Features of Blockchain

The Problem

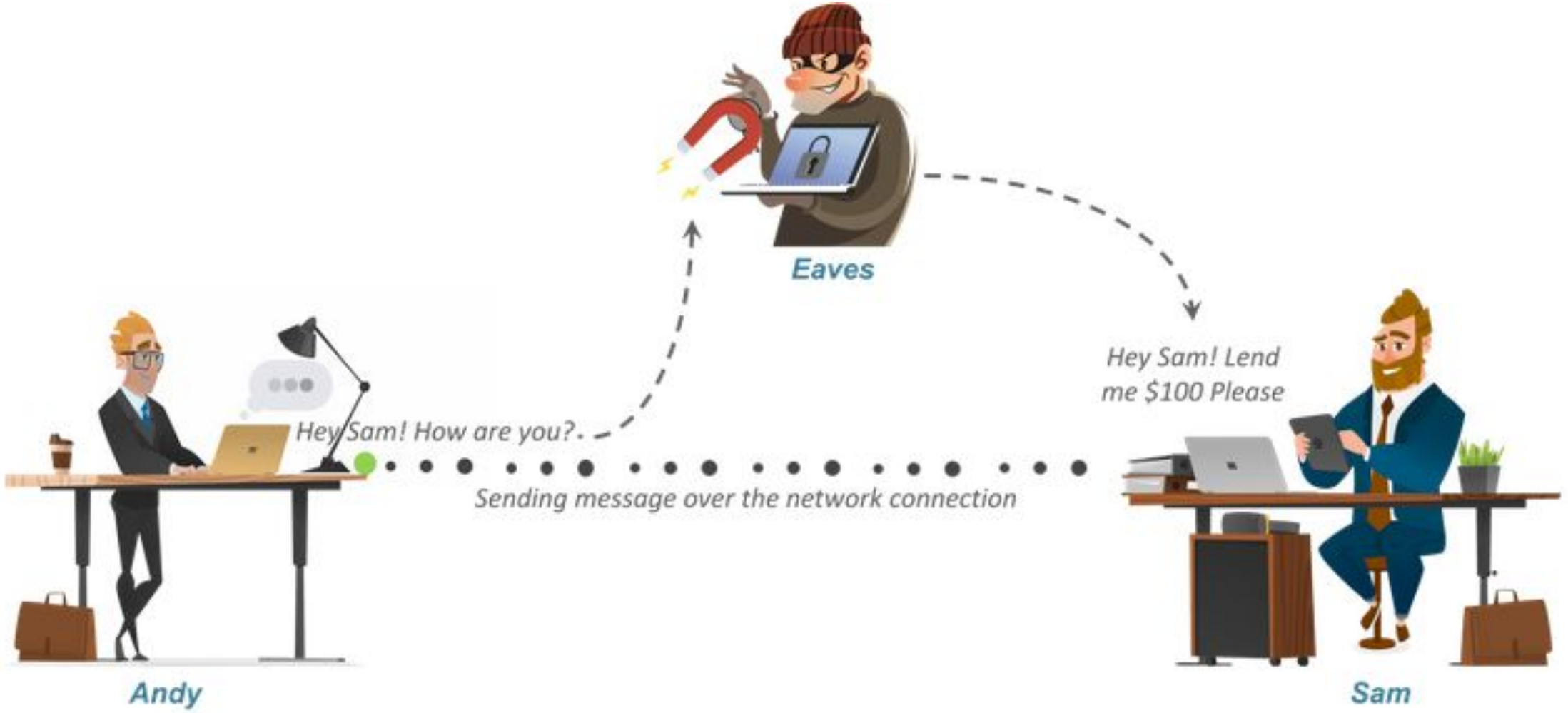
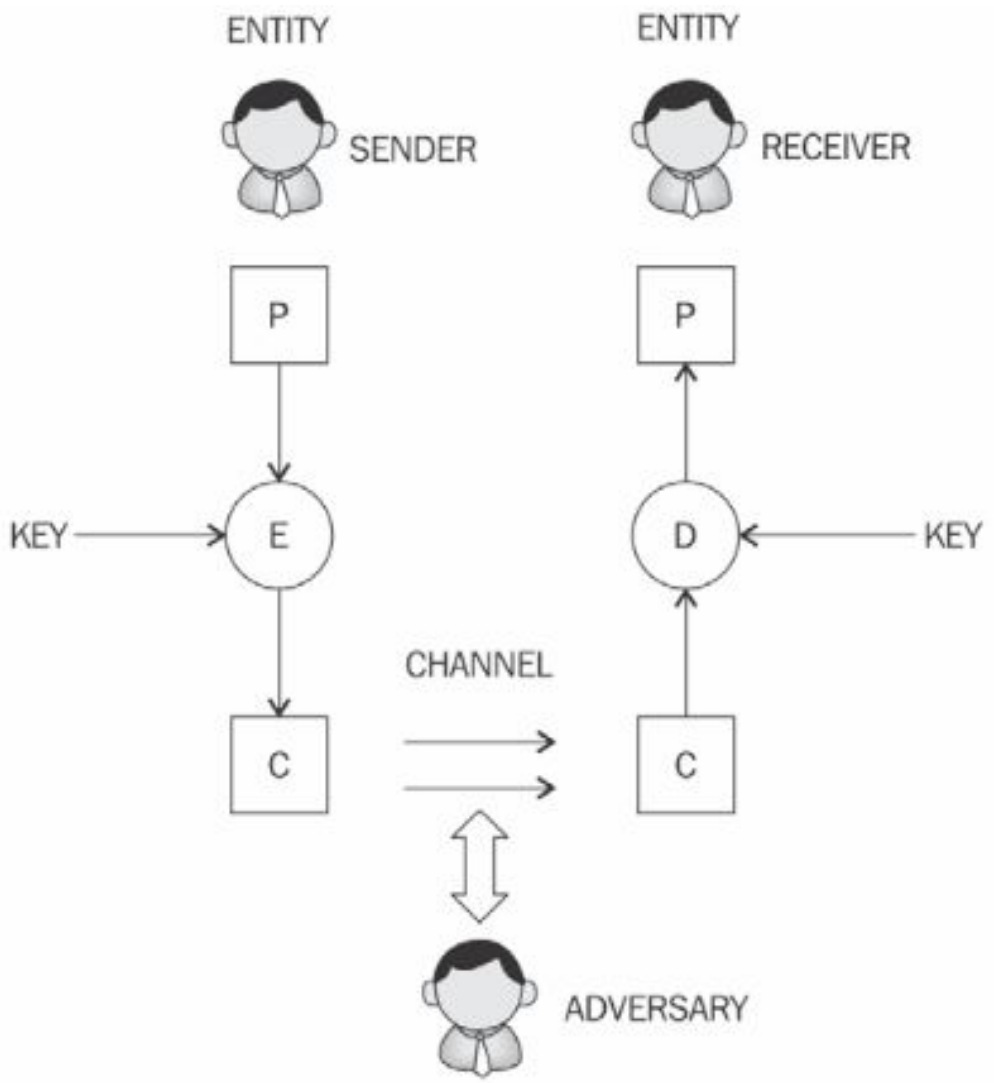


Image Source: https://www.edureka.co/blog/what-is-cryptography/

Cryptography

Cryptography *is the practice and study of and data in the presence of adversaries*



Solution

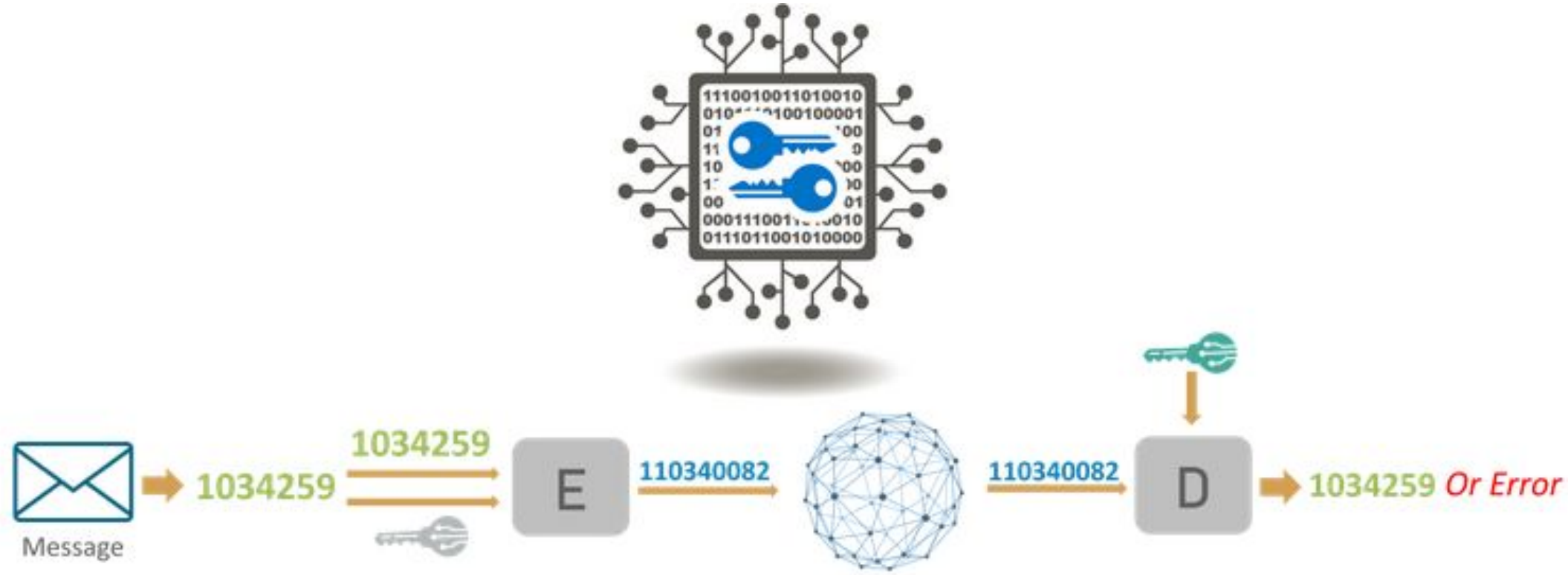


Image Source: https://www.edureka.co/blog/what-is-cryptography/

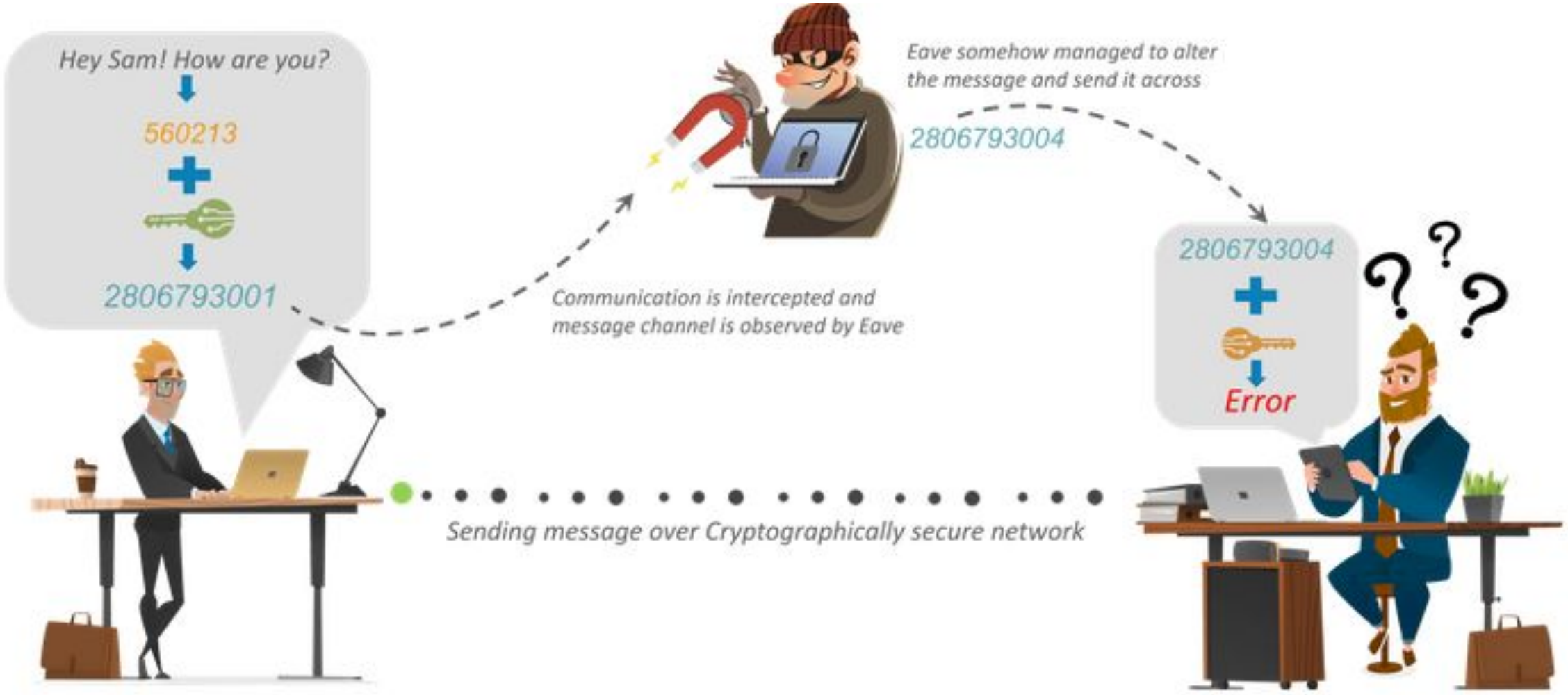
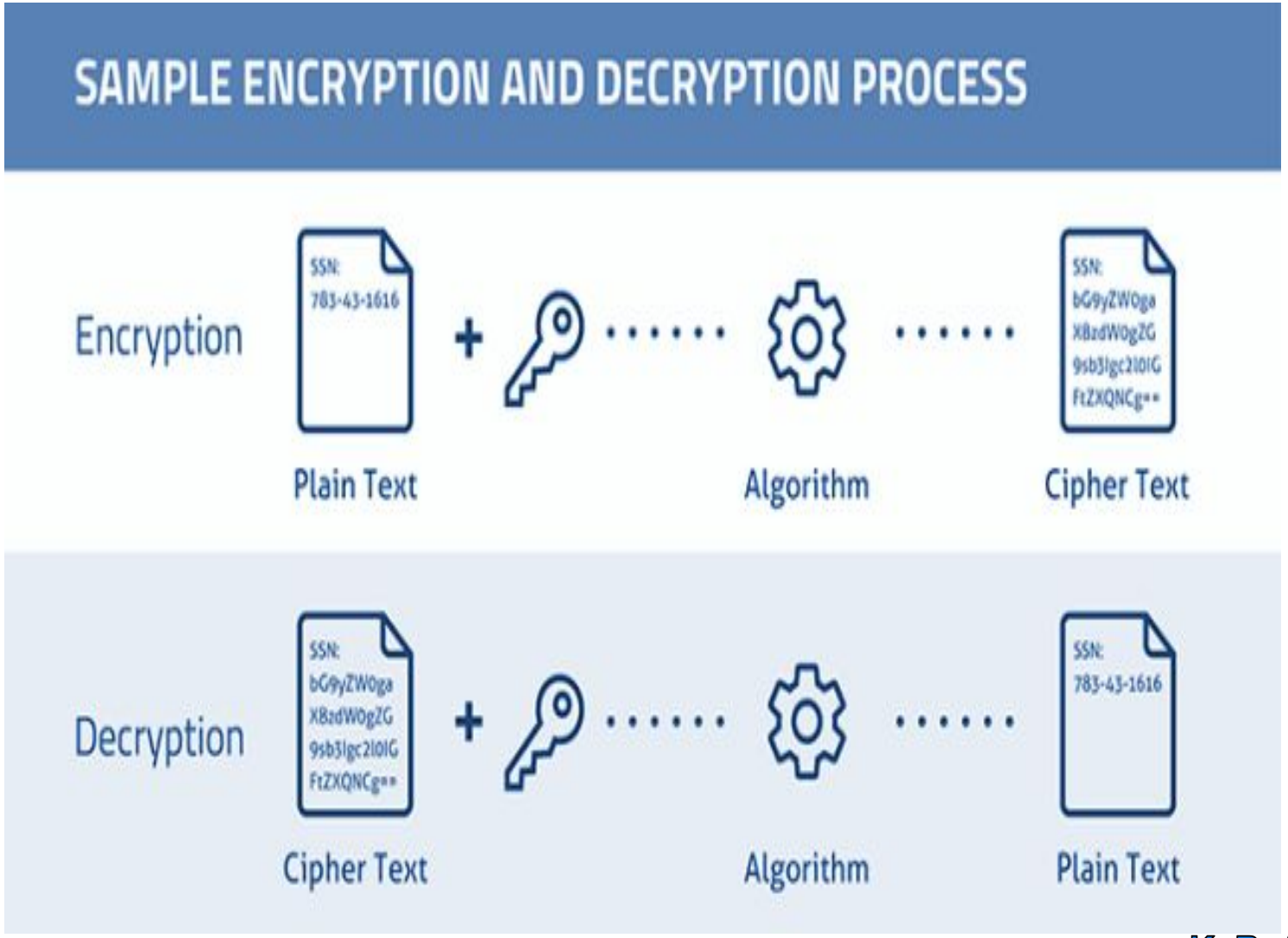


