Pakistan Blockchain Institute

PAKISTAN BLOCKCHAIN INSTITUTE

MODULE-2
BLOCKCHAIN AND SMART CONTRACT BASICS

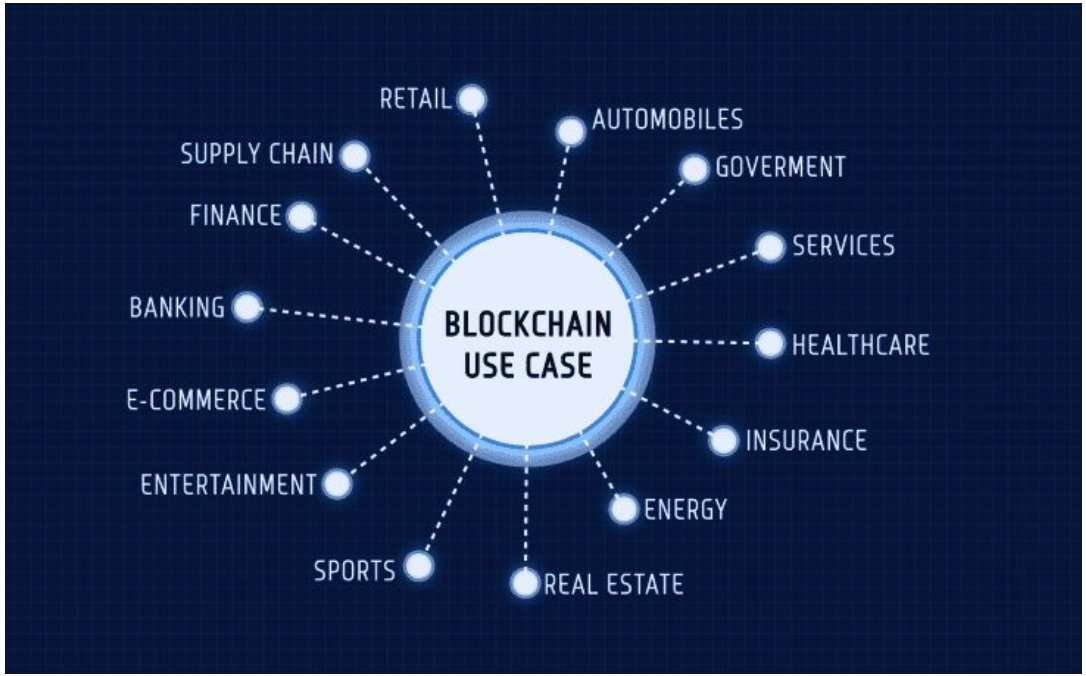
Class-2

Raja Rizwan Saleem
Lead Blockchain Trainer

Edversity.

BLOCKCHAIN USE CASES

WHAT IF;



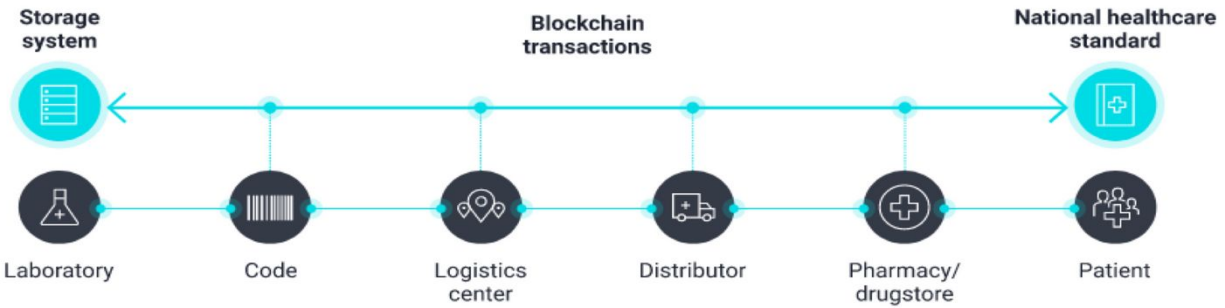
Edversity.

RECORD MANAGEMENT

- Case Study-1 (Real Estate)
- Case Study-2 (Car Registrations)
- Case Study-3 (Govt. record)
- Case Study-4 (Identity Management)

PHARMA

- End to End Drug traceability
  - Blockchain application helps overcome the increasing risk of counterfeit or unapproved drugs
  - Transactions are timestamped, drugs are registered by smart contract, pill containers are identified, and a complete path of origin



