Introduction to Blockchain Technology

- Blockchain

- Blockchain is simply a data structure where each block is linked to another block in a time- stamped chronological order
- It is a distributed digital ledger of an immutable public record of digital transactions.
- Every new record is validated across the distributed network before it is stored in a block.
- All information once stored on the ledger is verifiable and auditable but not editable .
- Each block is identified by its cryptographic signature.
- The first block of the blockchain is known as Genesis block.

Basics of Blockchain "A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography." The concept is introduced by Satoshi Nakamoto 2008.

Block

1.Data :"hello everyone"
2.Prev Hash:23432FRT123
3.Hash :123FFRE342

Blockchain

Figure 1.1.All blocks are cryptographically link together

- Key Characteristics:
- **Open**: Anyone can access blockchain.
- **Distributed or Decentralised**: Not under the control of any single authority.
- **Efficient**: Fast and Scalable.
- **Verifiable**: Everyone can check the validity of information because each node maintains a copy of the transactions.
- **Permanent**: Once a transaction is done, it is persistent and can’t be altered.

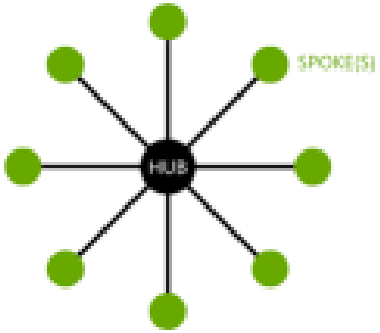
- What is Blockchain?
- A blockchain is a decentralized, distributed public ledger where all transactions are verified and recorded. Blockchain is a system comprised of..
- Transactions
- Immutable
- ledgers
- Decentralized peers
- Encryption processes
- Consensus mechanisms
- Optional Smart Contracts

- Transactions As with enterprise transactions today, Blockchain is a historical archive of decisions and actions taken
- Land registration
- Personal identification
- Transportation
- Banking
- Manufacturing

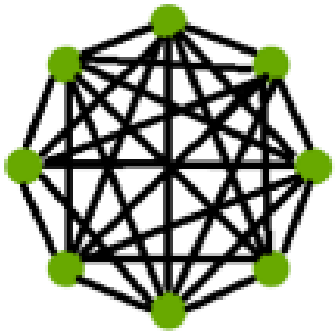
- Immutable As with existing databases, Blockchain retains data via transactions. The difference is that once written to the chain, the blocks can be changed, but it is extremely difficult to do so.
- Requiring rework on all subsequent blocks and consensus of each. The transaction is, immutable.
- In DBA terms, Blockchains are Write and Read only Like a ledger .

Decentralized Peers Rather than the centralized “Hub and Spoke” type of network, Blockchain is a decentralized peer to peer network. Where each NODE has a copy of the ledger.

Centralized DB



Distributed Ledgers



- Encryption Standard encryption practices. Some Blockchains allow for “BYOE” (Bring Your Own Encryption)
- All blocks are encrypted
- Some Blockchains are public, some are private.
- Public Blockchains are still encrypted, but are viewable to the public (read,write and participate) .
- Private Blockchains employ user rights for visibility, e.g. Customer – Writes and views all data
- Auditors – View all transactions
- Supplier A – Writes and views Partner A data
- Supplier B – Writes and views Partner B data

- Consensus Ensures that the next block in a blockchain is the one and only version of the truth.
- Keeps powerful adversaries from derailing the system and successfully forking the chain consensus algorithm is a process in computer science used to achieve agreement on some information among the distributed systems.

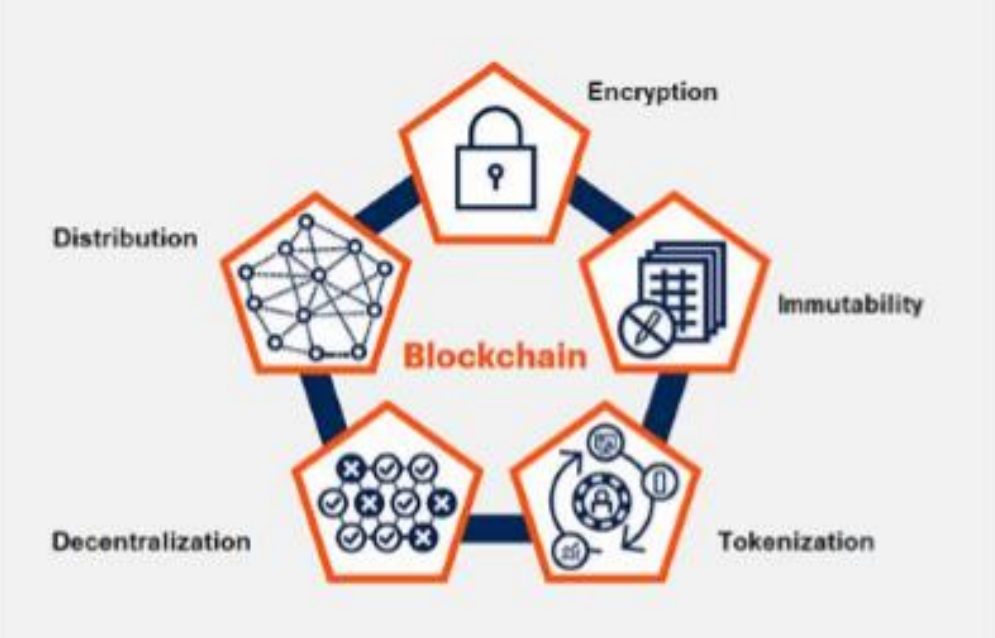
Smart Contracts Computer code Provides business logic layer prior to block submission.

Table 1.1 Example blockchain netwoks

Blockchain	Smart Contracts?	Language	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc, depends
Others	Depends	Depends	

- FEATURES

- Immutable and tamper-proof data store
- Sequential Chain with Cryptographic hashing
- Trust-free Consensus-based transactions
- Decentralized peer-to-peer network
- Distributed shared ledger



- Problems with the current system

- Banks and other third parties take fees for transferring money
- Mediating costs increases transaction costs
- Also, central authority in control can overuse the power and can create money as per their own will.

- We need a system which:
- Eliminates the need of middlemen or Third parties thereby making transaction costs nil or negligible.
- Is transparent and tamper resistant in order to avoid manipulation or misuse.
- Currency creation is not in control of any central authority.
- Is regulated to maintain the value of the currency.