Image Source: https://www.edureka.co/blog/what-is-cryptography/

Terminologies

- Encryption
- Key
- Decryption
- Cipher



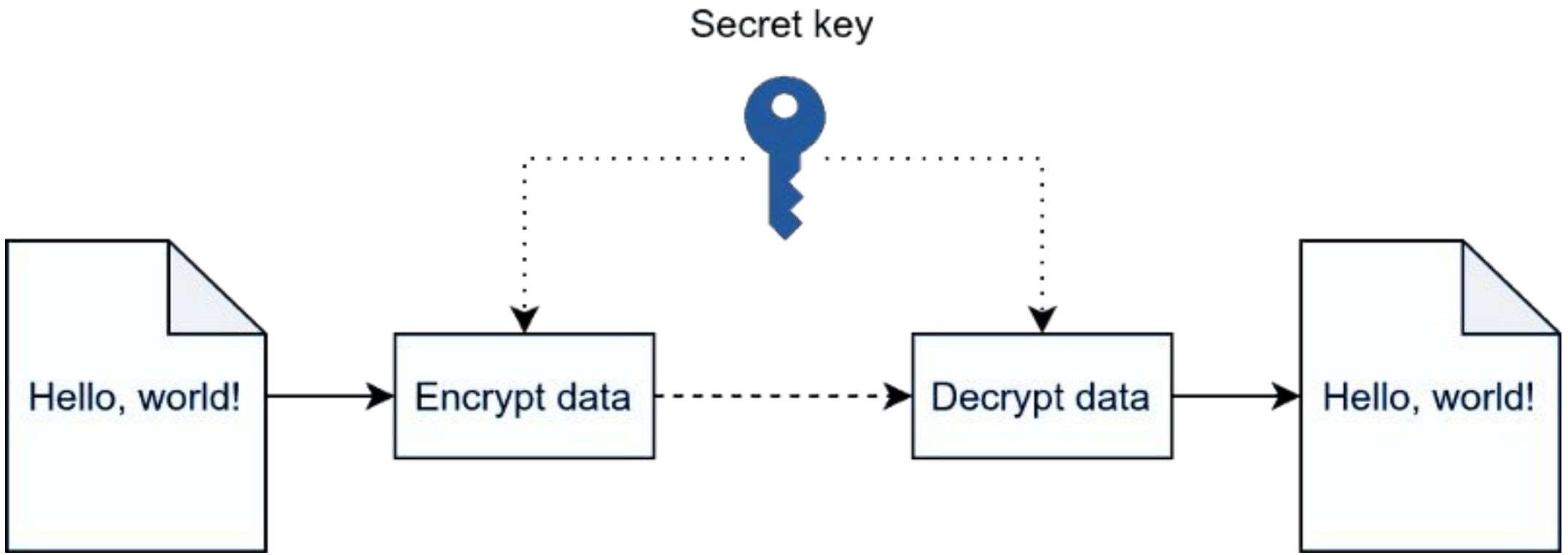
Cryptography

Security Services Provided by Cryptography

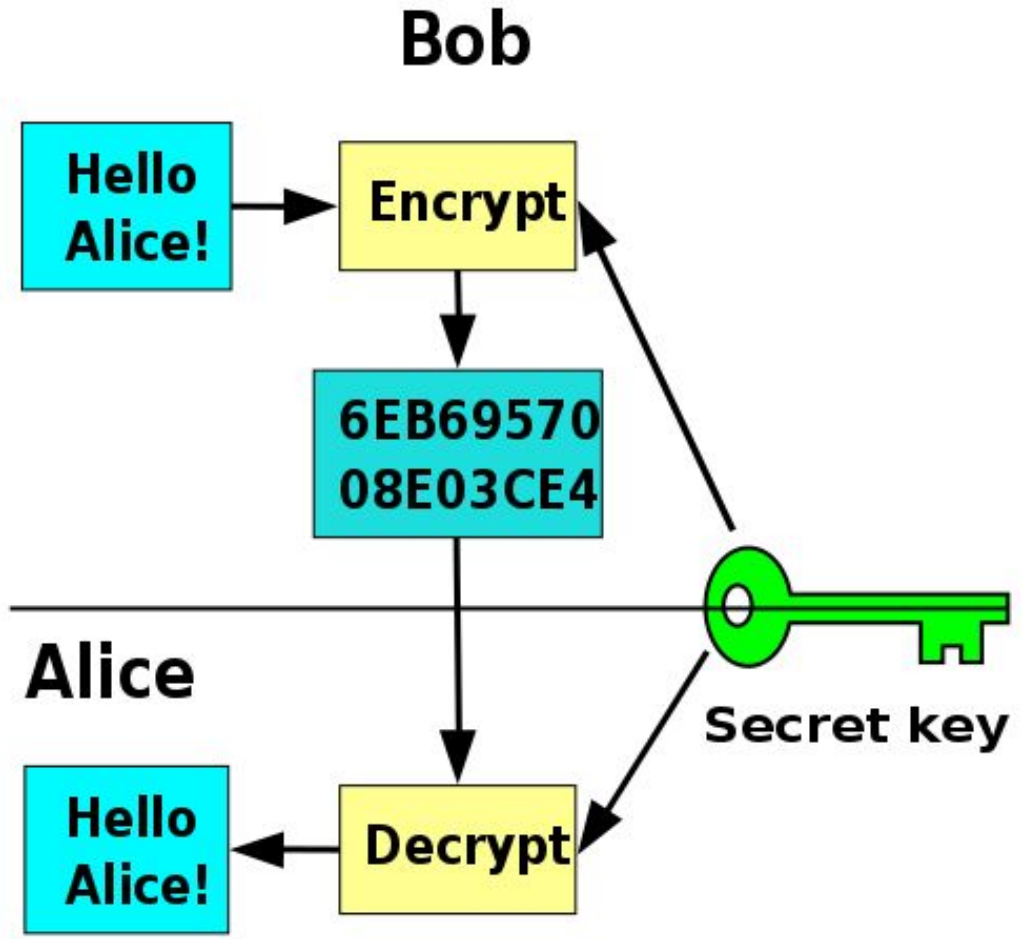
- **Confidentiality**
  - to protect the data or information being accessed by unauthorized entities
- **Data Integrity**
  - makes sure the information is not altered
- **Authentication**
  - provides the identification of the originator
- **Non-Repudiation**
  - assurance that some one cannot deny the ownership of the data shared

