Computer Science 3A

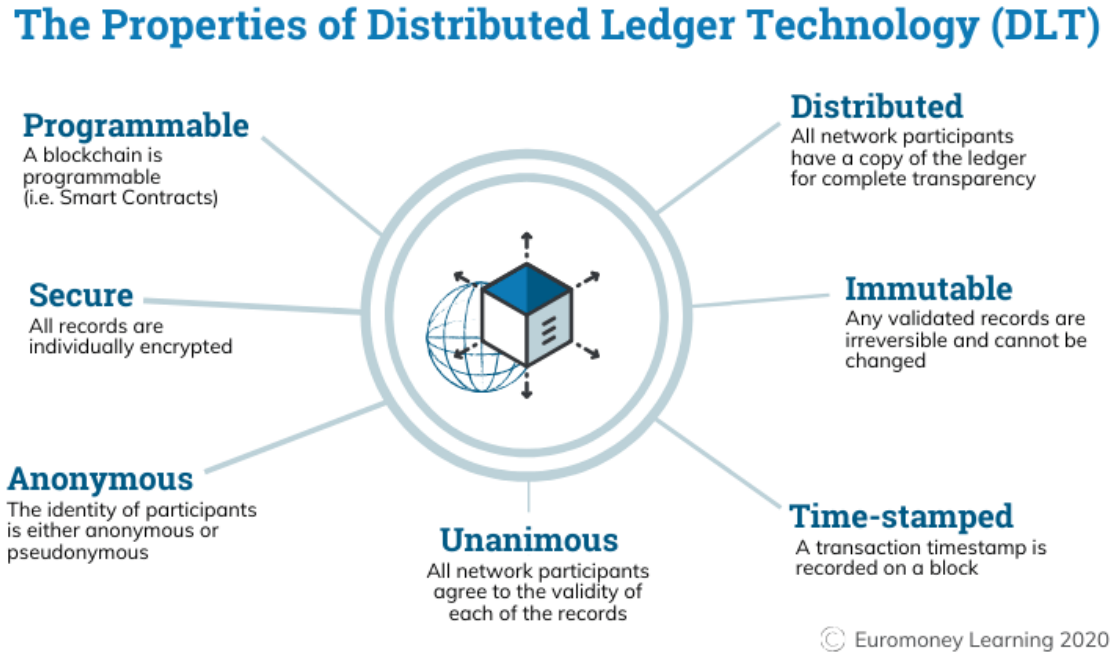
Mini Project Guidelines Video

18 March 2021

UNIVERSITY OF JOHANNESBURG

What is a Blockchain?

- A system of recording information in a way that makes difficult or impossible to change, hack or cheat the system.