Distributed system attempt to solve the problem

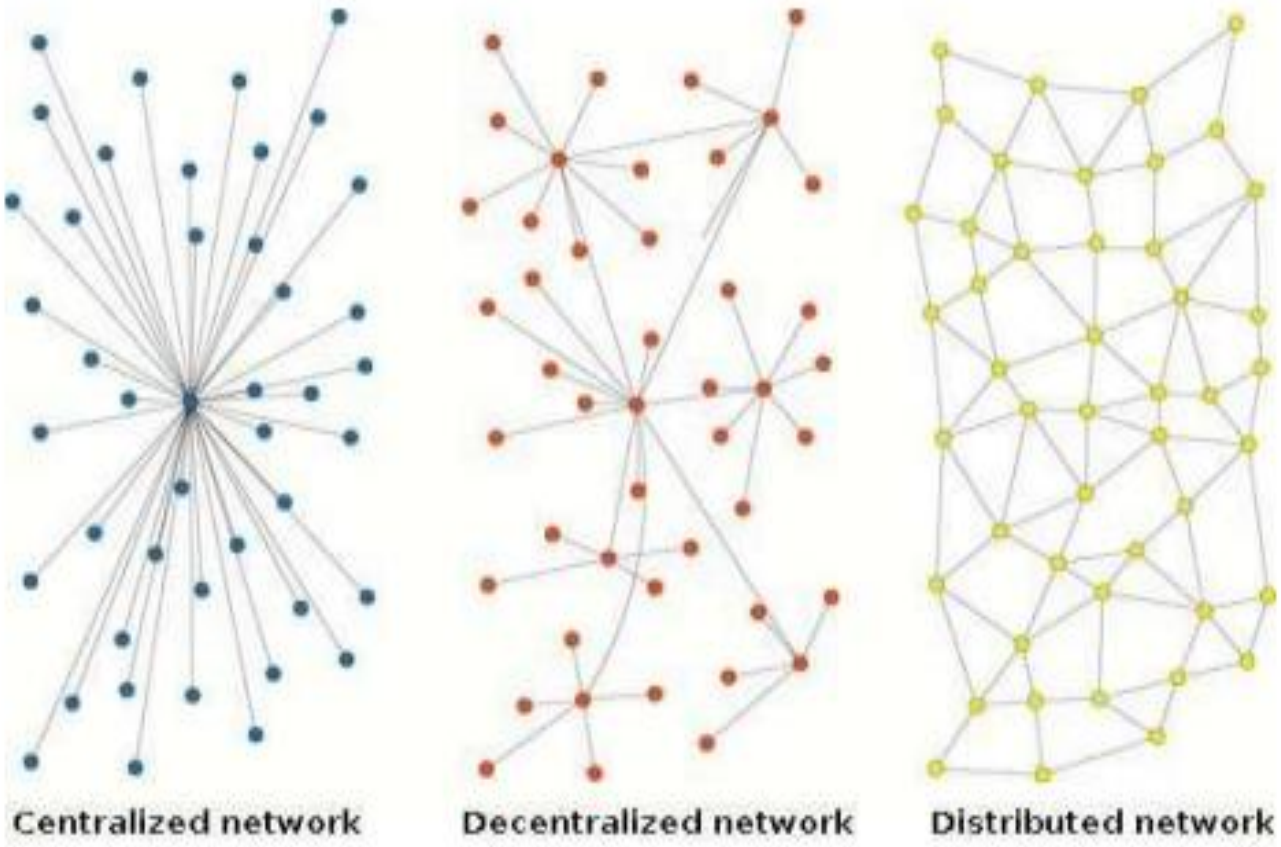


Figure 1.6 Different network of systems

Distributed system enables a network of computers to maintain a collective bookkeeping via internet this is open and is not in control of one party. it is available in one ledger which is fully distributed across the network.

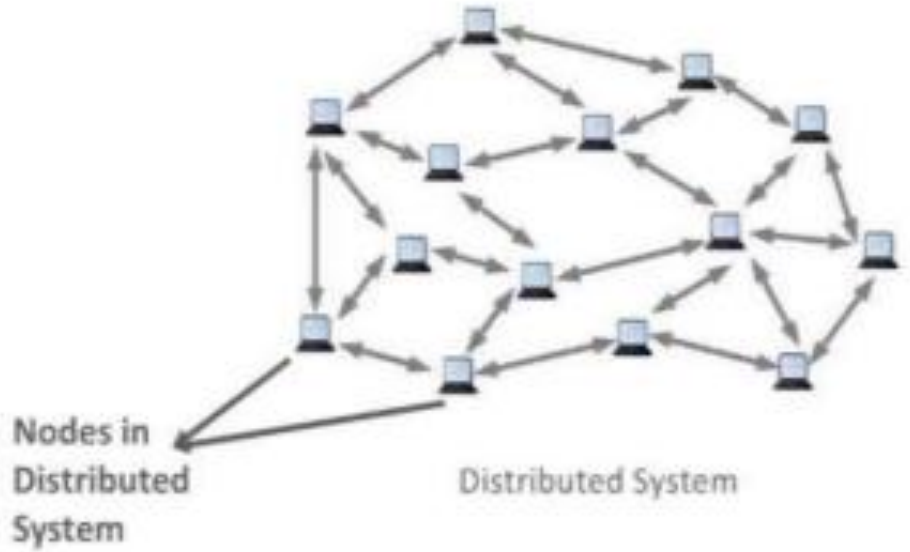
- Centralized These Centralized applications are made of two things- The back End and Front end. Any standard application runs on a computer system operated by an organization. There may be many users on the node side but the backend is controlled by a single organization.

Decentralized

- Means no node is instructing any other node as to what to do.
- The code runs on a peer-to-peer network of nodes and no single node has control over the dApp.
- Depending on the functionality of the dApp, different data structures can be used to store the application data.
- Bitcoin uses a blockchain decentralized ledger of transactions

Applications in which computation is distributed across components, communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal.

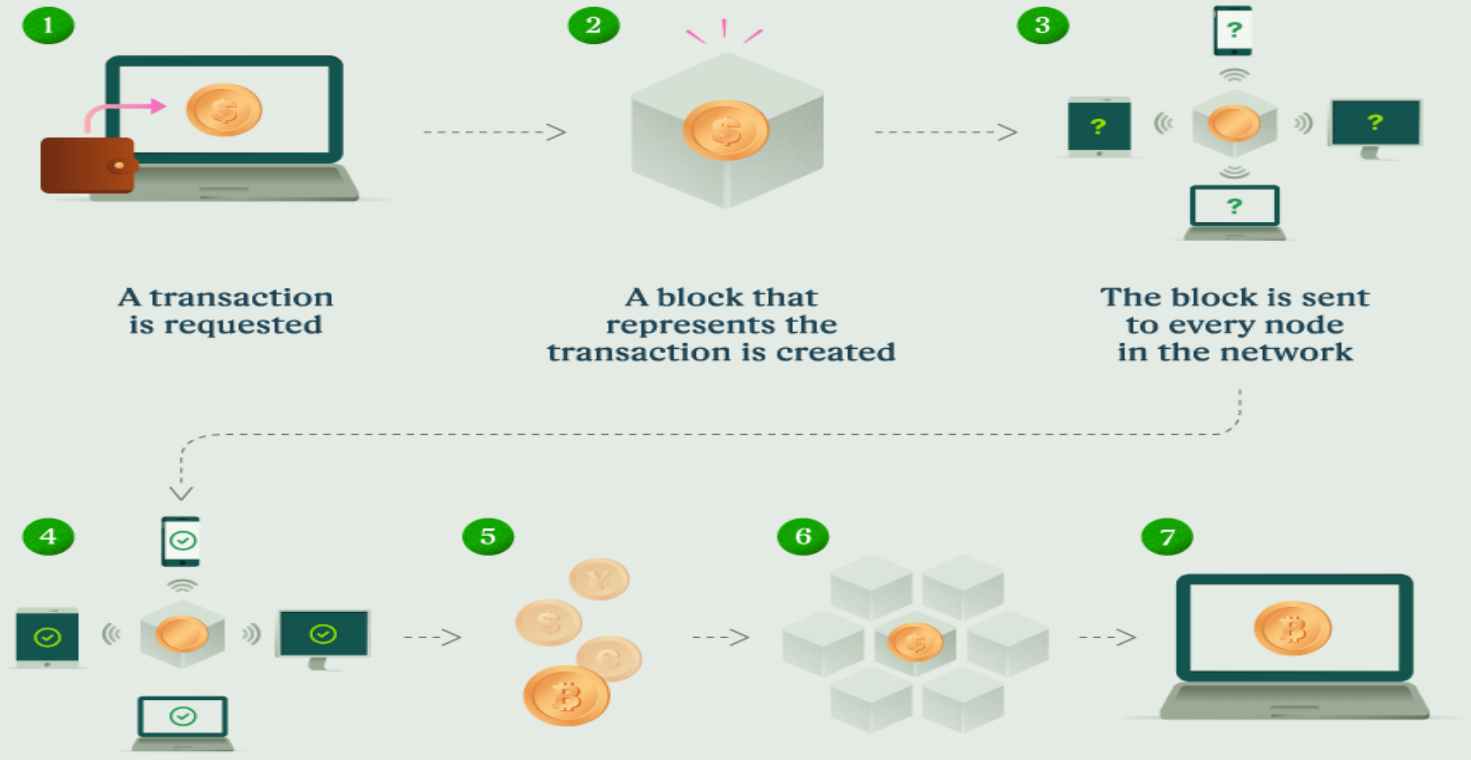
Distributed system



How Does It Work

- These are the core blockchain architecture components:
- Node - user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)
- Transaction - smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain
- Block - a data structure used for keeping a set of transactions which is distributed to all nodes in the network
- Chain - a sequence of blocks in a specific order
- Miners - specific nodes which perform the block verification process before adding anything to the blockchain structure
- Consensus (consensus protocol) - a set of rules and arrangements to carry out blockchain operations