Types of Cryptography: Symmetric-Key Cryptography

- Symmetric-Key Cryptography / Private Key Cryptography

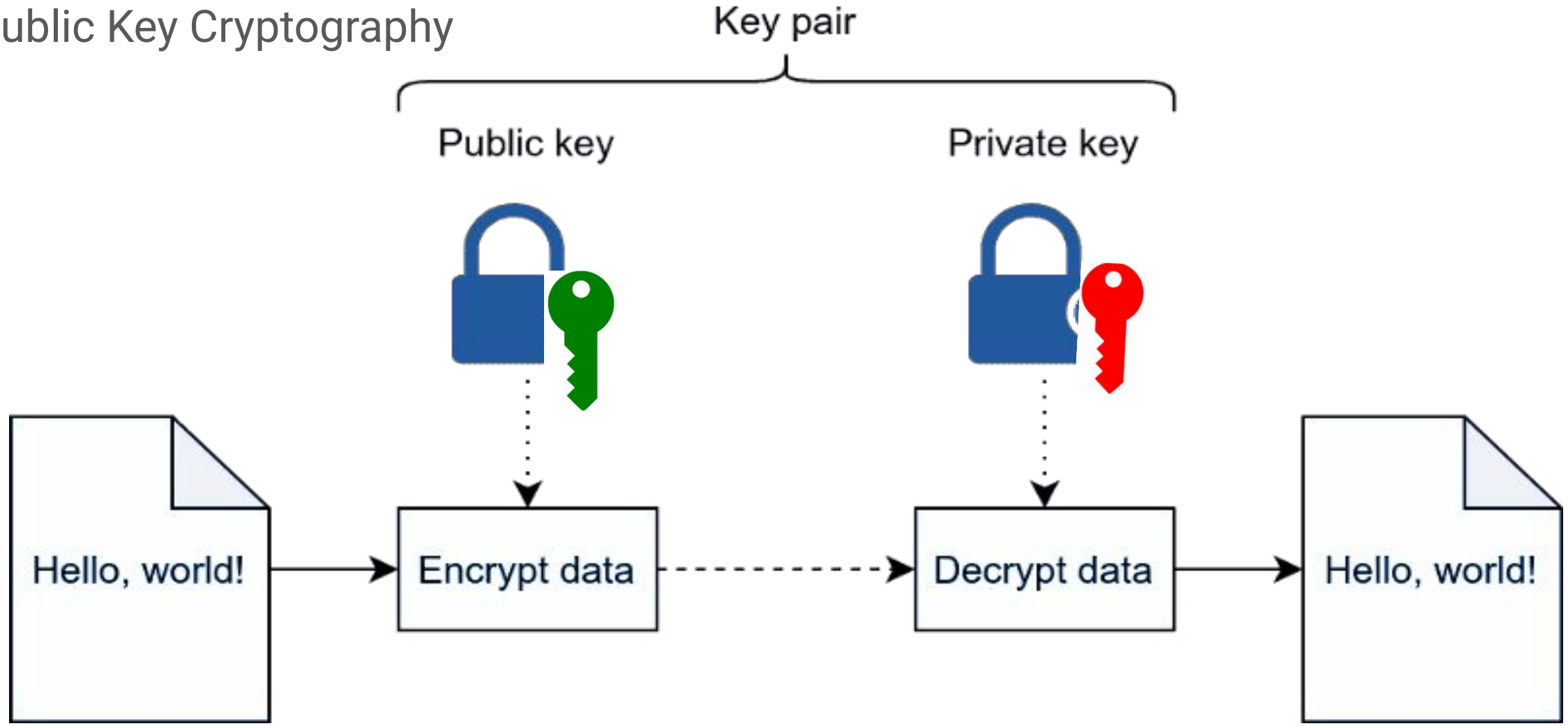


Symmetric-Key Cryptography

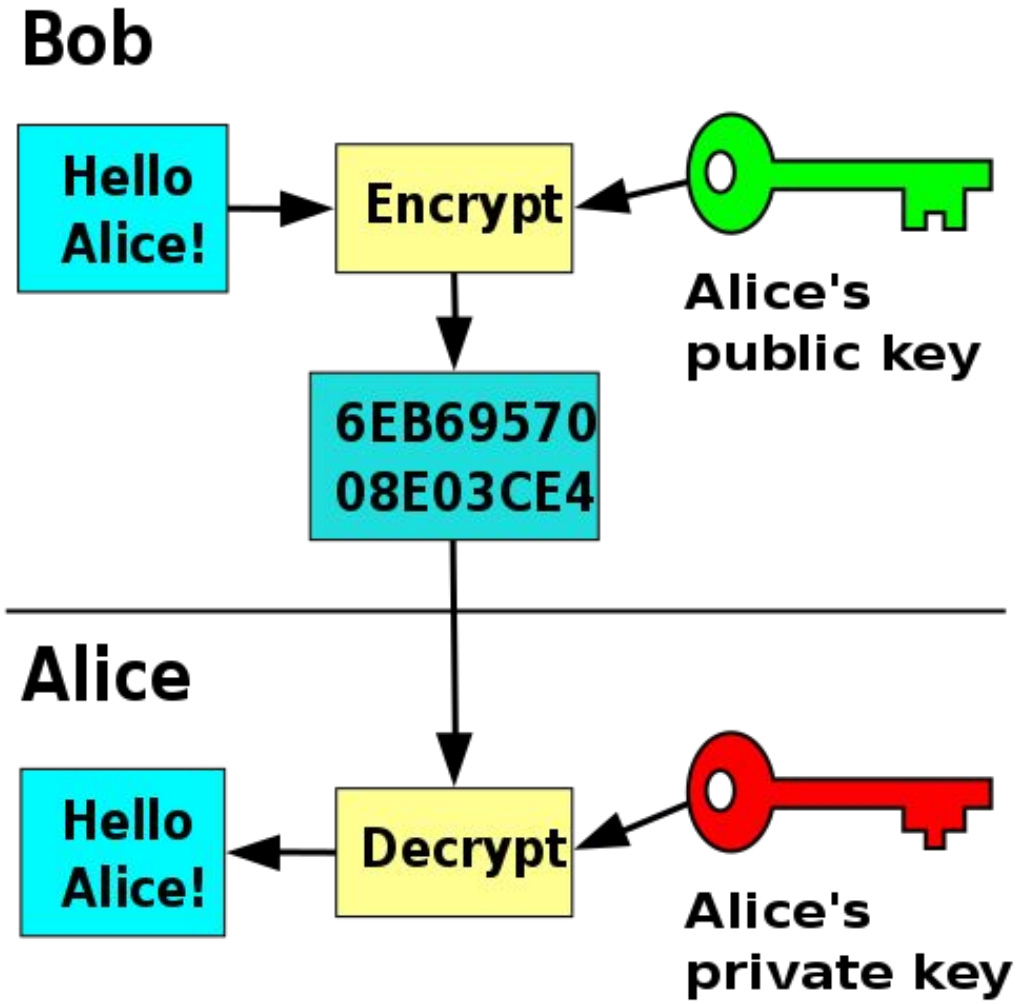


Types of Cryptography: Asymmetric-Key Cryptography

Public Key Cryptography



Types of Cryptography: Asymmetric-Key Cryptography



Hash Function

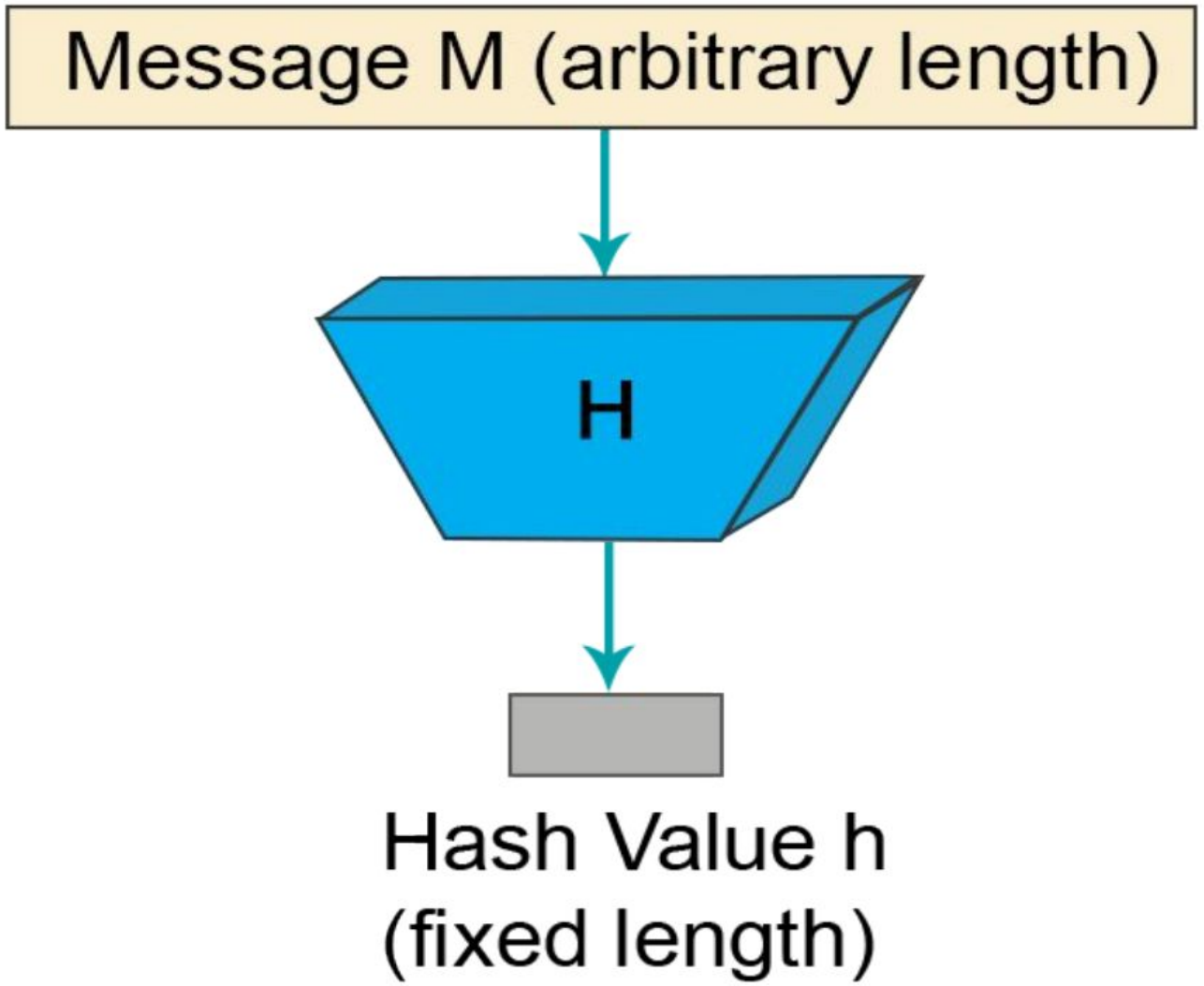
Hash functions ***compress*** arbitrary messages into ***fixed-length*** digests

They are ***easy*** to compute

Hash functions are ***keyless***

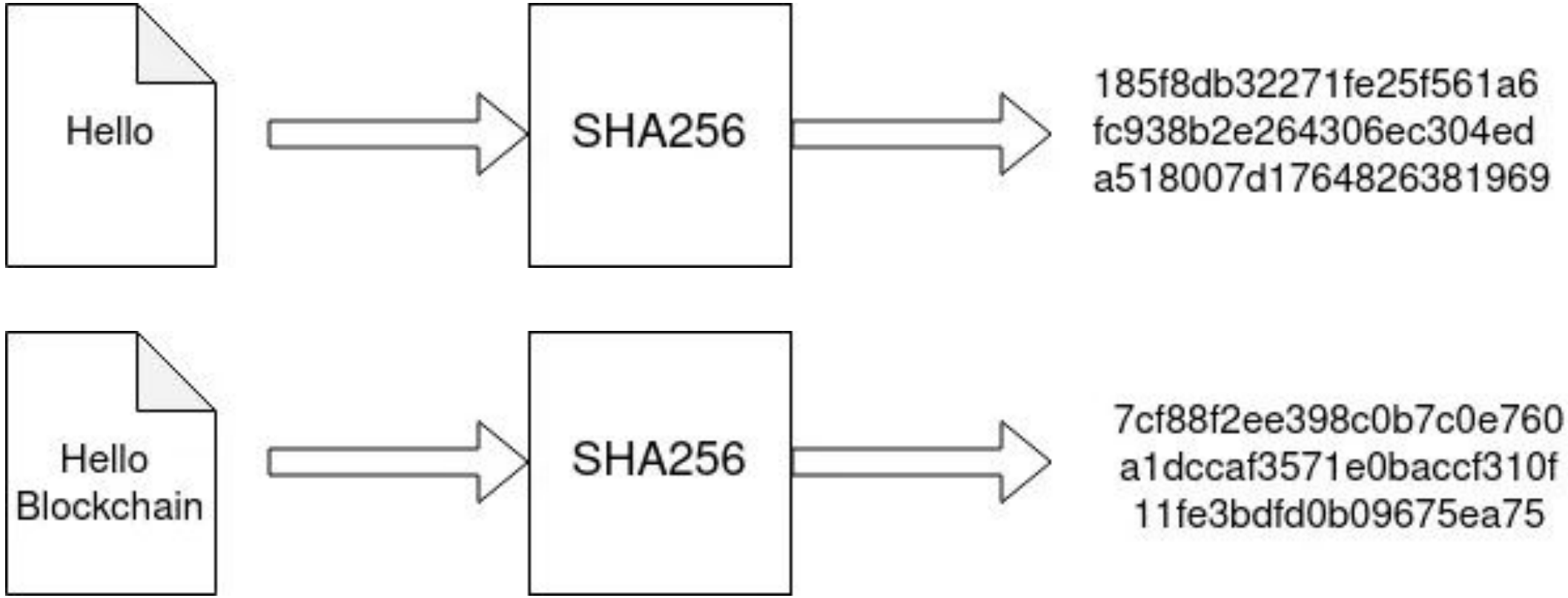
They provide a ***data integrity*** service

Example: SHA256



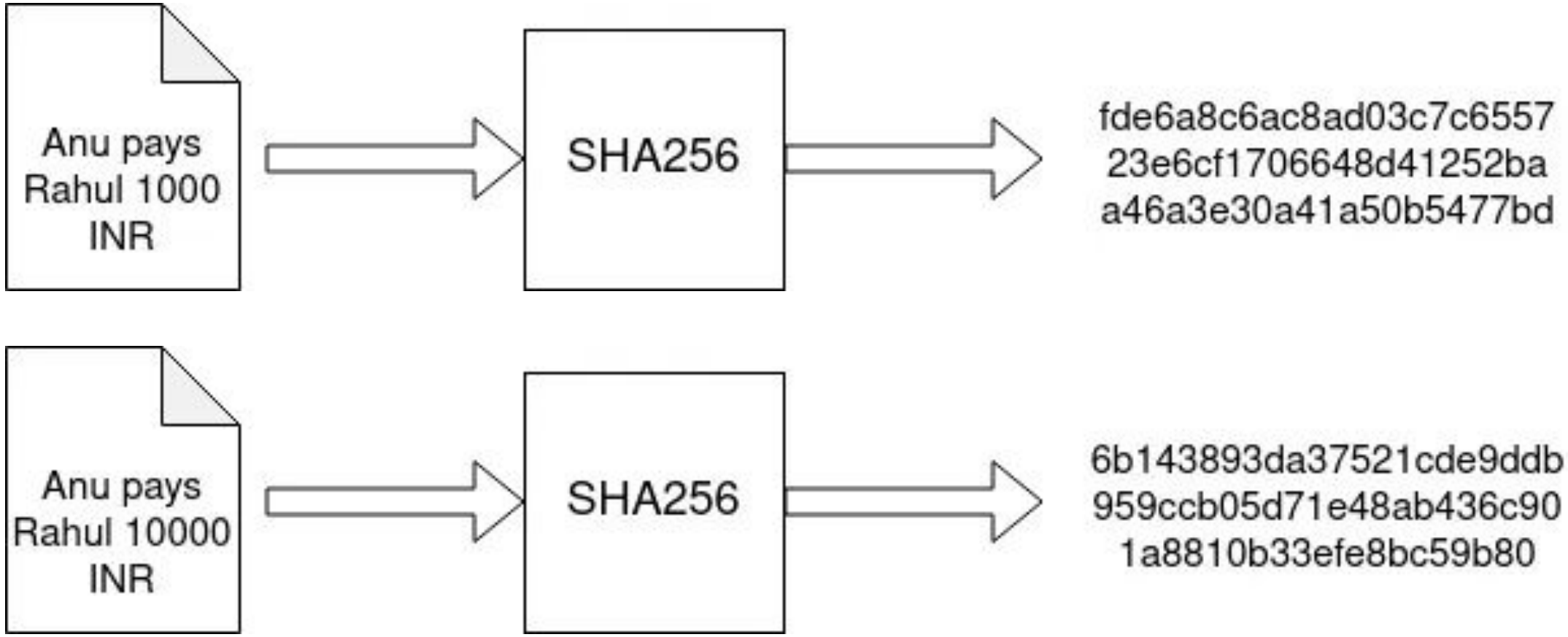
Hash Functions: Properties

Deterministic: Hash functions will always give the same output for a particular input.