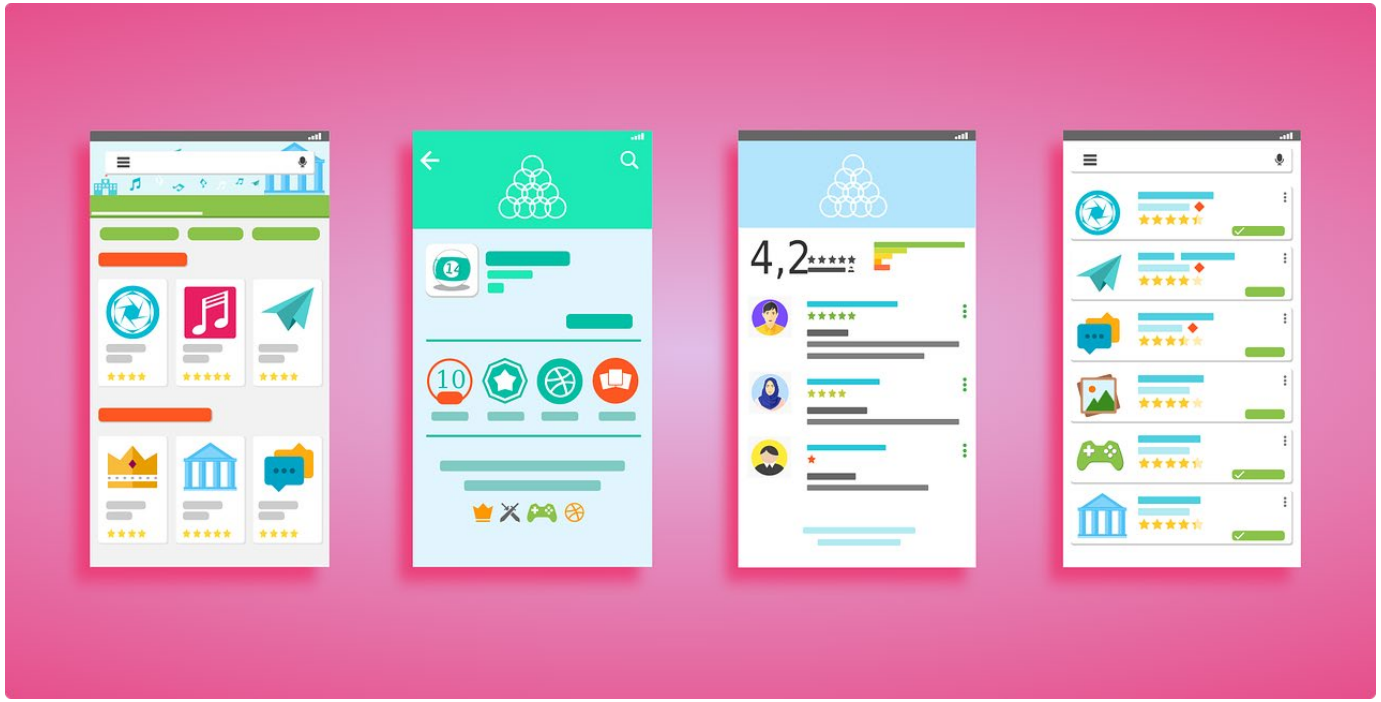


What are the components of a Blockchain (in the mini project)

- User Interface
- Record
- Block
- Network
- Block verification
- Blockchain Example

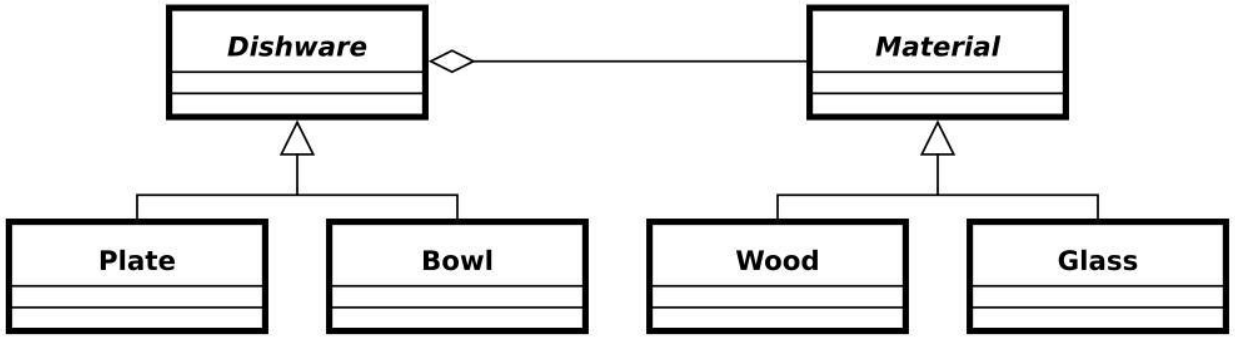
User Interface

- Provides mechanism for users to use the system
- Can take user input
- And display system output