How blockchain works



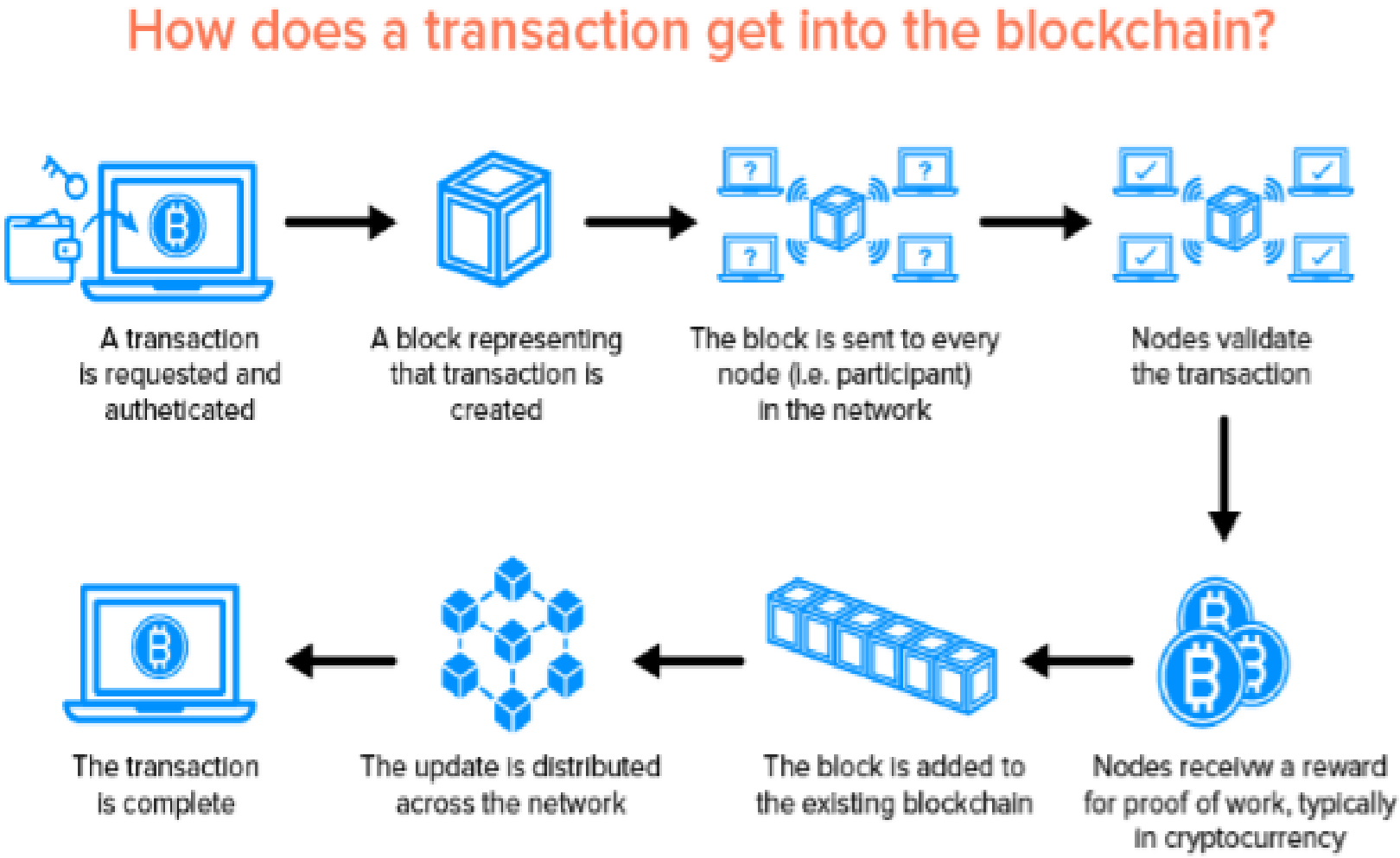
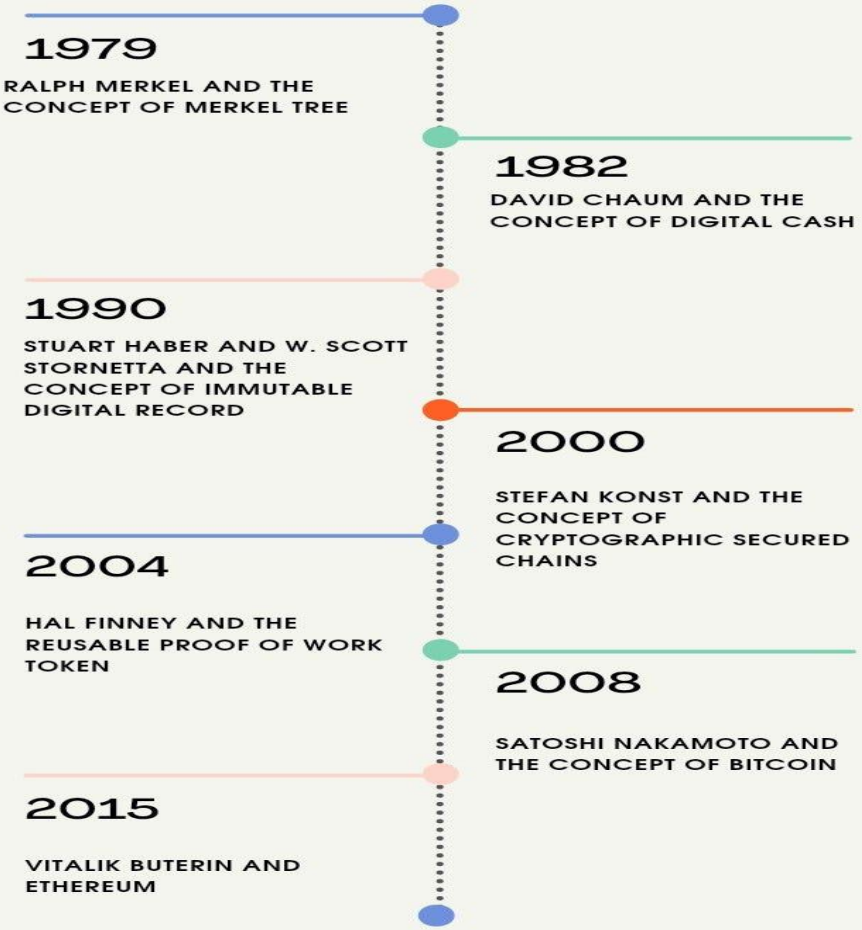
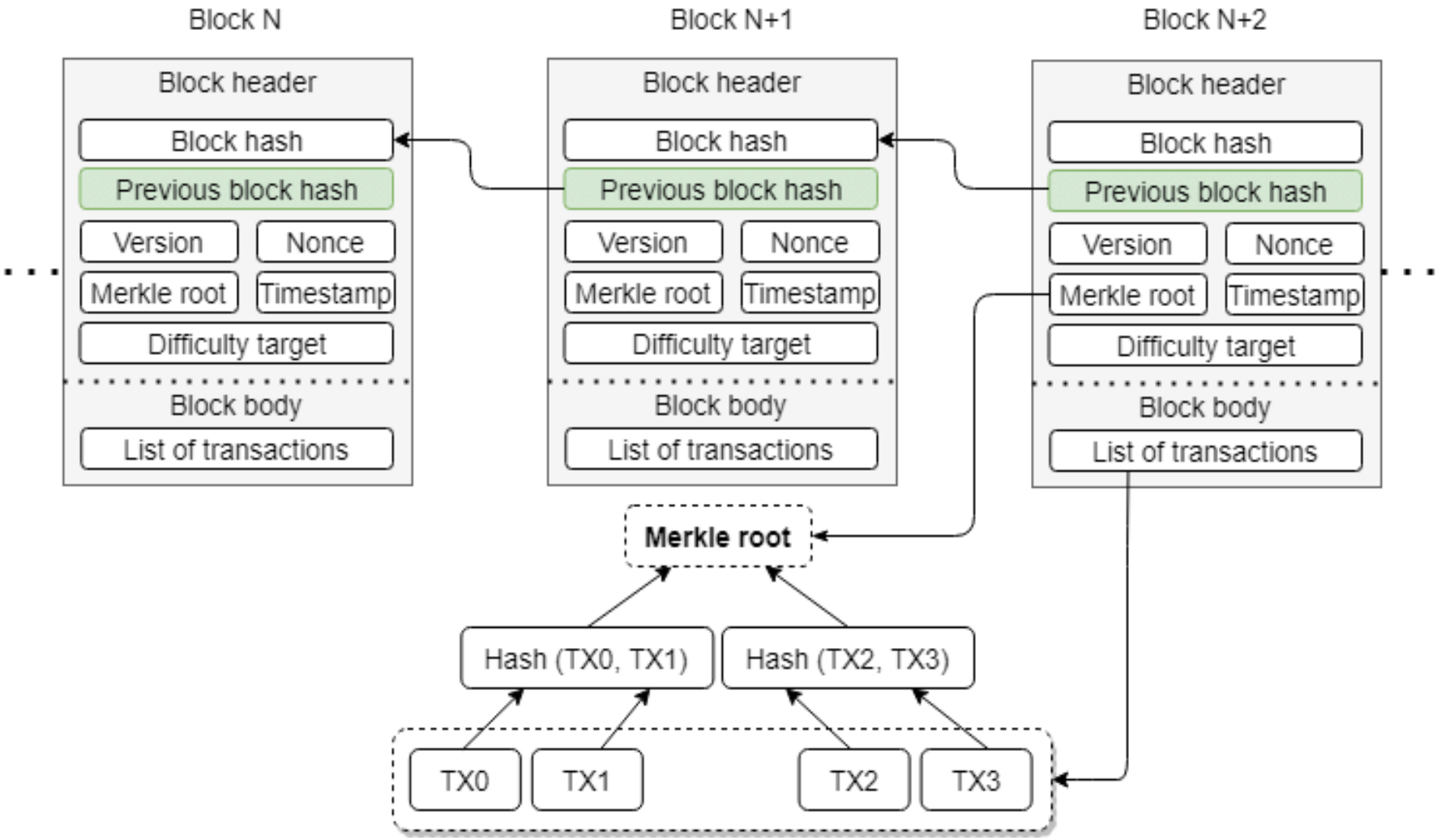