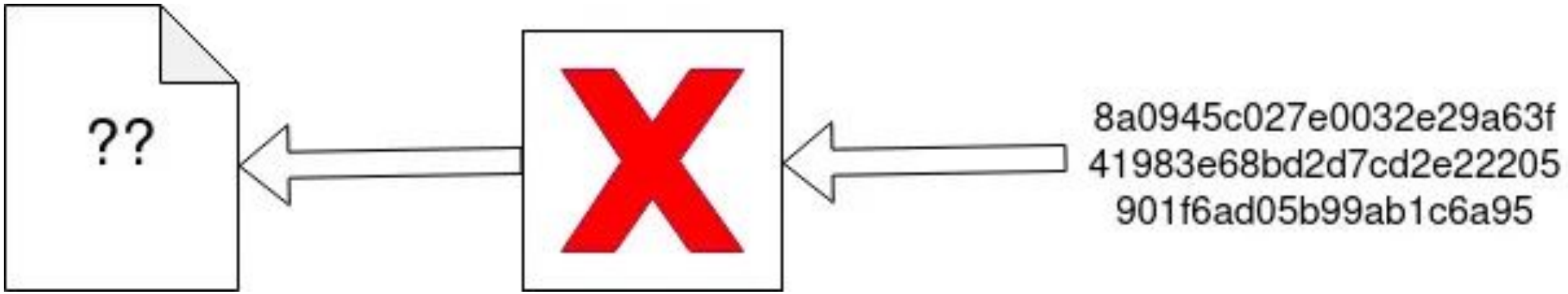
Hash Functions: Properties

Diffusion / Avalanche effect: Even if the input is changed slightly, there will be a notable and unpredictable change in the hash value.



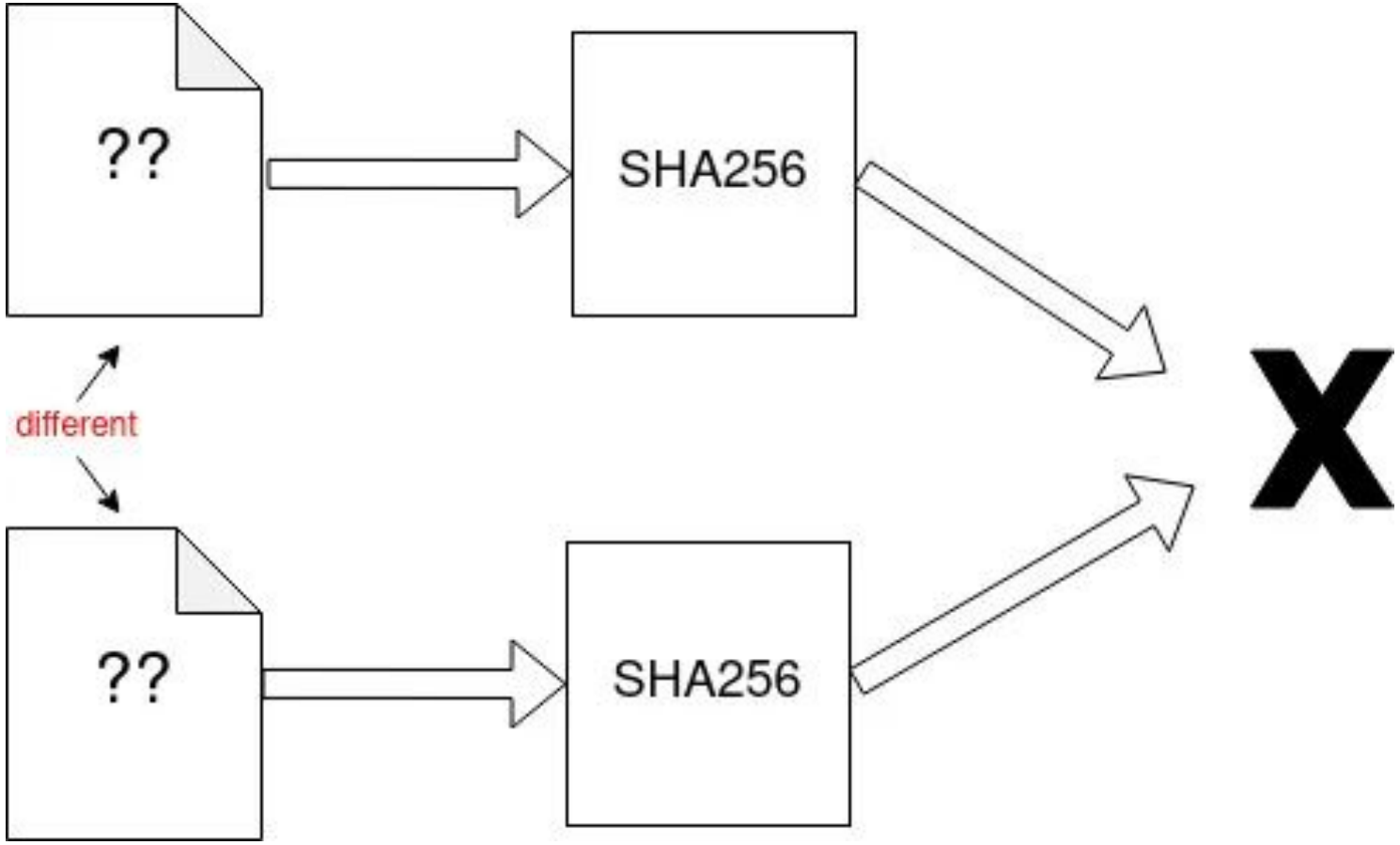
Hash Functions: Properties

Irreversible: *Hash functions are one-way, computationally impractical to reverse.*



Hash Functions: Properties

Collision Resistance: *Two different inputs will not give the same hash value.*



Digital Signatures

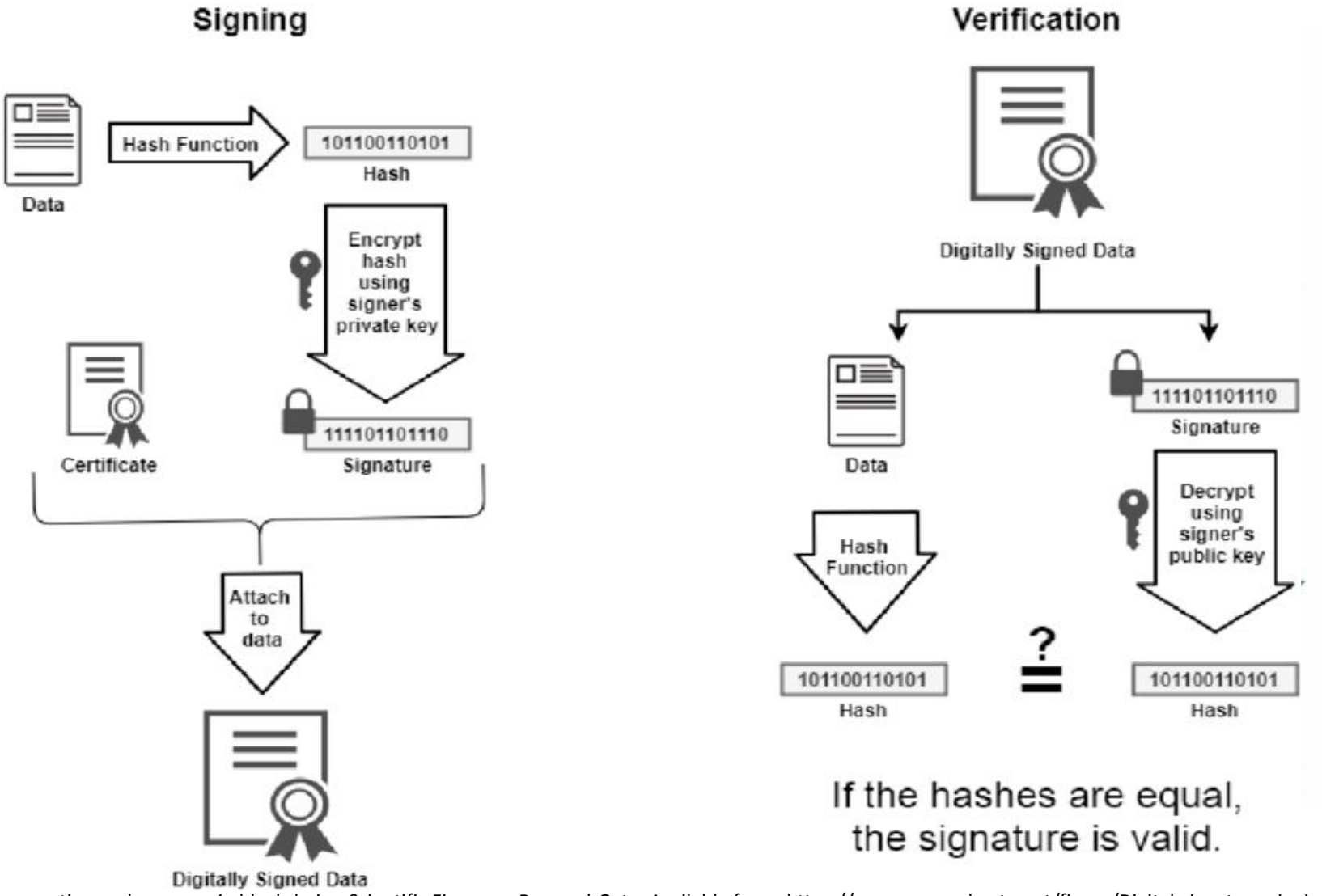
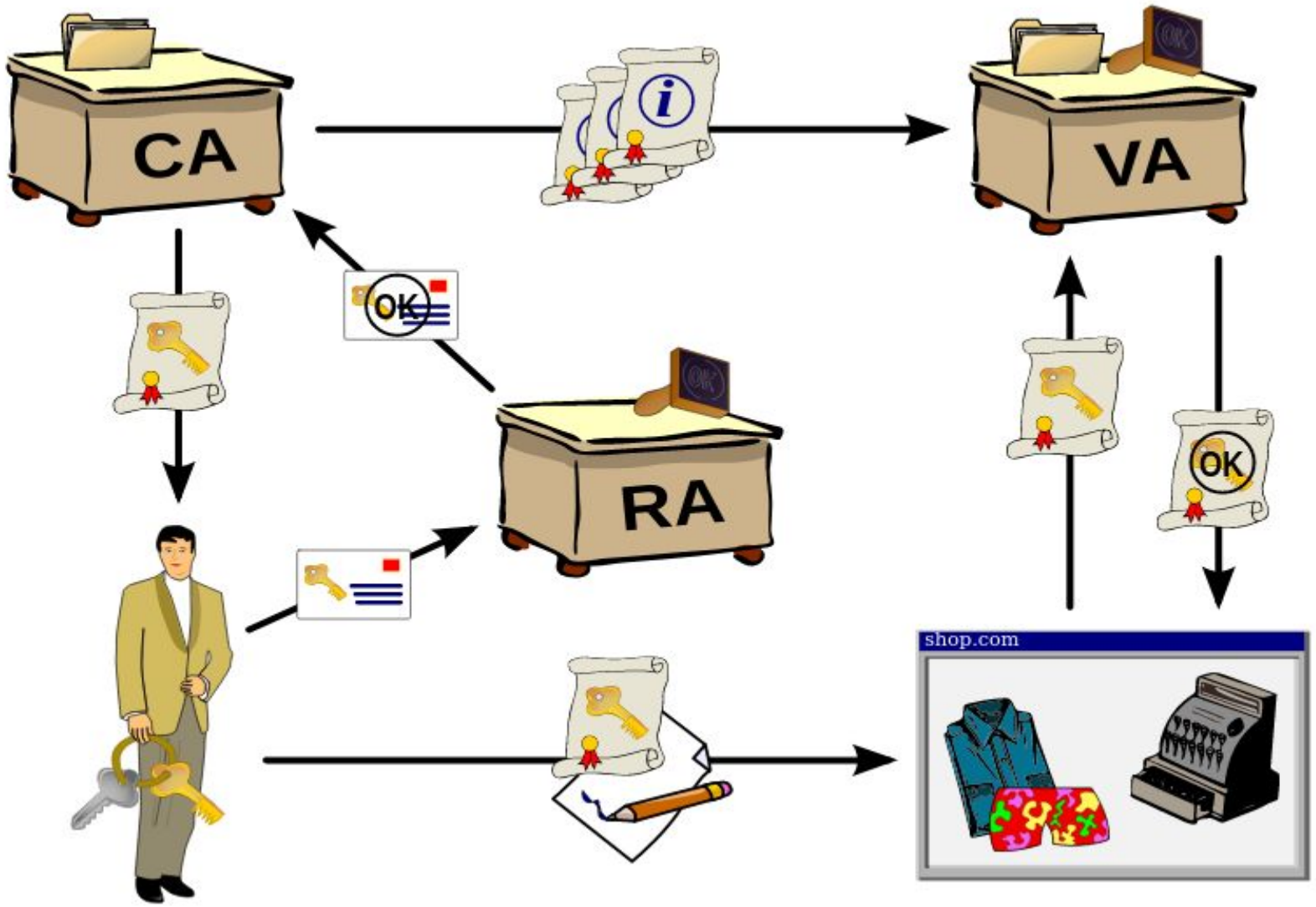


Image Ref: Private key encryption and recovery in blockchain - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Digital-signature-signing-and-verification_fig3_334361184

Public key Infrastructure



Cryptography

In blockchain, cryptography is primarily used for two purposes:

1. Securing the identity of the sender of transactions.
2. Ensuring the past records cannot be tampered with.

Block

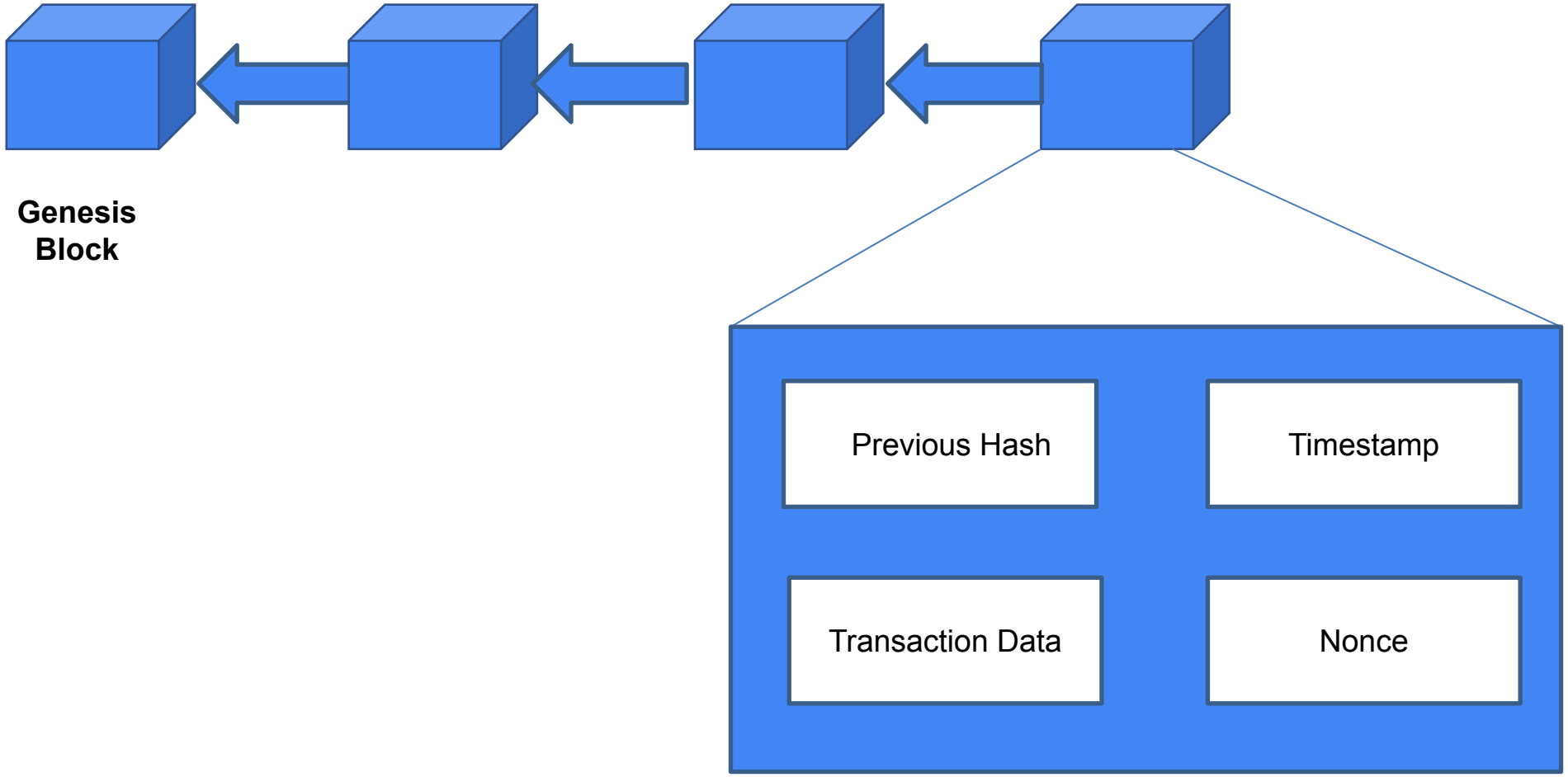
Timestamp: Block creation time

Nonce: A random number

Root Hash: Hash of all transactions

Previous Hash: Hash of previous block (header)

Blockchain


Genesis Block
Previous Hash
Timestamp
Transaction Data
Nonce

Inside a Block

Block 855993

00000000000000000083c94ef813e81902e6aee545b8d8a0c6e5b685a0668c

Block was mined on 2024-08-09 11:15:22 GMT +5.5. It has 8 confirmations on the Bitcoin blockchain. There are 3173 transactions in block 855993.

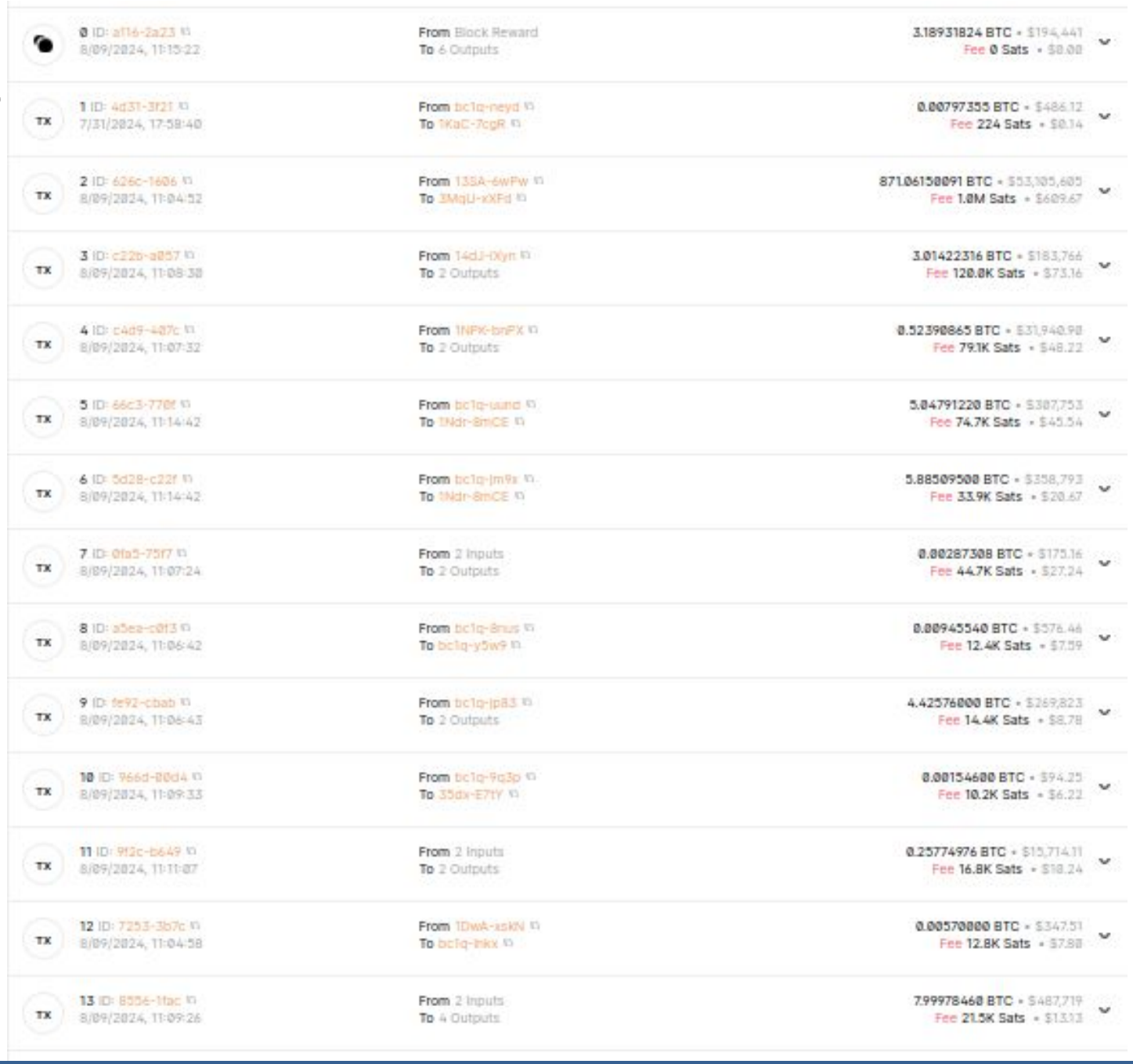
PREVIOUS NEXT

DETAILS

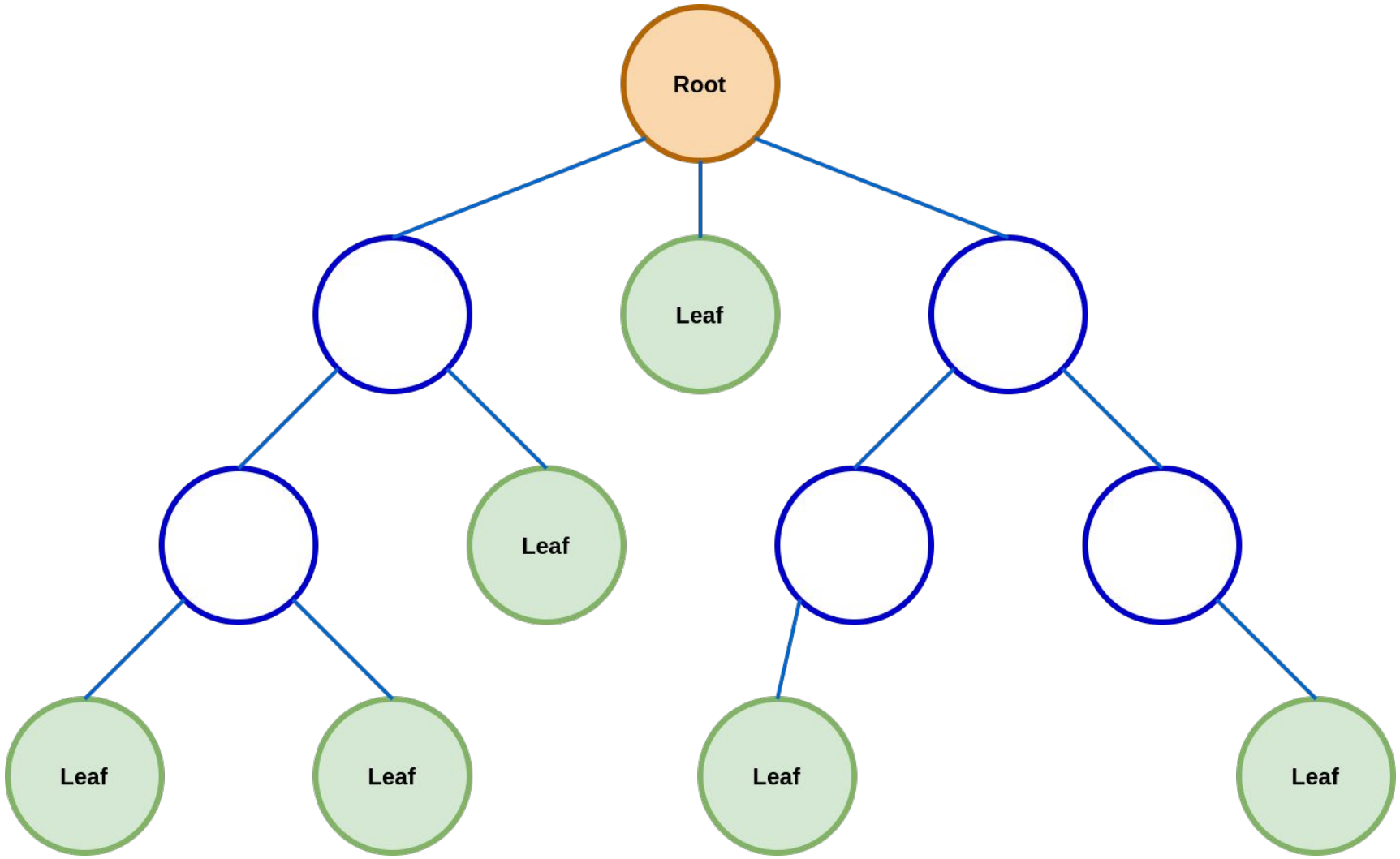
HEIGHT	855993
STATUS	In best chain (8 confirmations)
TIMESTAMP	2024-08-09 11:15:22 GMT +5.5
SIZE	1595.212 KB
VIRTUAL SIZE	1000 vKB
WEIGHT UNITS	3997.723 KWU
VERSION	0x2a2ac000
MERKLE ROOT	c5e5565bc78aade109358604bcf532f7fbae1b0a07bf490dad0e85f4f64f7975
BITS	0x17031abe
DIFFICULTY	90666502495565.78
NONCE	0x400b4105