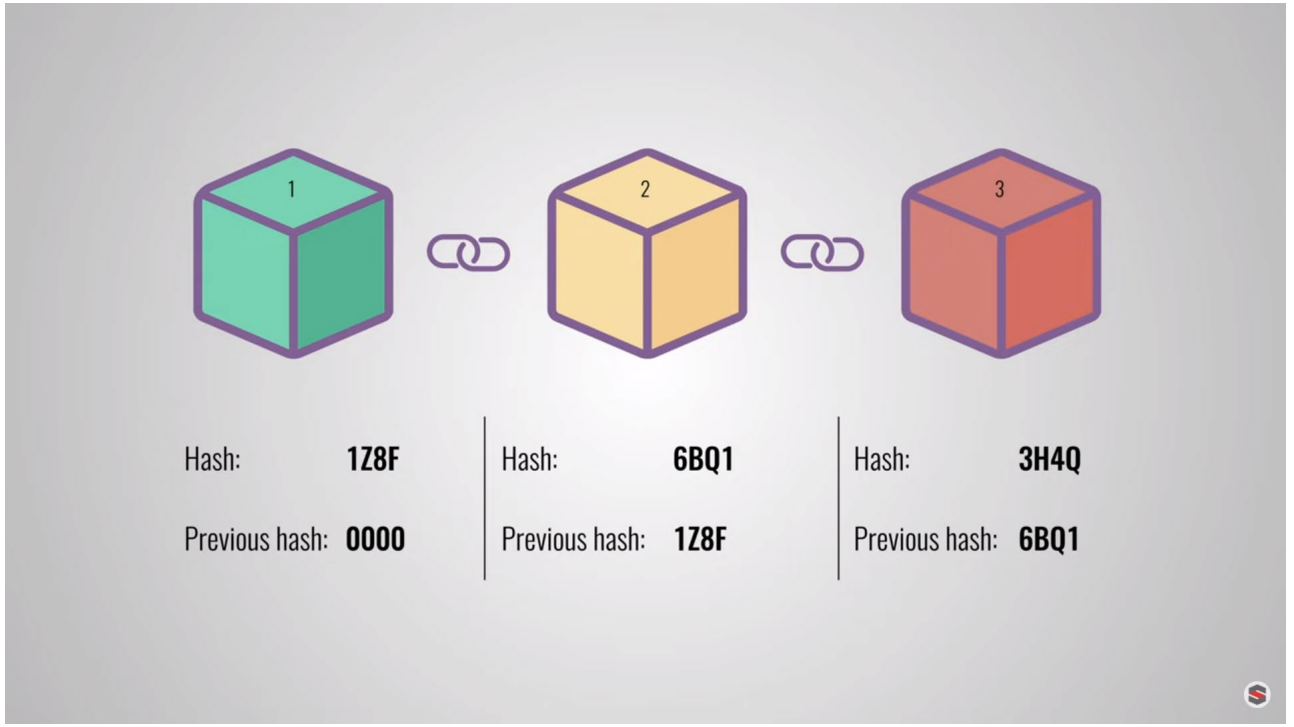
Records

- Depends on use case but is just like an object and typically includes:
  - State
  - Behaviour (if smart contract)