Figure 1.14 Blockchain Flow diagram

HISTORY OF BLOCKCHAIN

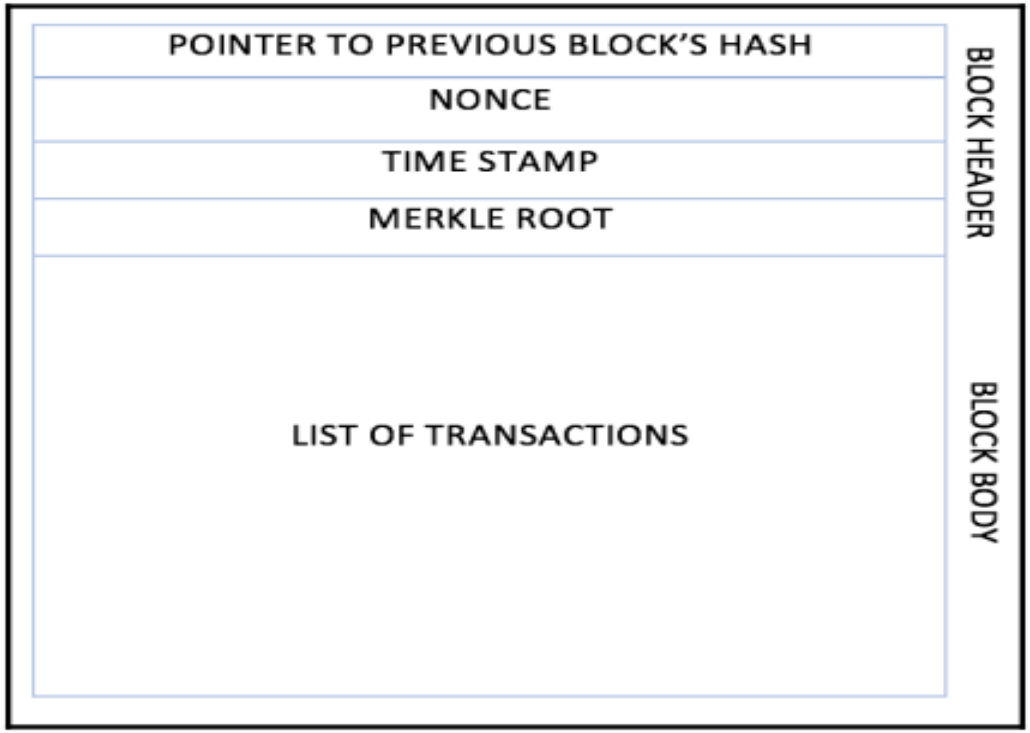


Simplified Architecture



Structure of a Block

Blocks are the fundamental components of the blockchain with a block header and body. Block body will be nothing but the transactions that will be part of created or proposed blocks in the form of a Merkle tree.



- **Previous hash pointer (hashPrevBlock):** The first blockchain block is Genesis Block, which has no parent. The Previous hash pointer is a 32-byte field containing the 256-bit hash address of the previous block header and the previous block's Hash.

- **Nonce** – This 4-byte field contains a 32-bit random value that is altered/updated to try different permutations to achieve the required difficulty level. It is calculated using trial and error.
- **Timestamp (Time)** – This 4-byte field contains a timestamp of the current block to arrange the block chronologically.

- **Merkle root (hashMerkleRoot)** – This 32-byte field represents the aggregation of all the hash values of the transactions into a 256-bit single hash value.

- **List of Transactions**

Introduction to SHA -256 Secure Hash Algorithm

Key properties of Secure Hash Algorithms (SHA) SHA-256 used in Bitcoin is one of the examples of a cryptographic hashing algorithm. SHA-256 always generates a 256-character hash value irrespective of the input data size. Secure hash algorithms used in blockchain should have the following properties:

Same hash value should always be generated for the same input

Hash should be calculated from the data, but it shouldn't be possible to derive data from the hash