KBA

Transactions



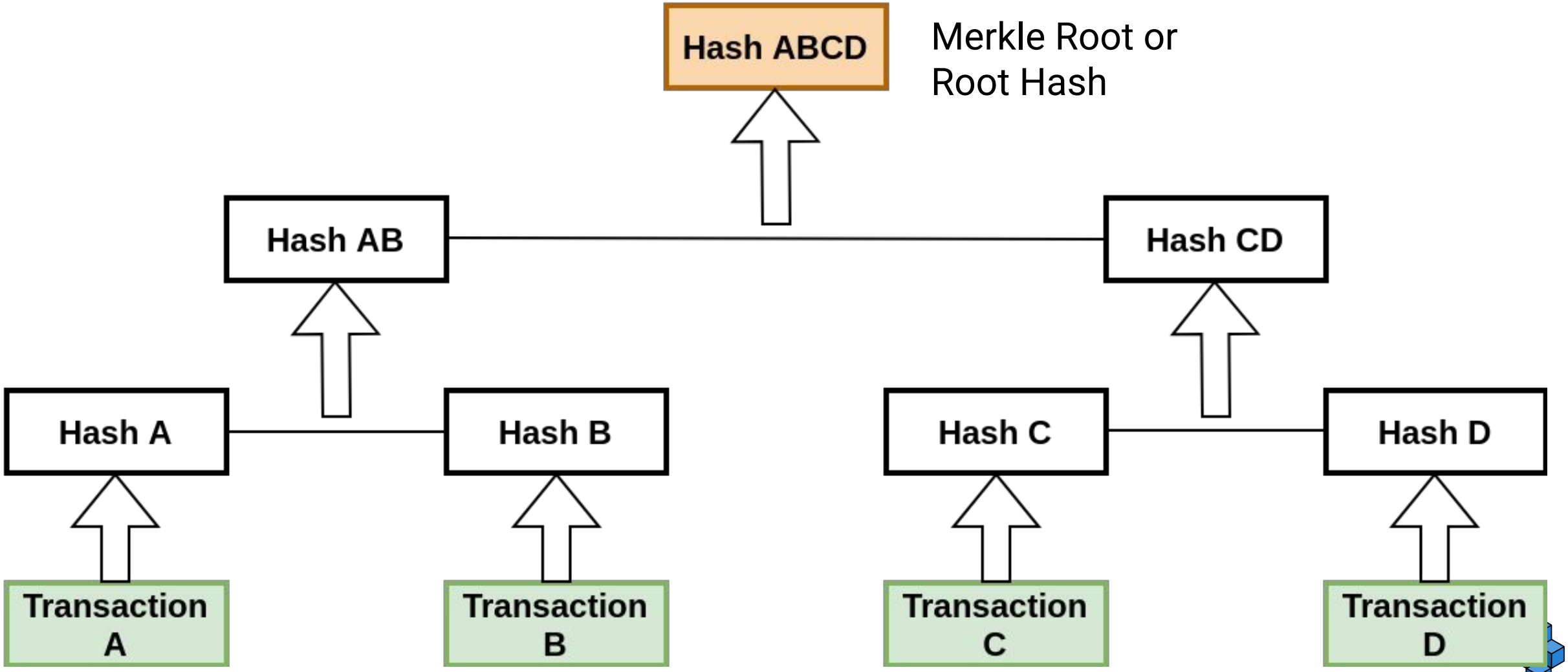
Tree



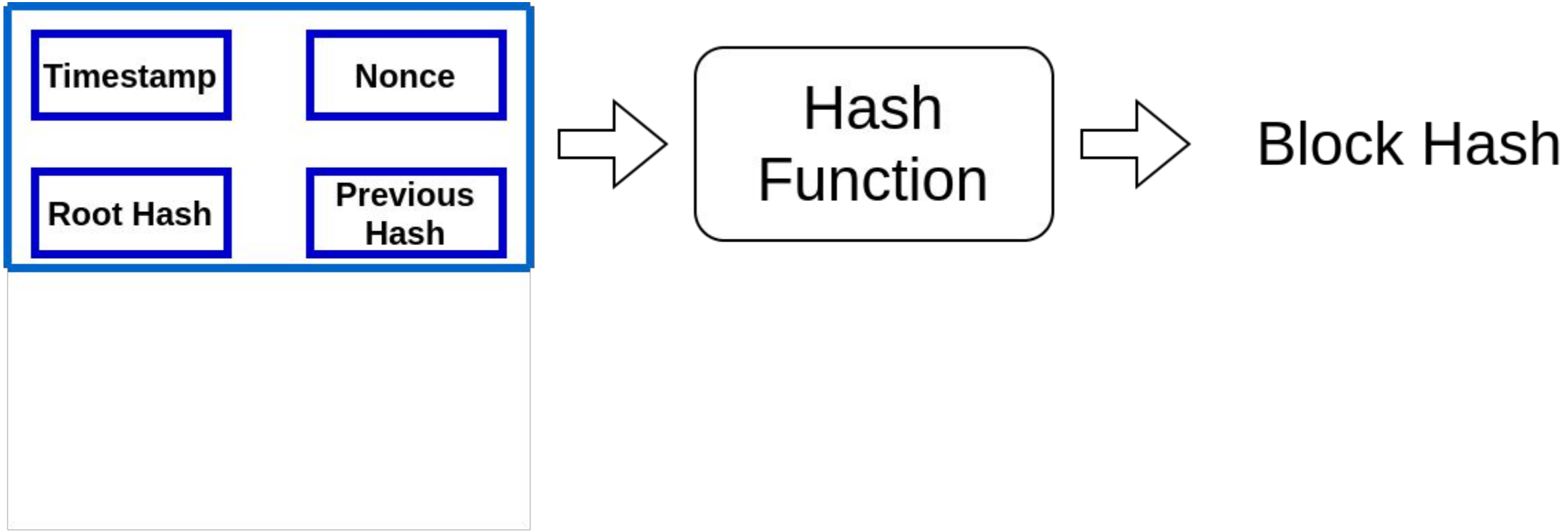
Transaction

1. From address
2. To address
3. Value
4. Transaction Hash

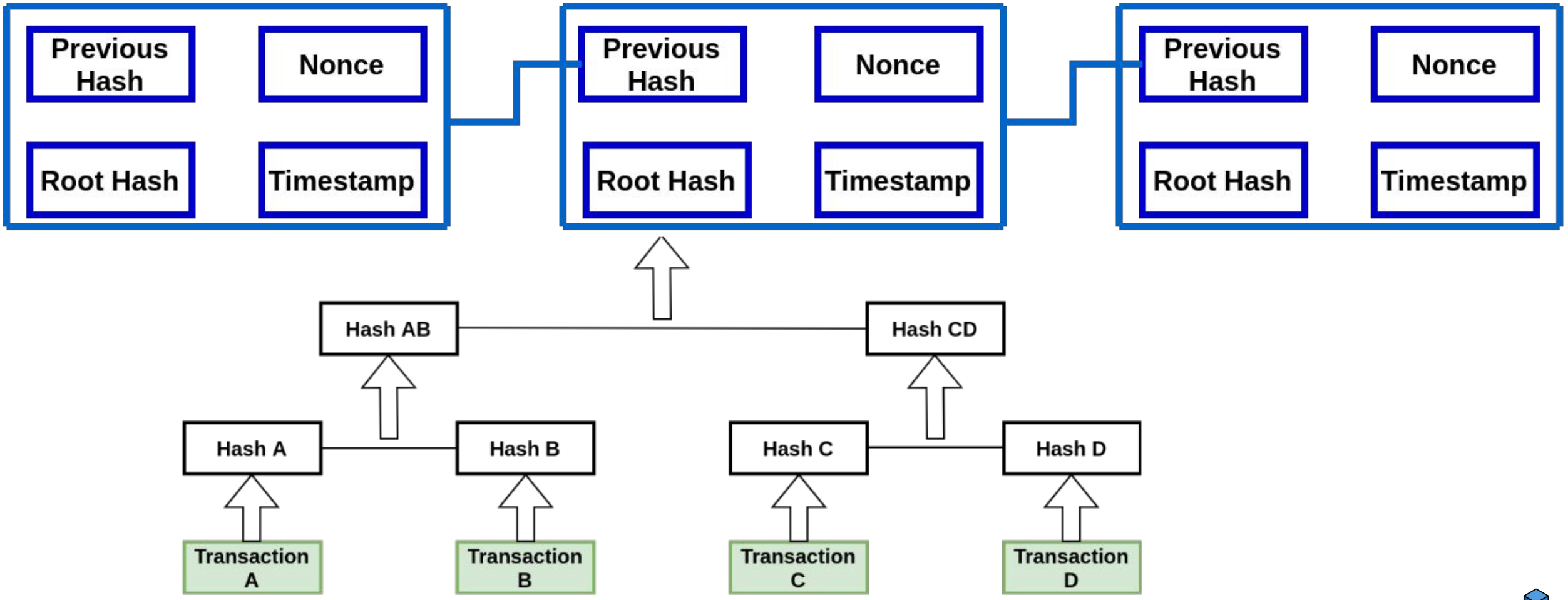
Constructing a Merkle Tree



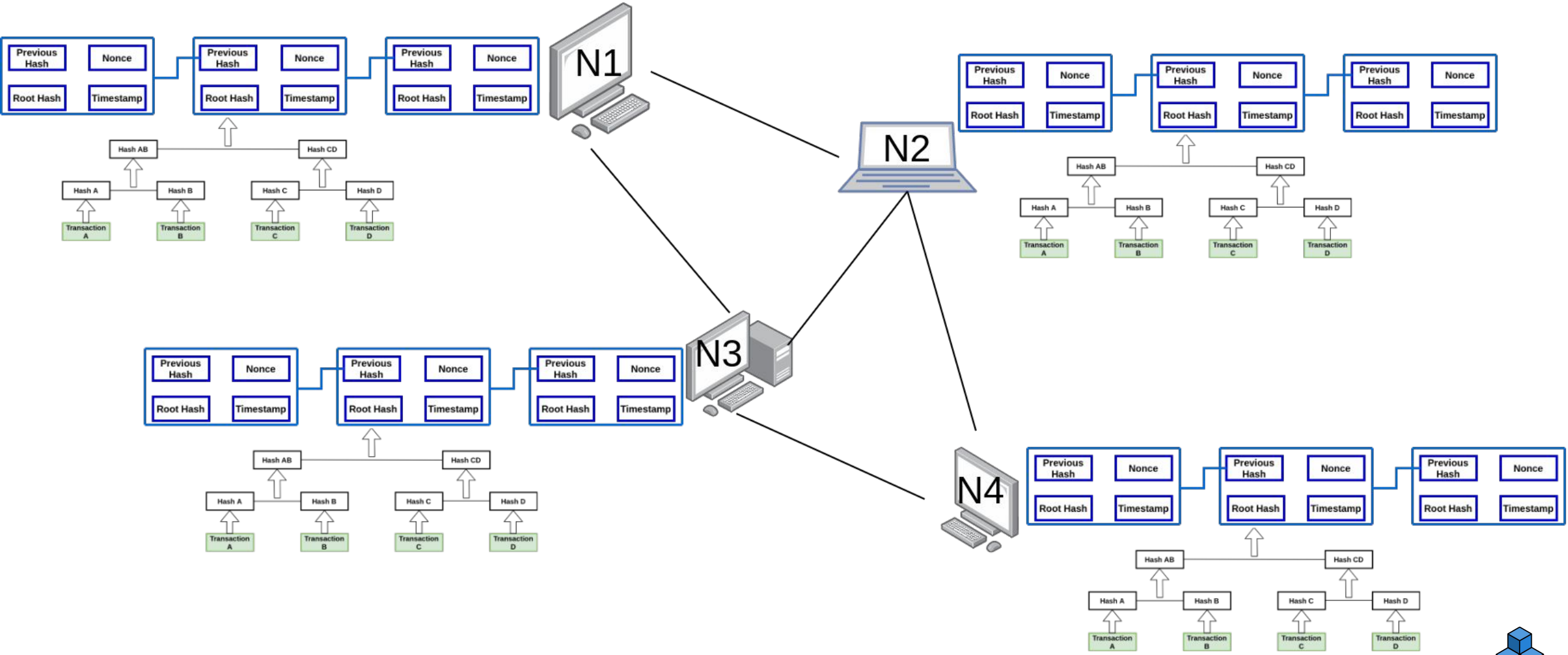
Block Hash


Timestamp
Nonce
Root Hash
Previous Hash
Hash Function
Block Hash

Hash Chain


Previous Hash
Nonce
Root Hash
Timestamp
Previous Hash
Nonce
Root Hash
Timestamp
Previous Hash
Nonce
Root Hash
Timestamp
Hash AB
Hash CD
Hash A
Hash B
Hash C
Hash D
Transaction A
Transaction B
Transaction C
Transaction D

Blockchain Network



Blockchain user

- Users are identified by their **addresses**
- Addresses are unique identifiers used in a blockchain transaction to denote senders and recipients.
- Sender digitally signs a transaction using the **secret key**

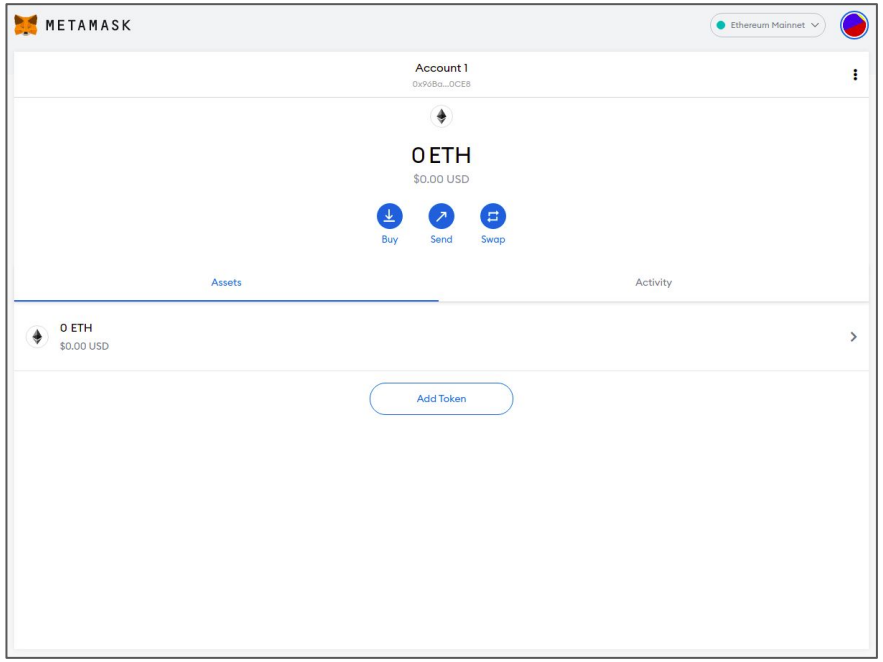
Addresses and Keys

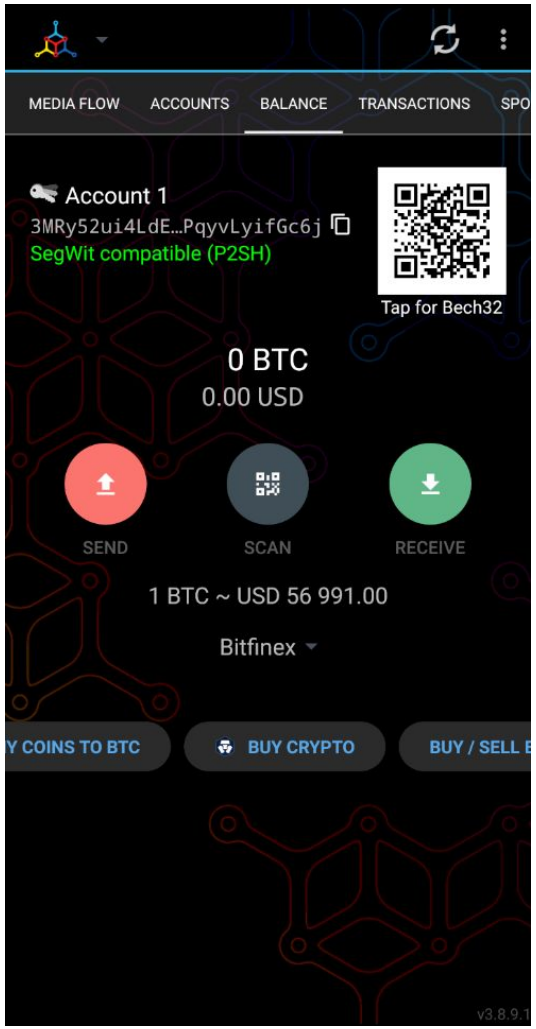
A Bitcoin **private key** is a random 256-bit number that allows bitcoins to be transacted.