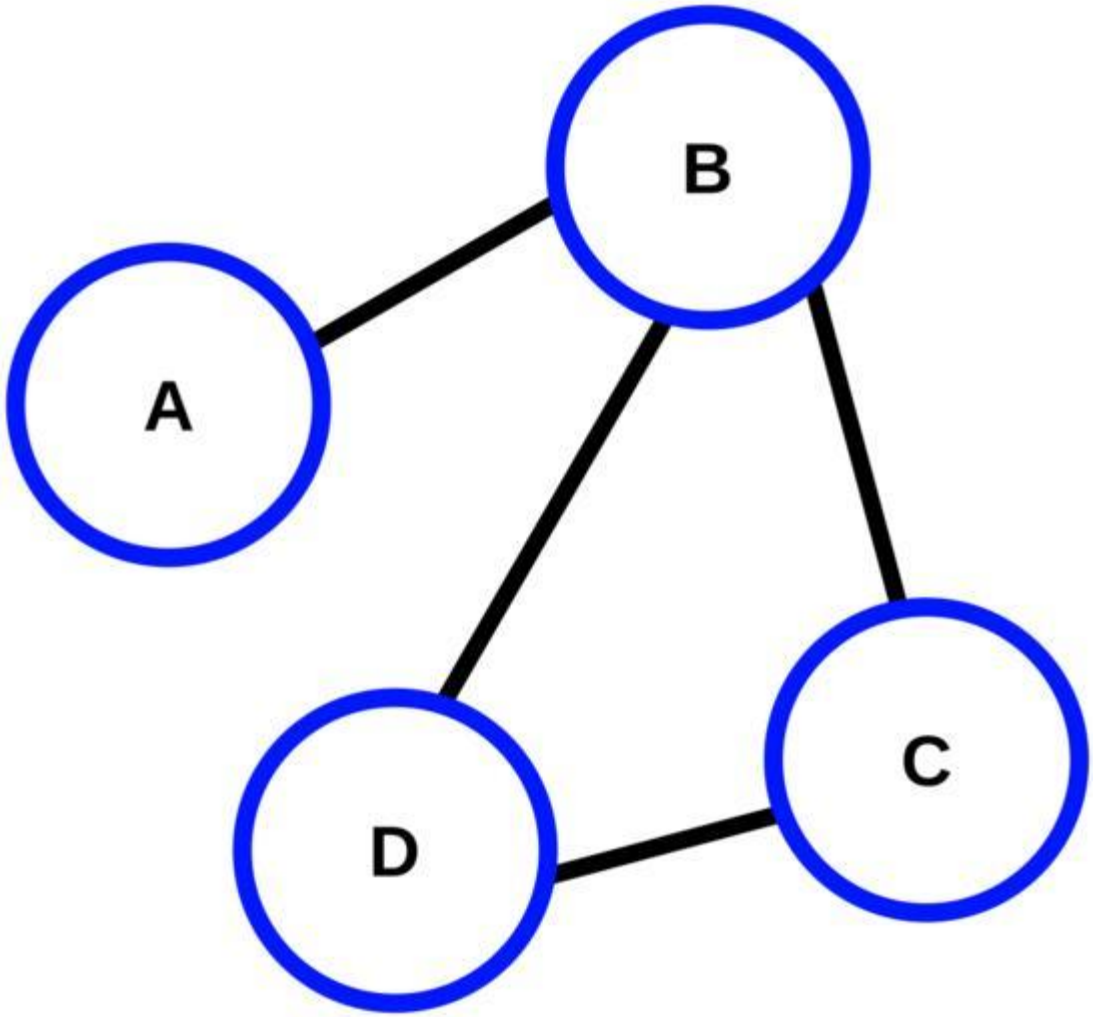
Blocks

- Each blocks contains:
  - Data (record - sometimes encrypted with private key)
  - Hash (or nonce)
  - Hash of previous block (0000 for genesis block)