Even a slight change in the data should change the hash value completely

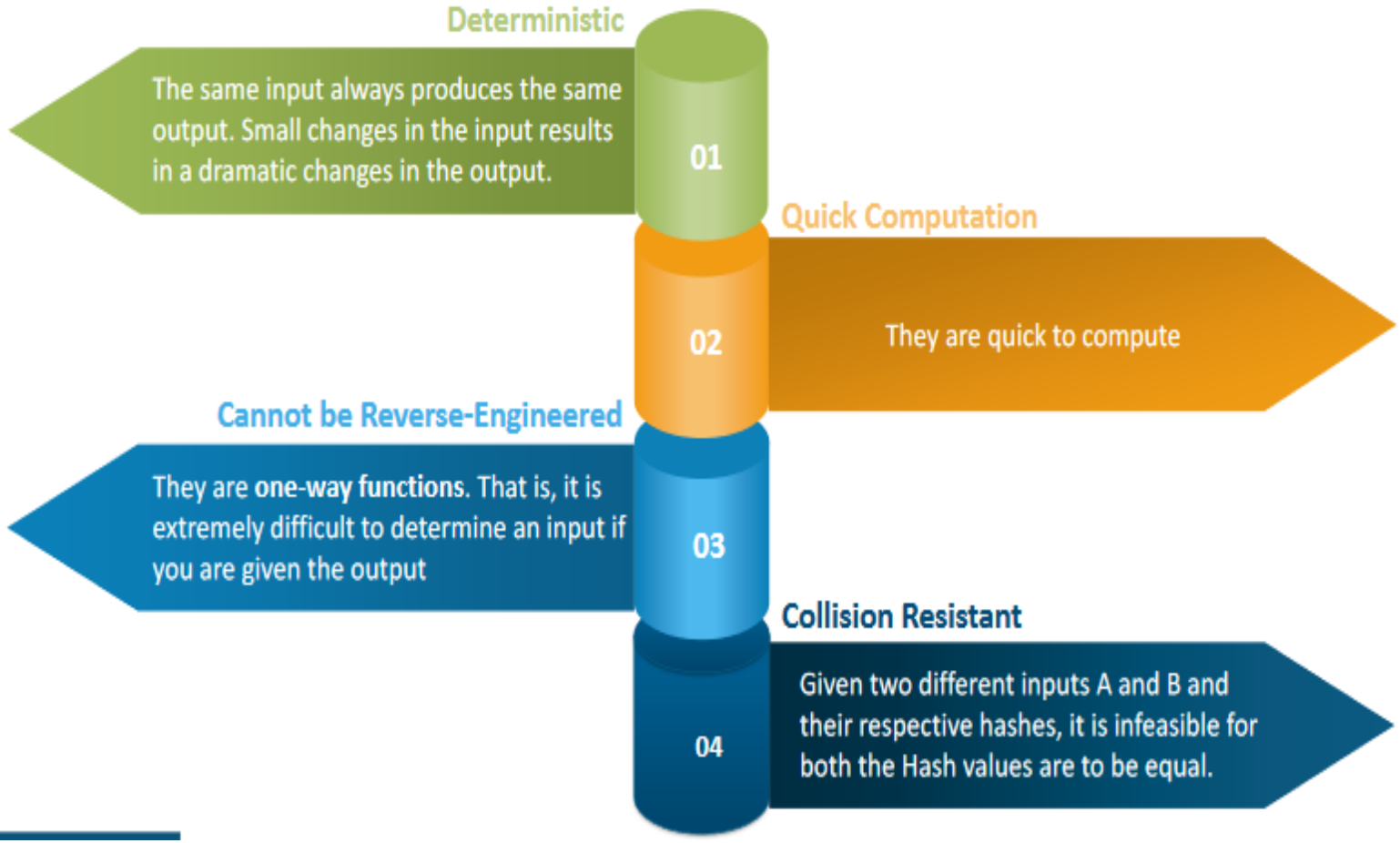
Example : Passwordgenerator.net sha256.

Hash Function

- **Hashing** is a mathematical process that takes input data of any size, performs an operation on it and returns string of ***random letters and numbers of fixed size***.
- **Hash Function** is a programmatically developed method, which perform the hashing.

Example of Hashing :
a0680c04c4eb53884be77b4e10677f2b

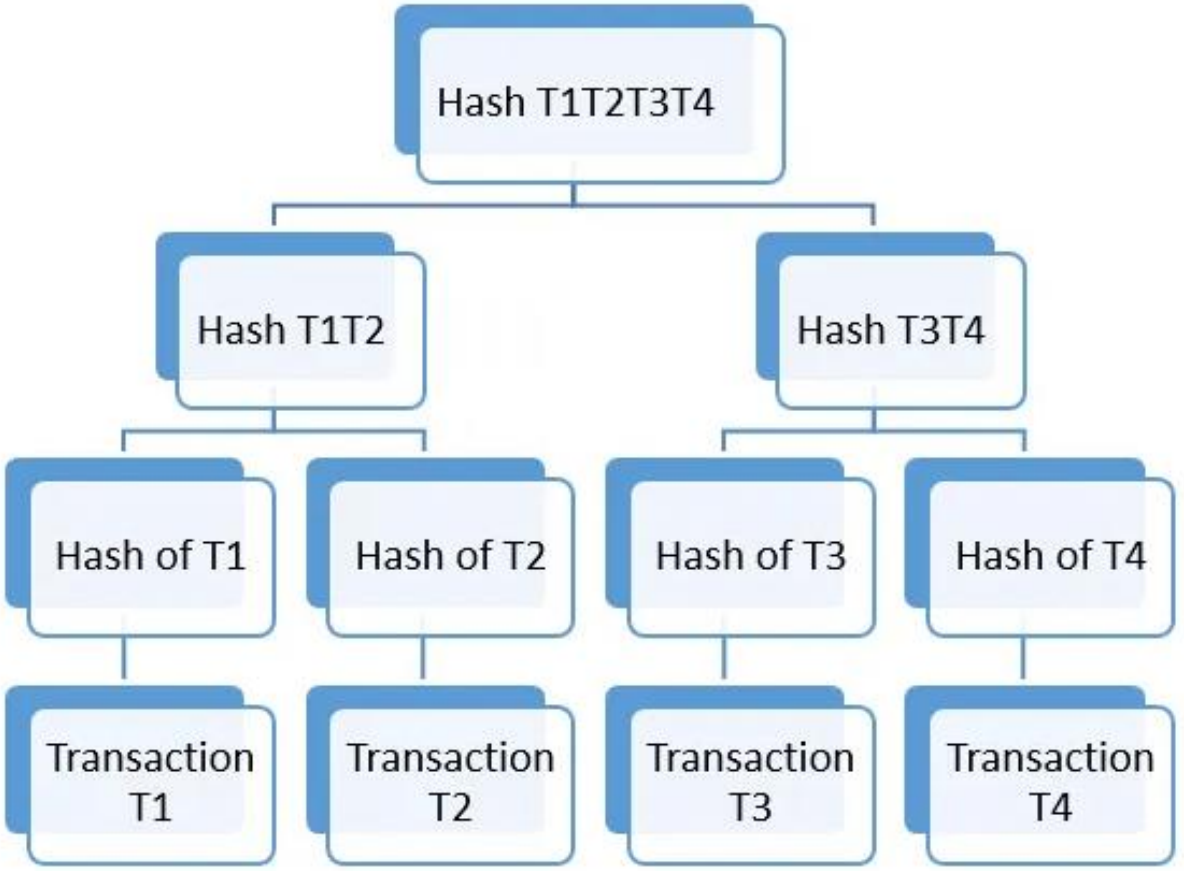
Properties Of Hash Functions



- Merkle Tree
- The concept was patented by Professor Ralph Merkle back in 1979. Now it helps to solve problems in large decentralized networks.
- A Merkle tree is a data structure that is used for secure verification of data in a large content pool. It is also efficient and consistent when it comes to verifying the data.
- Ethereum and Bitcoin both utilize Merkle Trees. Problem in blockchain : Each data is copied among the nodes. So, it is a challenge to efficiently access data.
- The challenge is also to make a copy of the data and share it among nodes. On top of that, the shared data needs to be verified for each of the receiving nodes.

- Solution :
- Merkle Trees enable decentralized blockchains to share data, verify them, and make them trustworthy. Merkle trees are data structure trees where the non-leaf node is defined as a hash value of its respective child nodes. The Merkle tree is inverted down where the leaf nodes are the lowest node. At the core of Merkle trees, we need to learn three important terms. They are as below:
- Merkle Root
- Leaf Nodes
- Non-Leaf Nodes

The tree is capable of summarizing a whole set of transactions by itself. This means that the user can verify if a transaction is part of the block or not.



Introduction to Bitcoin

- Bitcoin
  - Released in 2008 by Satoshi Nakamoto.
  - Focus on crypto-currencies and micro-payments
  - Proof of Work Consensus

What is Bitcoin?

- A peer-to-peer internet currency that allows decentralized transfers of value between individuals and businesses

- Bitcoin is the official first cryptocurrency that had been released in 2009. It is basically a digital currency and only exists electronically.
- Bitcoin is the first successful electronic cash system and coincidentally, the first instance of a successful Blockchain.
- Bitcoin introduced the concept of cryptocurrency; decentralized digital money secured by cryptography, and used to create valuable digital assets that cannot be counterfeited.