A **public key** is a corresponding identification number that does not need to be secret.

Wallets

Software wallets





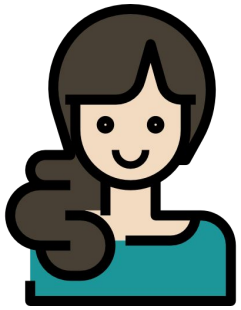
Life Cycle of Transaction

Transaction Lifecycle in Blockchain

1. Initiate a **transaction**.
2. **Sign** the Transaction.
3. Transaction is **validated locally**.
4. Transaction **broadcasted** to P2P computers (nodes).
5. Nodes **validate** the transaction.
6. Transactions combined to form a **data block**.
7. New block **added** to existing Blockchain.
8. The transaction is **complete**.

Transaction Life Cycle - The Sender

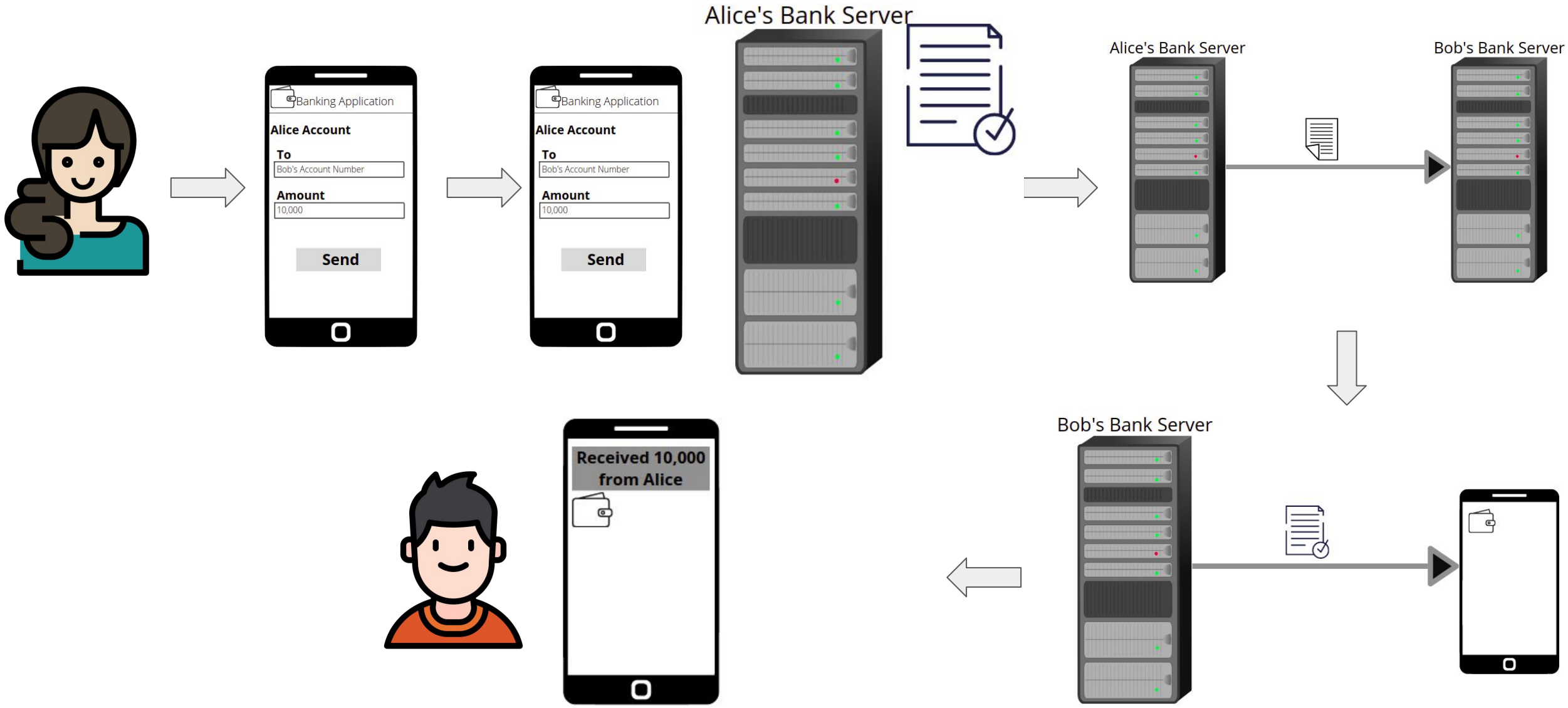
1. Initiate Transaction.



Alice opens her Blockchain Wallet

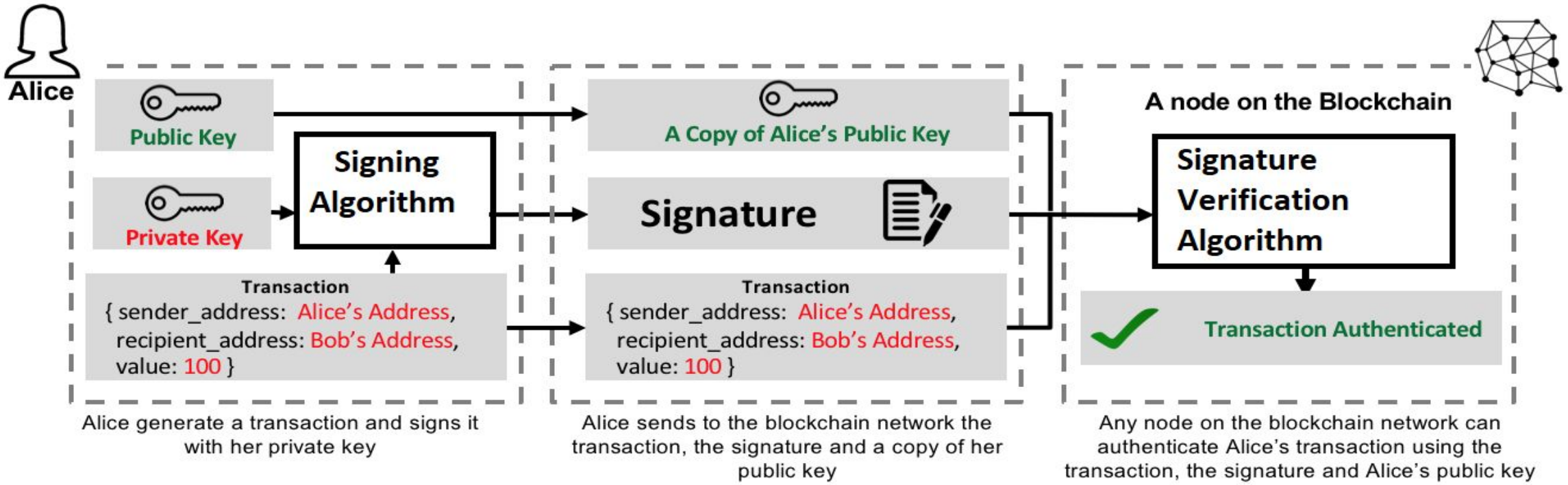
Provide the address of Bob and the amount to transfer, and sends

Online Banking Transaction



Authentication of Transaction

2. Sign the Transaction.
3. Transaction is validated Locally.

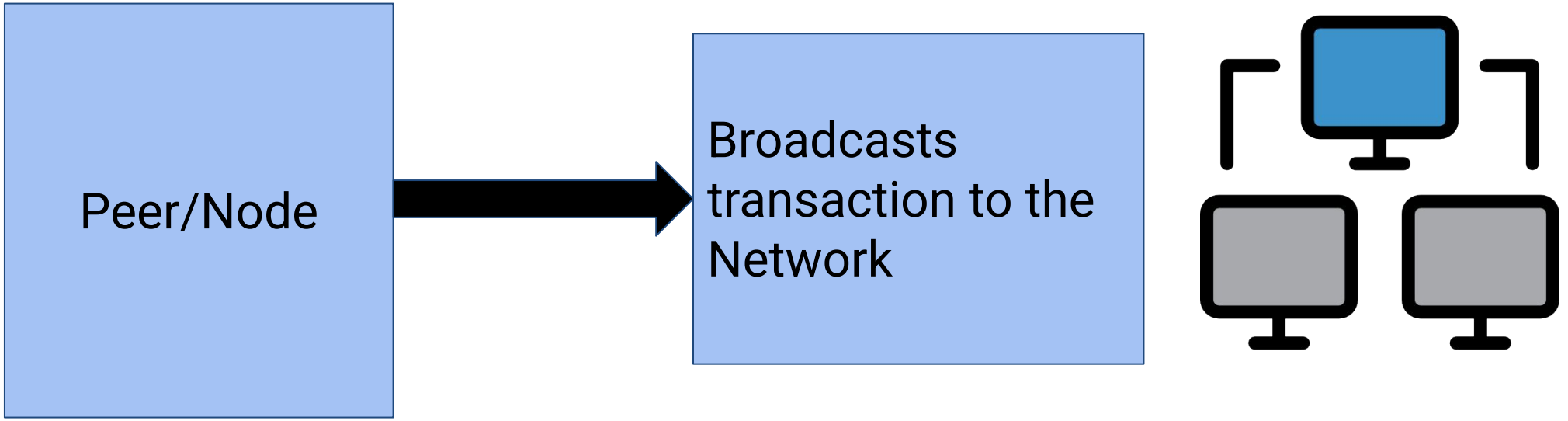


Authentication Process for Transactions on the Blockchain

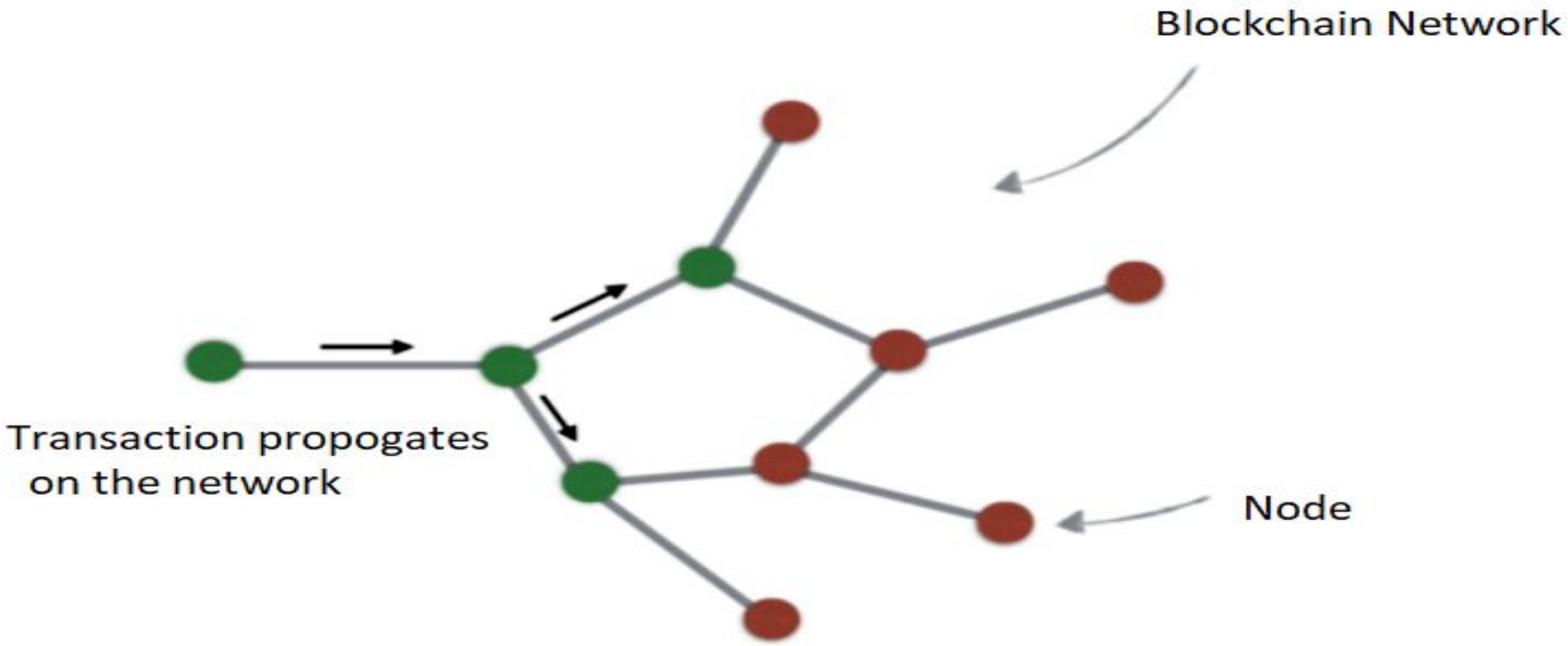
source:http://adilmoujahid.com/posts/2018/03/intro-blockchain-bitcoin-python/

Transaction Life Cycle -The Network

4. Transaction **broadcasted** to Blockchain Network.



Transaction Life Cycle -The Network



Each *node* receives the transaction request message,
updates its own copy of the *ledger*

Transaction Life Cycle -The Miners

5. Nodes **validate** the transaction.
6. Transactions combined to form a **data block**.
7. New block **added** to existing Blockchain.