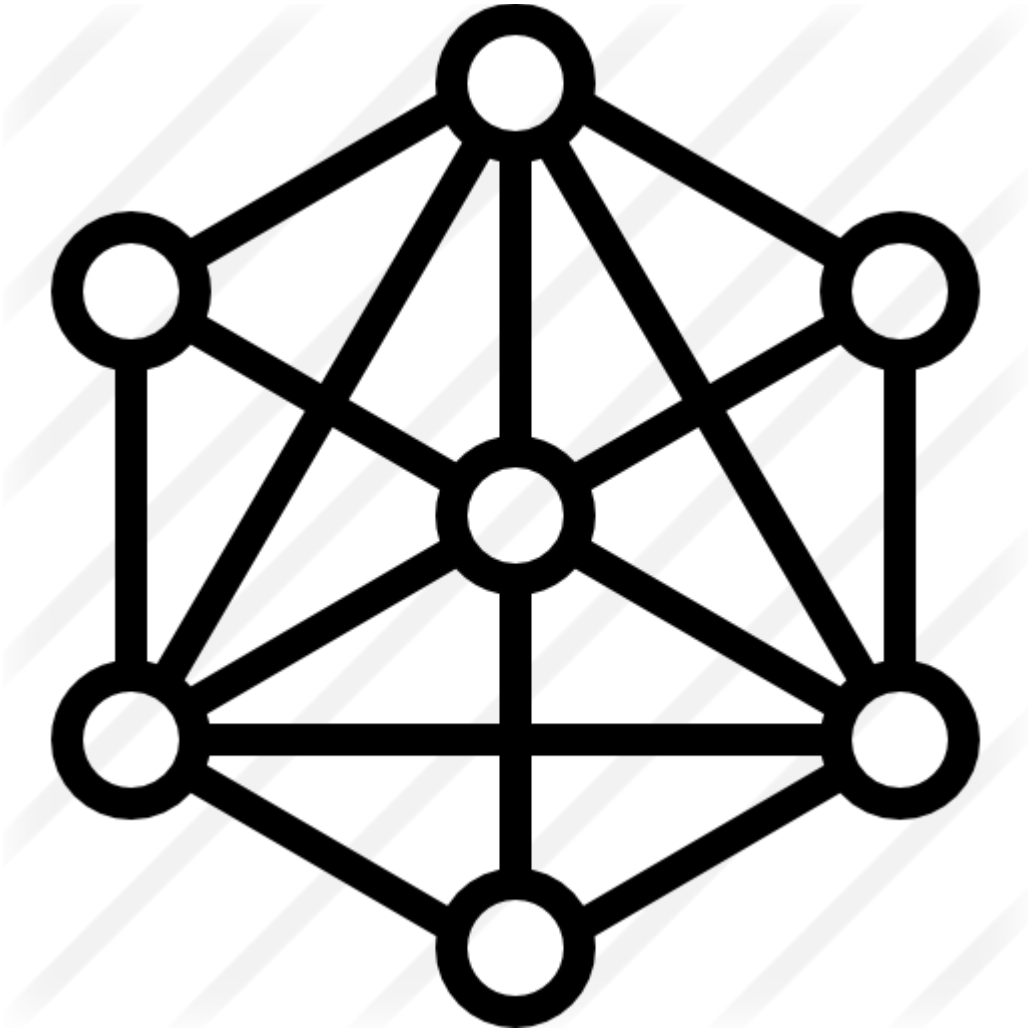
Network

- The collection of clients or users in the system
- In the mini project this is abstracted as a Graph, where nodes are clients and edges are connections between clients