- Bitcoin transactions are authorized in a peer-to-peer network.
- Each node stores the history of the chain of blocks, containing validated transactions
- Counterfeiting is impossible because if one node's history is corrupted the others stay the same, and no central authority (i.e. bank) needs to confirm; this is called decentralization

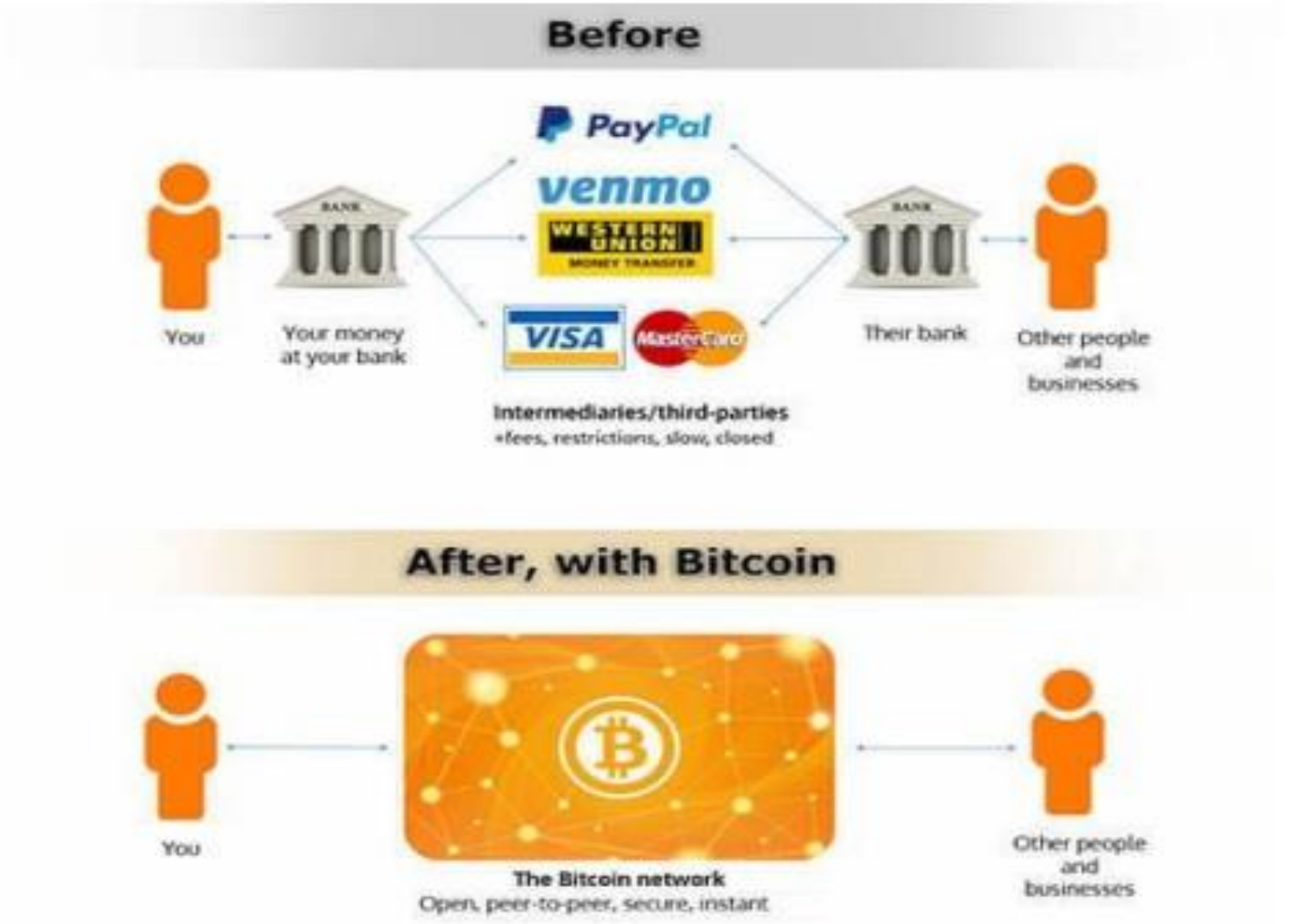


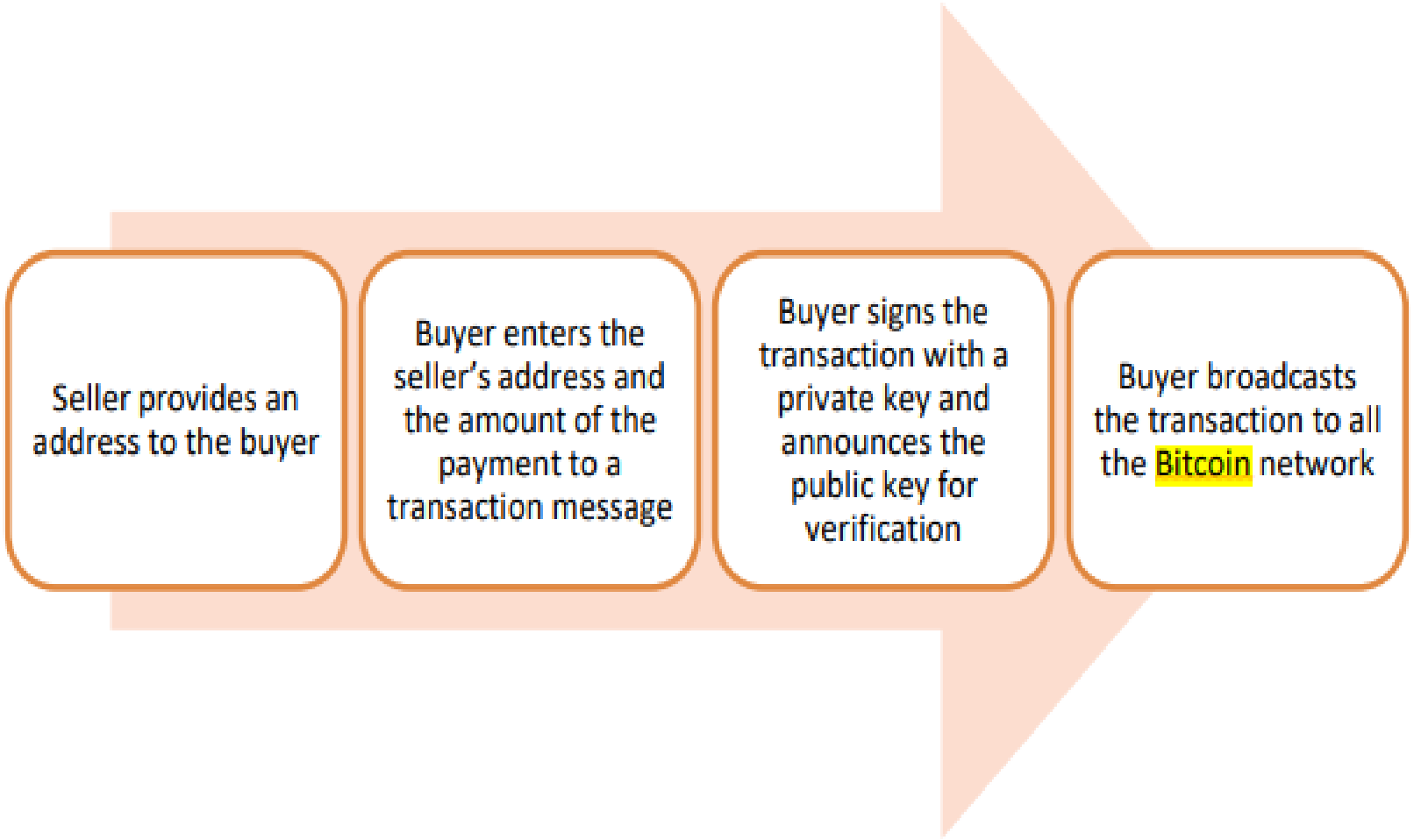
Figure 1.28 before and after bitcoin

Mining bitcoins

- Miners solve complicated algorithms to find a solution called a hash.
- Finding a hash creates a block that is used to process transactions.
- Each new block is added to the block chain.
- Until there are 21 million bitcoins, miners are paid for finding a hash in new coin.
- After 21 million, miners will charge transaction fees for creating a new block.
- The amount paid per hash goes down by half about every 4 years.