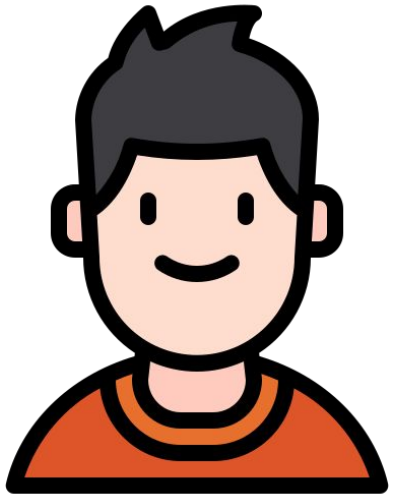
The miners collect all transactions for a time duration

Miners construct a new block and tries to connect with the existing blockchain

Once the mining is over and the hash is obtained,the block is included in the existing blockchain.
The updated blockchain is propagated in the network

Transaction Life Cycle -The Receiver

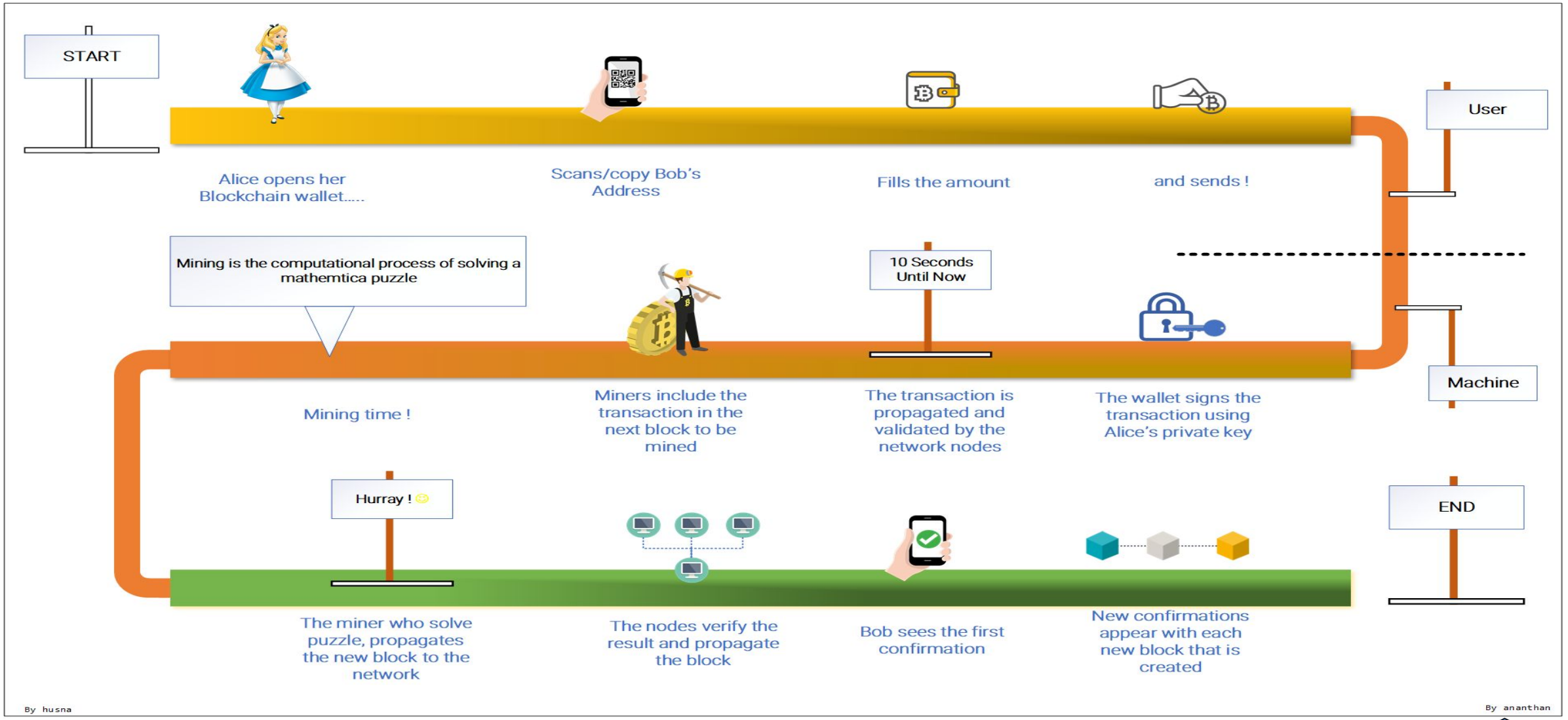
8. The transaction is **complete**.



Bob open his Blockchain wallet and refreshes, the Blockchain gets updated

The transaction reflects at Bob's wallet

Transaction Flow



KBA

Process Flow

1. Transactions submitted to network
2. Nodes verify transactions
3. Bundle the transactions into a block
4. Select the header of most recent block and insert it into the new block as hash
5. Consensus algorithm
6. New block is added to the local blockchain and propagated to the network

Security Features of Blockchain

Data Immutability

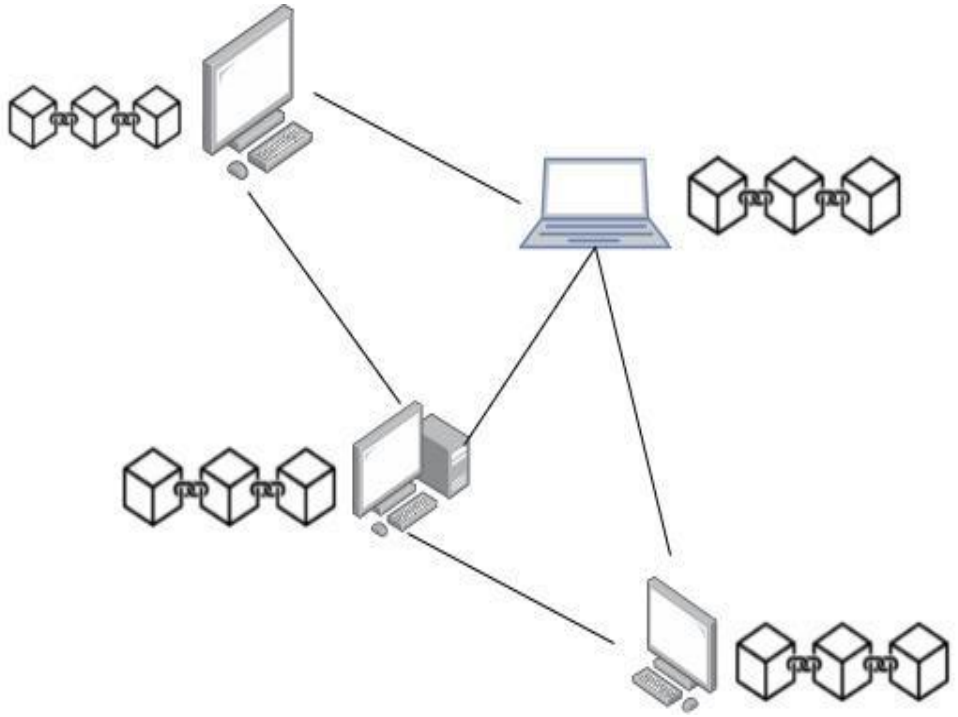
Validation creates a cryptographic link to a block's parent block

- Requires computation power

If any block's information is altered, the links will need to be re-computed

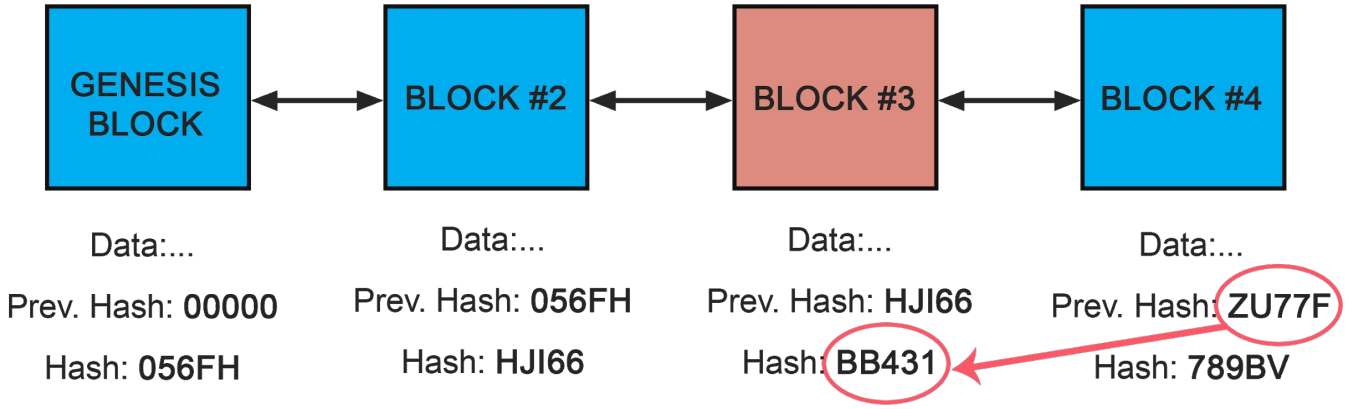
- This amount of computation is infeasible for an attacker

Data cannot be deleted because it is backed up on every node.



Tamper proof

- Each block in the chain contains transaction data.
- Is cryptographically hashed.
- The blocks of hashed data draw upon the previous-block in the chain
- This ensures all data in the overall "blockchain" has not been tampered with and remains unchanged.
- Hacker would need to change the block containing that record as well as those linked to it to avoid detection.



Embedded Security

- The reward of breaking in does not outweigh the input energy required to use it dishonestly in the first place.
- Similarly hacking a blockchain is economically disadvantageous.
- Blockchain networks are secure by design

Forgery Protection

Once secure addresses and keys are generated, a user is protected from forgery in the network with public key encryption.

- transactions are signed using private key as a “digital signature”
- Digital signature cannot be forged without access to key

Private key management is crucial to security.

Data Encryption

Public key encryption is used to create “digital signatures”, *not to encrypt the blockchain data itself*.

Bitcoin Example:

- All nodes need to have read access in order to verify the block.
- Encrypted data cannot be validated.
- Therefore, all transaction data must be public.

Zero-knowledge proofs may be used to validate encrypted data

Counterfeiting Protection

Counterfeit Attack	**Blockchain Characteristics and Security**
Generate counterfeit copies of currency	Infeasible because there is no currency to copy, only a record of balance. Changing a former block is implausible due to verification protocols
Trick network into validating counterfeit record	Record cannot be modified because of immutability.

Fault Tolerance

Fail-recover faults:

- Nodes that go down can recover by querying local nodes until they are sure they have the longest chain

Delayed/lost messages:

- Messages cannot be corrupted due to cryptographic signing
- Messages cannot be lost due to decentralization

Miners and Incentives

Miners are network nodes actively verifying Blockchain transactions.

- Transactions must be able to be verified by anyone who wants to participate.
- Miners must be incentivized to participate honestly

Block rewards and **transaction fees** incentivize miners.

- The network is organized to require an absurd amount of investment in order to manipulate the consensus.

Malicious miners would need to control 51% of the network to modify the consensus, so it is too expensive and too risky to try and manipulate.

Peer to Peer Networking

A distributed network that partitions transactions of verification between peers.

- Peers are equally privileged participants, playing on level field within the application.
- Resources shared between peers without the use of a centralized administrative system.

Accounting Model

As a distributed ledger, blockchains validate transactions by checking consistency between inputs and outputs.

- Sender must own sufficient inputs
- Sender must be authorized to send the inputs in the transaction

Similarly, firms maintain records with double entry accounting:

- Debits must equal credits
- Total impact recorded

Auditing

Financial statements are used by people outside the firm. Each of the following is an issue of trust that auditing tries to solve concerning financial statements:

- Existence.
- Completeness.
- Valuation.
- Rights and Obligations.
- Presentation and Disclosure.

Blockchain solves the issues of trust through post unforgeable transactions and multiparty secure computations.

Triple Entry Accounting

Double entry can still be manipulated:

- Inputs and outputs can be changed to add up as desired.
- Outside stakeholders cannot trust a company's books.

Triple Entry Accounting:

- Transaction data cannot be modified by firm as it is recorded on a general ledger
- Data can be queried by any network participant
- Advantages in: reconciliation, transparency, trust -> **no longer a need for third party auditing services.**

Anonymity

Theoretically, a private/public key pair can be kept anonymous:

In practice:

- If a public key is used in more than one transaction, transactions can be traced
- Transaction inputs and outputs can be linked to identify participants
- User can generate a new key every time
- User can use cryptocurrency tumblers

Anonymity or pseudonymity can depend on network rules/ user choice.

Zero Knowledge Proofs can be used to further maintain privacy in blockchain transactions

References

- Hash demo - https://andersbrownworth.com/blockchain/hash
- Block demo - https://andersbrownworth.com/blockchain/block
- Blockchain demo - https://andersbrownworth.com/blockchain/blockchain
- Crypto tutorial videos - https://andersbrownworth.com/blockchain/
- Merkle trees - https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch09.asciidoc
  - https://kbaiiitmk.medium.com/merkle-tree-a-beginners-guide-5c53a7defeb9
- Cryptography : https://kbaiiitmk.medium.com/explaining-cryptography-in-blockchain-6e1766d50596
- Hash Functions: https://kbaiiitmk.medium.com/hash-function-the-heart-of-blockchain-fa35e90e0bc1
- DAG:https://kbaiiitmk.medium.com/directed-acyclic-graph-dag-based-distributed-ledgers-e2f42c39366

Thank You