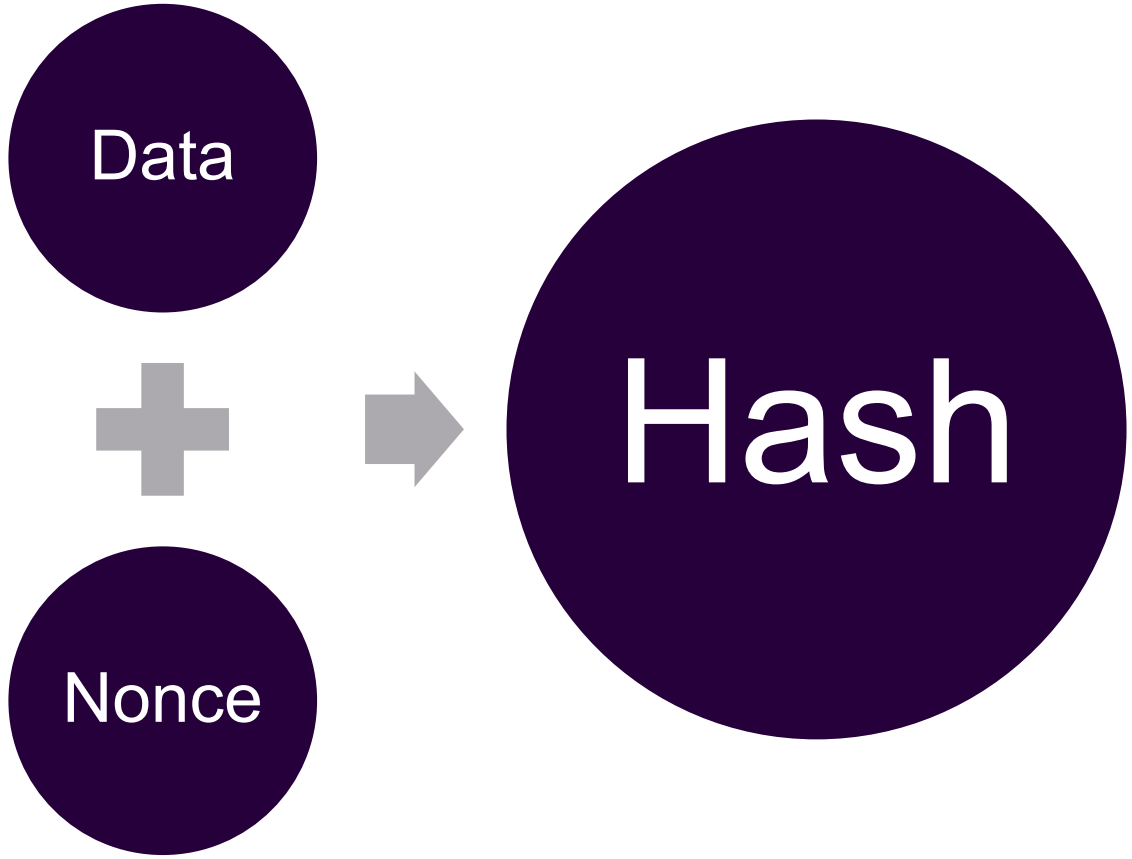
Block verification

- For a block to be added to the blockchain it needs to be verified or vetted
- Each client can in the blockchain can potentially do this
- A proof of work or proof of stake algorithm is used