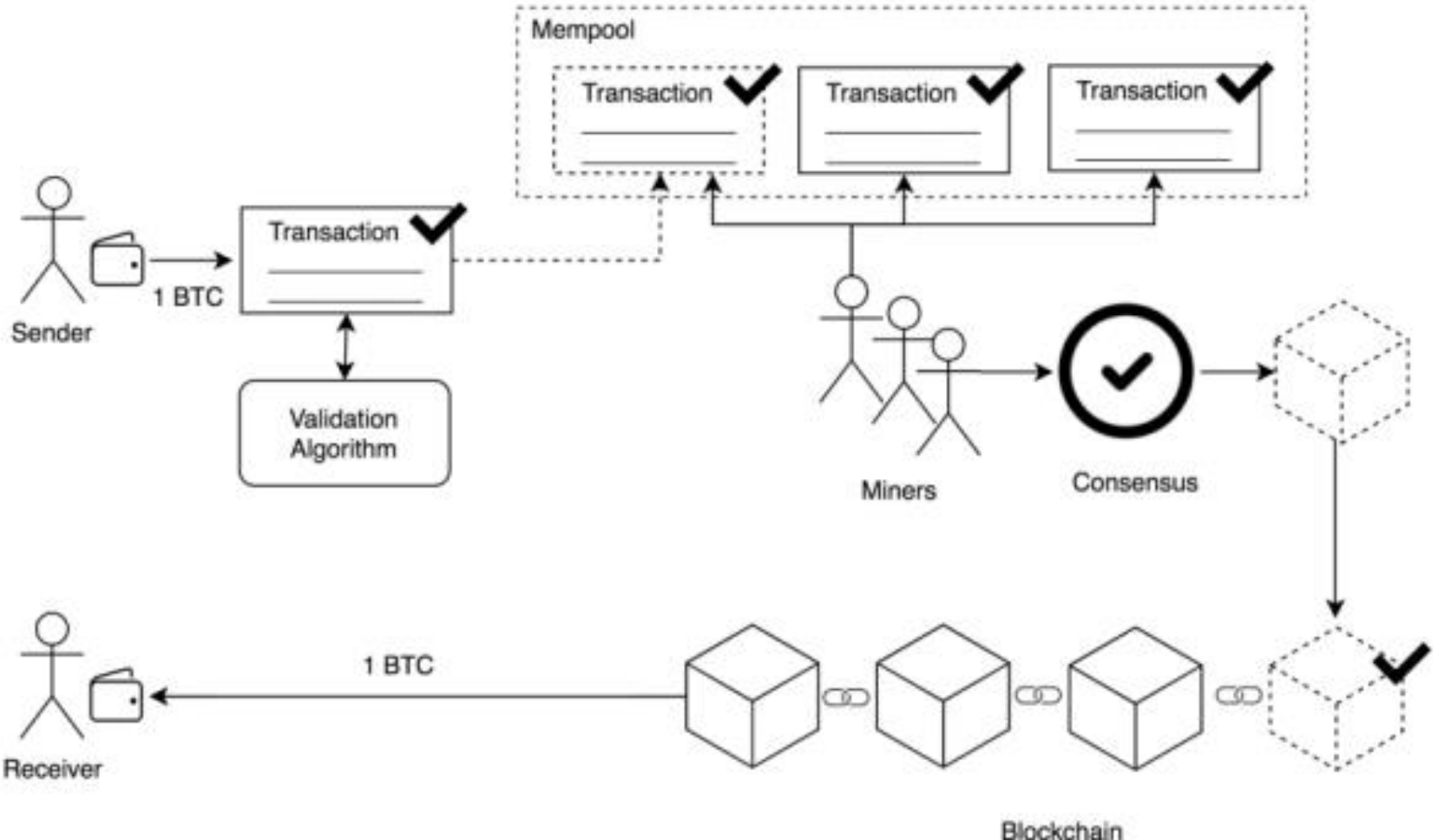
- Owning bitcoins
  - Users create accounts called wallets.
  - Wallets are secured using passwords and contain the private keys used for transferring bitcoins.

Spending bitcoins



The Bitcoin lifecycle

- Sender wants to send 1 Bitcoin to Receiver. This is what is going to happen:



Bitcoin Life cycle

1.Sender creates a transaction.

2. Sender's bitcoin wallet validates the transaction. 3. The transaction is sent to Mempool.

4. Miners get the transaction from Mempool and start mining the block using a consensus algorithm.

5. After the block is fully mined, it is added to the network.

6. The chain validates the new block and every peer in the network will get the blockchain with the new block added.

7. Finally, the Receiver get your BTCs

Introduction to public key Cryptography

Digital Signatures for Blockchain

- Digital Signature stands apart from an electronic signature due to its advanced encryption. It is akin to an electronic fingerprint, which verifies a person’s identity and secures documents.

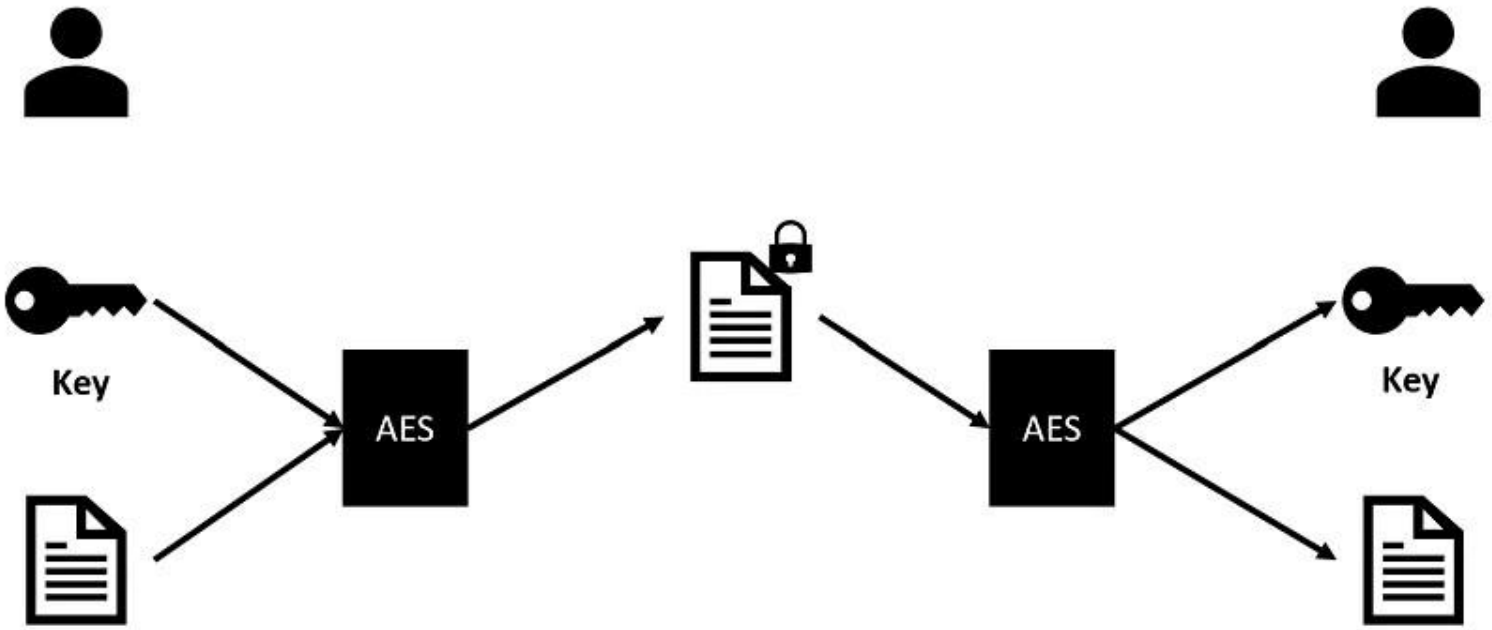
Types of Cryptography

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

- Symmetric Digital Signatures

- A Symmetric digital signature uses a single key to encrypt the messages.
- The sender encrypts the message with that key and sends it to the receiver.
- Once the receiver receives it, they need the SAME key to decrypt or unlock that message.
- So, the sender also shares the key they encrypted the message with so that the receiver can use it to decrypt the message.

