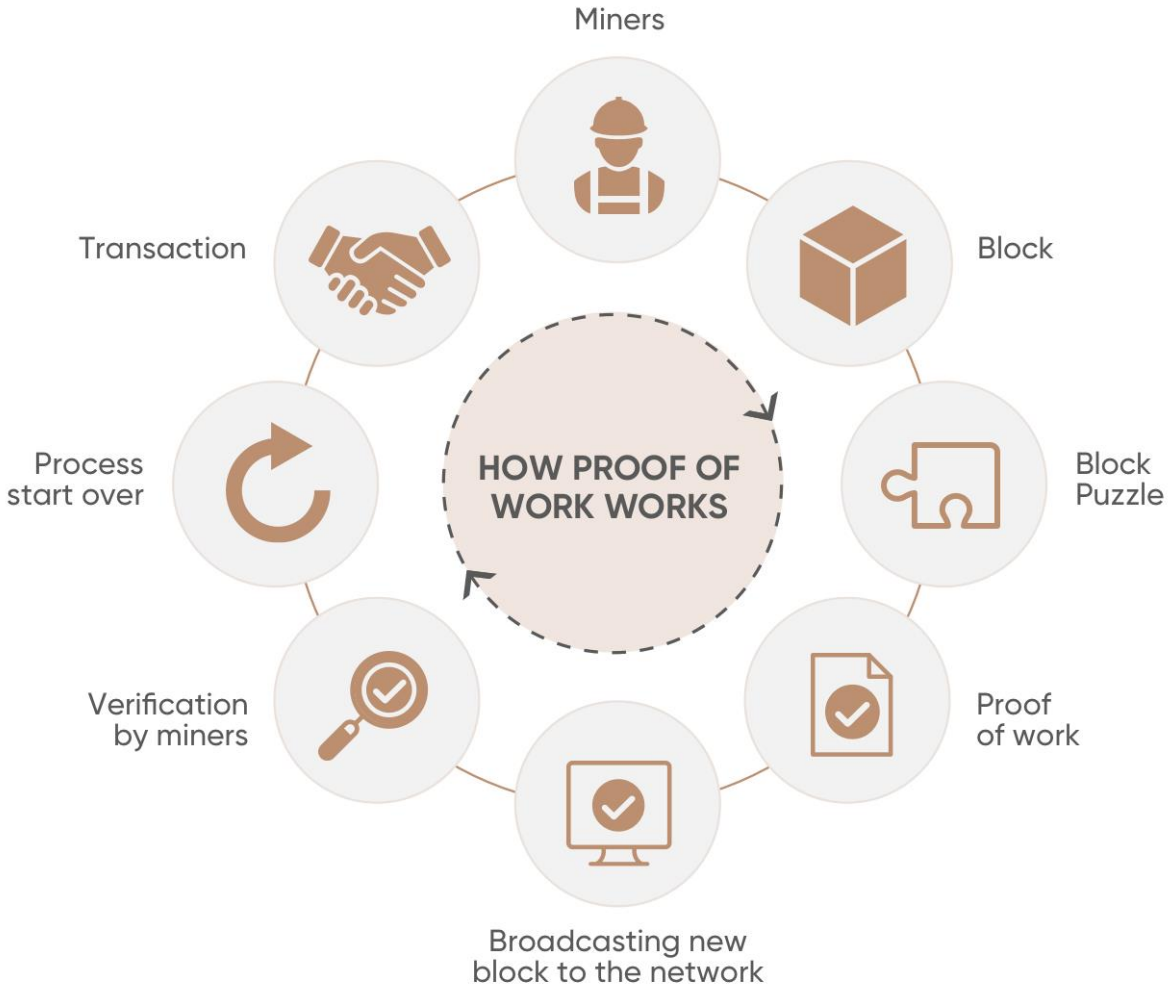
$$\frac{\texttt{ffffffff}}{\texttt{0000ffff}} \times 100\% = 0.0015\%$$

Difficulty increases exponentially.



Blockchain Network

- **Peer-to-peer network**.
- Every node gets an **exact same copy** of the blockchain. (distributed)
- Every node has **equal permissions and responsibilities**. (distributed)
- **No central authority** to manage the state of the blockchain. (decentralized)



Consensus protocol

- Not having a central authority cause a problem. **How to determine the state of the data?**
- Nodes must collectively decide the state of the data.
- Nodes don't / cannot trust each other.
- Nodes come to an agreement / consensus according to the consensus protocol.
- **Proof-of-Work** / **Proof-of-Stake**

BISTEC
Hearts Academy

Let's write our first smart contract using Remix IDE

gayashan4lk/solidity-first-contract (github.com)

The Web 3.0 Developer Road Map.

BISTEC
Hearts Academy

Web 2.0 Skills

Fundamentals of Blockchain

Ethereum & Smart Contracts

Solidity & Web3 Development Tools

Dapps (Decentralized Applications)

Enterprise blockchain solutions

First mile

Second mile

Third mile

BISTEC
Hearts Academy

Thank You.