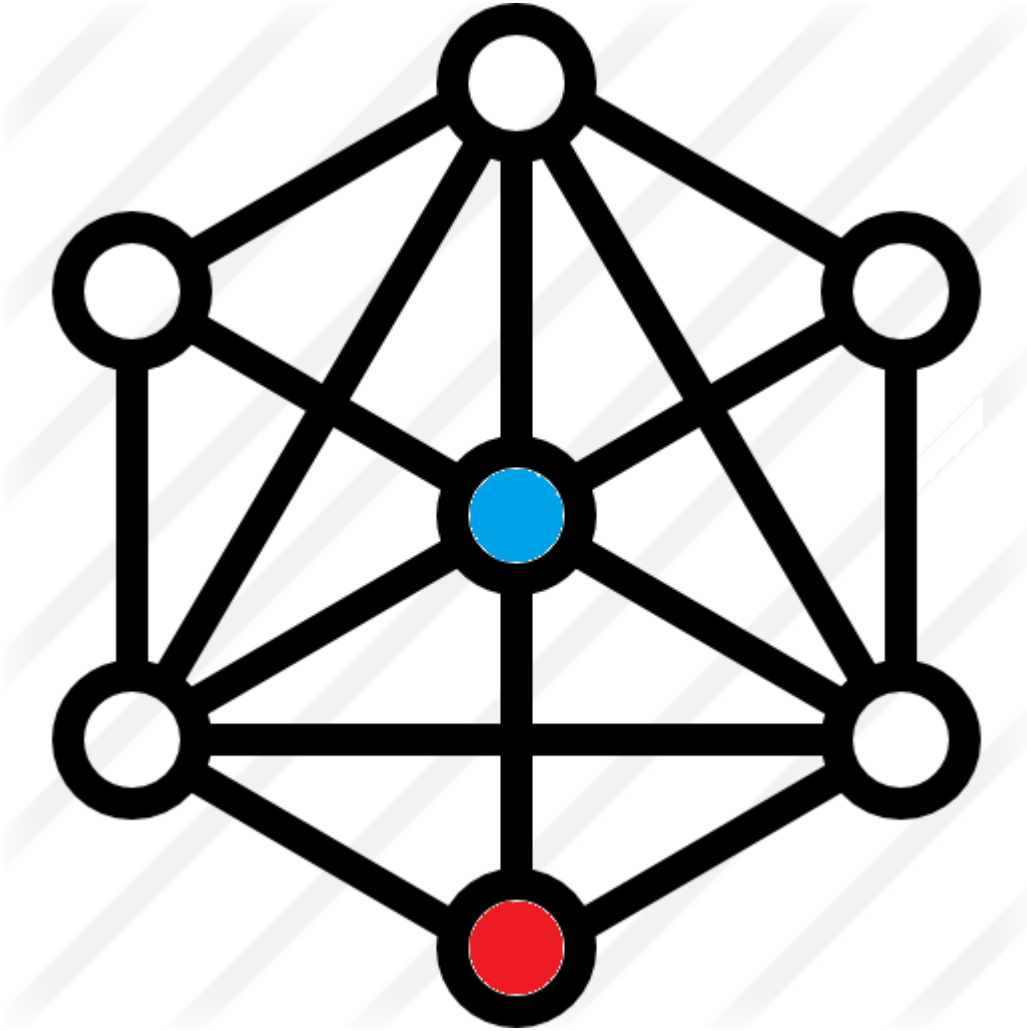
Block verification II

- Algorithm categories of PoW:
  - Challenge-response
  - Solution-verification
- List of functions:
  - Hashcash
  - Diffie–Hellman–based puzzle
  - Cuckoo Cycle
  - Other puzzles



Block verification III

- For proof of stake:
  - Each block to be added is prioritized
  - One client is randomly elected to verify the block in the network
  - If another two clients disputes a verified block that client is penalised



Blockchain Example

- Client Types:
  - Wine farm
  - Retailers

Blockchain Example II

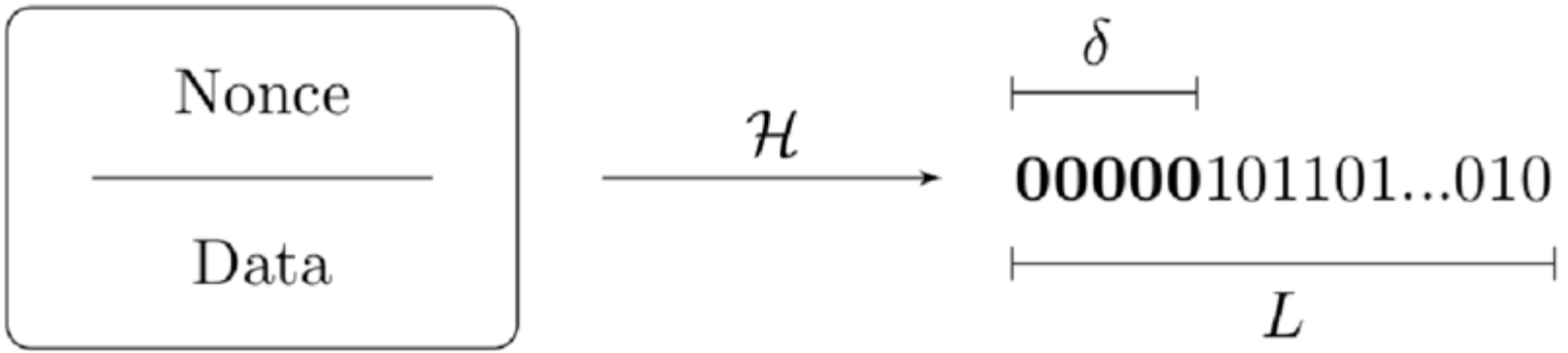
- Record:
  - Record Type (order or offer)
  - Name
  - Wine Type
  - Vintage year
  - Price
  - Volume
  - timestamp
  - *discount(int volume)*

Blockchain Example III

- Block creation
  - Data
  - Hash
  - Previous hash

Blockchain Example IV

- Block distribution
- Block verification
  - PoS
  - Hashcash
- Blockchain update
  - Each block is added to each client's blockchain



Blockchain Example V

- Querying the blockchain
  - Start at genesis block
  - Inspect block
  - Logic
  - Dispute?
  - Traverse to next block