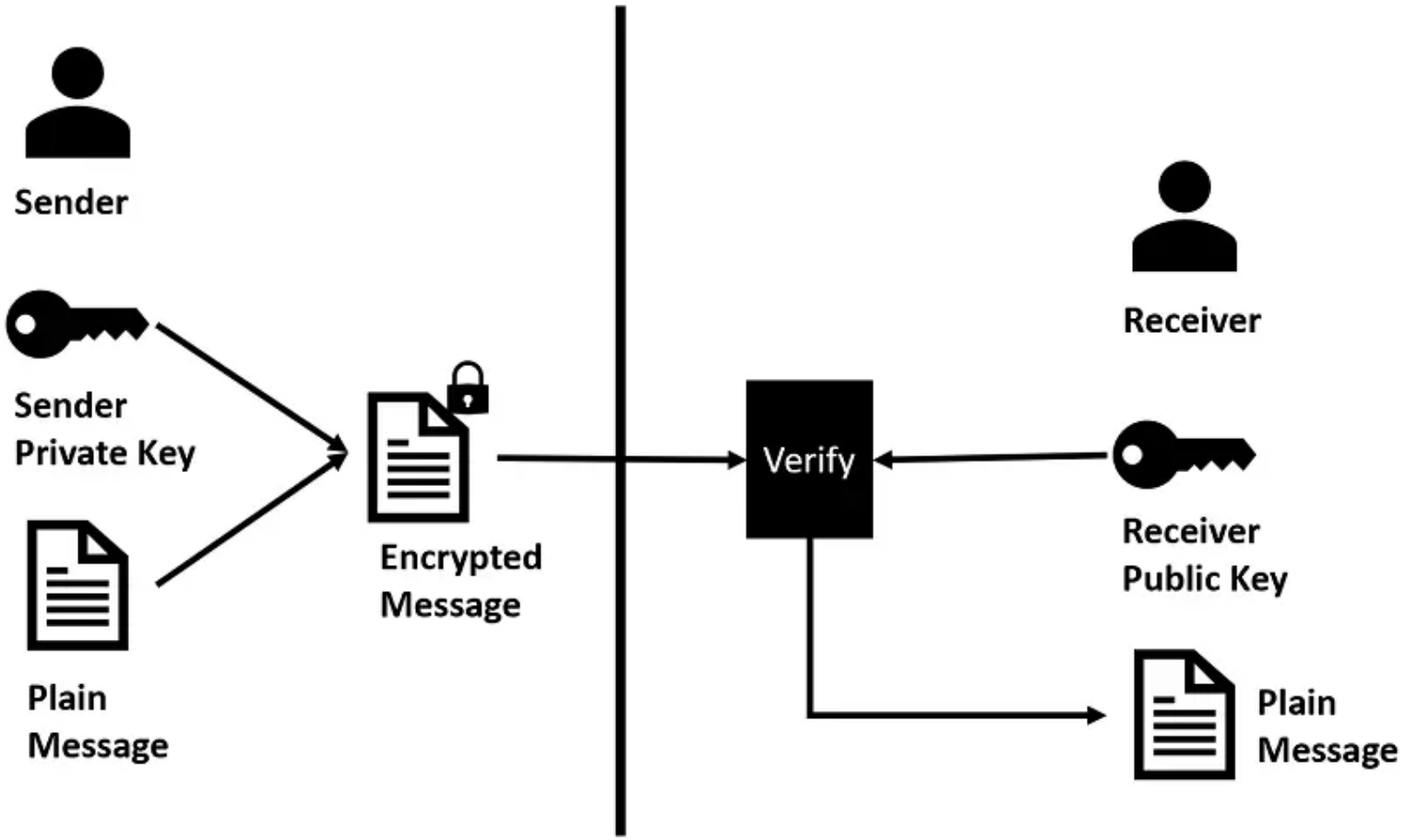
Symmetric Key Cryptography

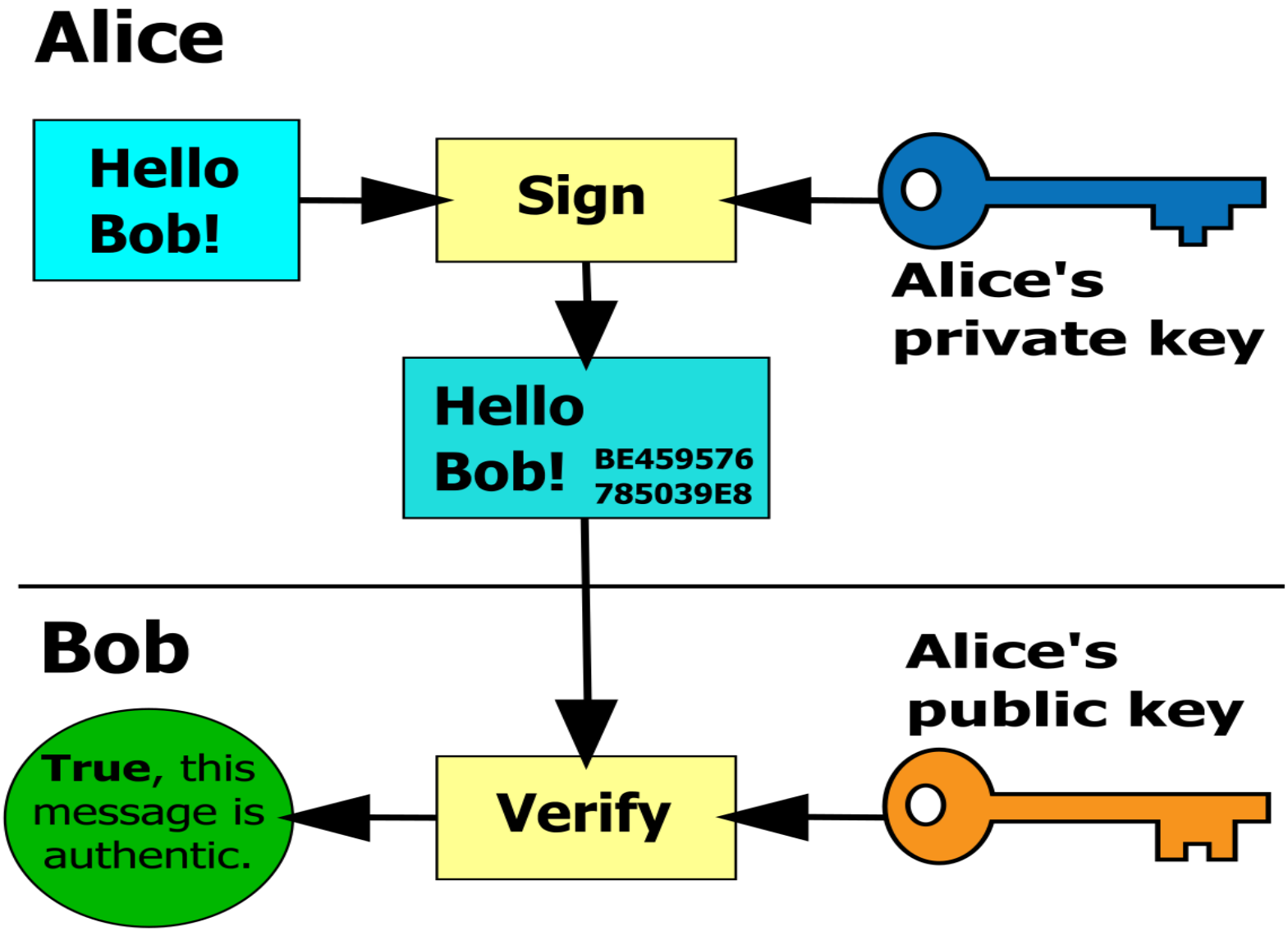


- **Asymmetric Digital Signatures**

- The acceptance of asymmetric digital signatures is much more than symmetric digital signatures. Asymmetric digital signatures use a pair of public and private keys.
- A message encrypted with a public key **can only** be decrypted with the corresponding private key of the public-private key pair and vice versa.
- The public key of each participant is shared across the network, and the private key is held secret only by the individual

Asymmetric Digital Signatures




Alice
Hello Bob!
Sign
Alice's private key
Hello Bob!
BE459576
785039E8
Bob
Alice's public key
True, this message is authentic.
Verify