REAL TIME USE-CASES

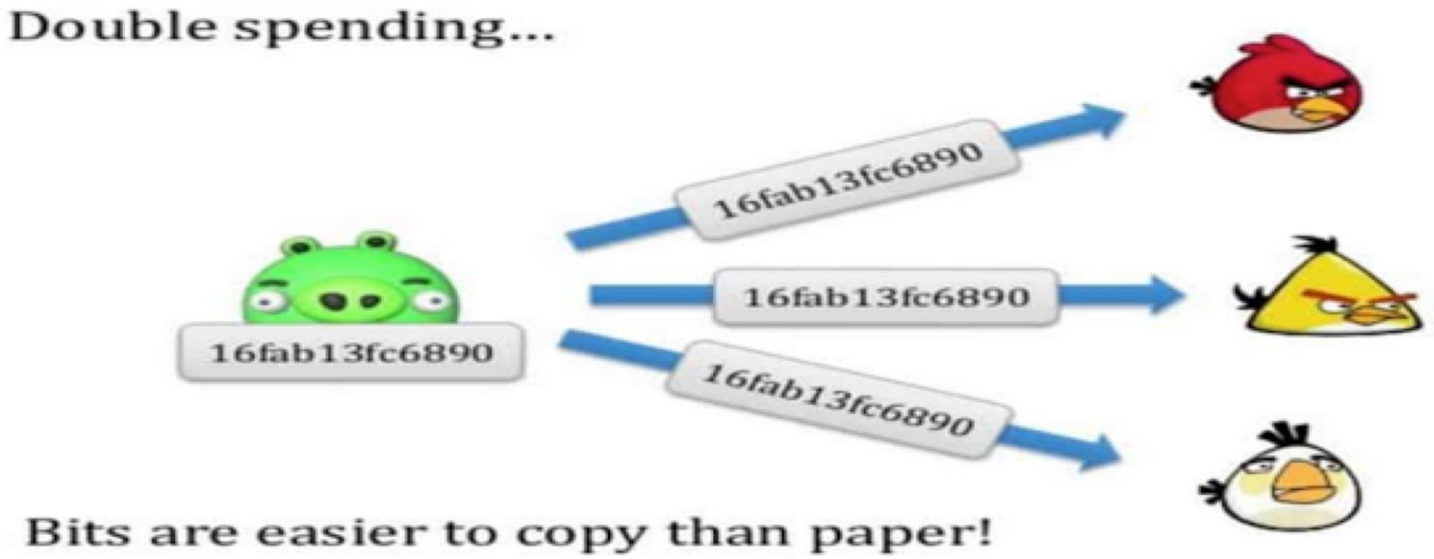
REAL TIME CASE-STUDIES

- Bitcoin
- Crypto Kitties
- Walmart

WHAT IS BITCOIN?

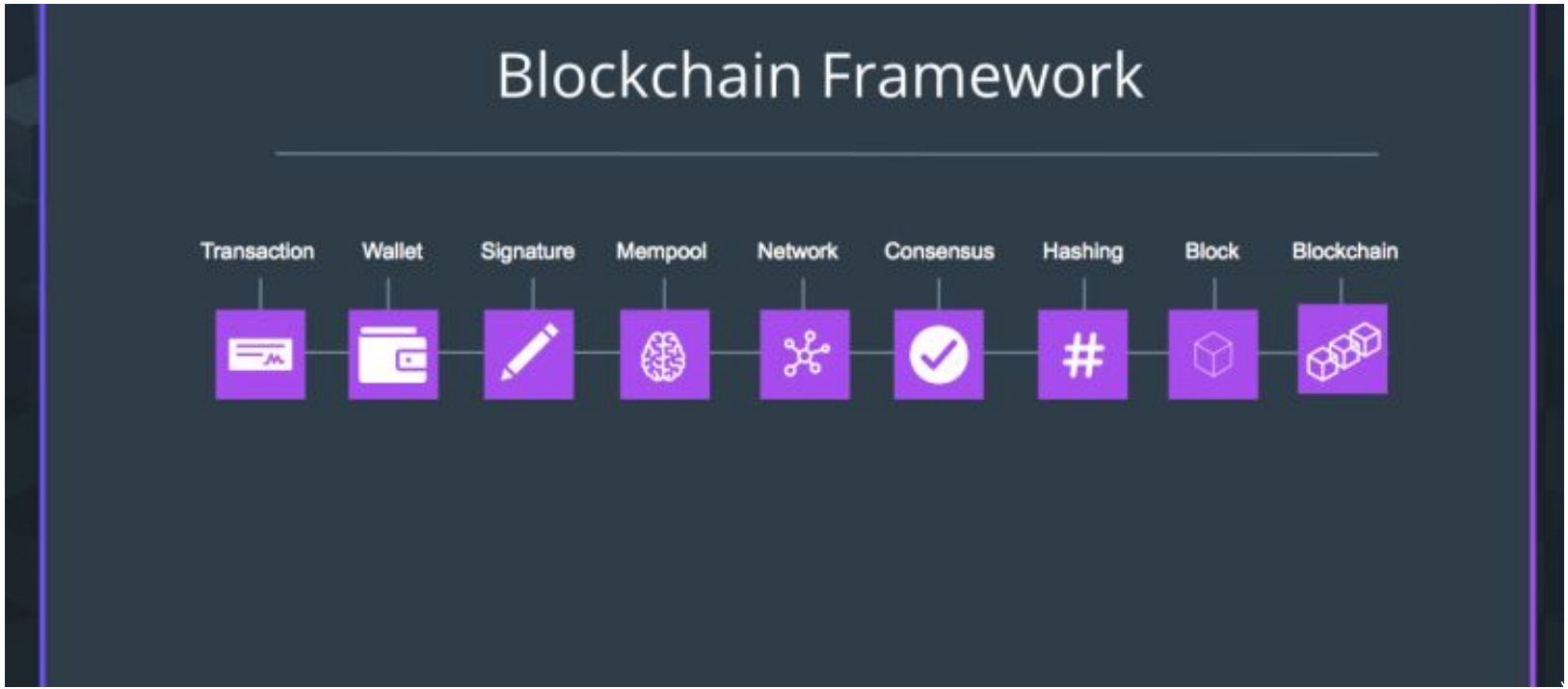
- White paper has been published in 2008
- White paper is written by Satoshi Nakamoto (No body know who he is or he is single person or group of people)
- Bitcoin is peer to peer cash system
  - Which have been made to bring one common currency in the world
  - But it’s not using as it’s required
  - It’s not a currency as per the definition of currency mentioned in Google
  - It’s like Prize Bond, Saving Certificates or Lottery Ticket
- Total limit of Bitcoins is 21 Million which will be completed by Year 2140

WHAT PROBLEM IT SOLVED?



HOW BITCOIN WORKS?

Blockchain Framework



PEOPLE ARE IMPORTANT

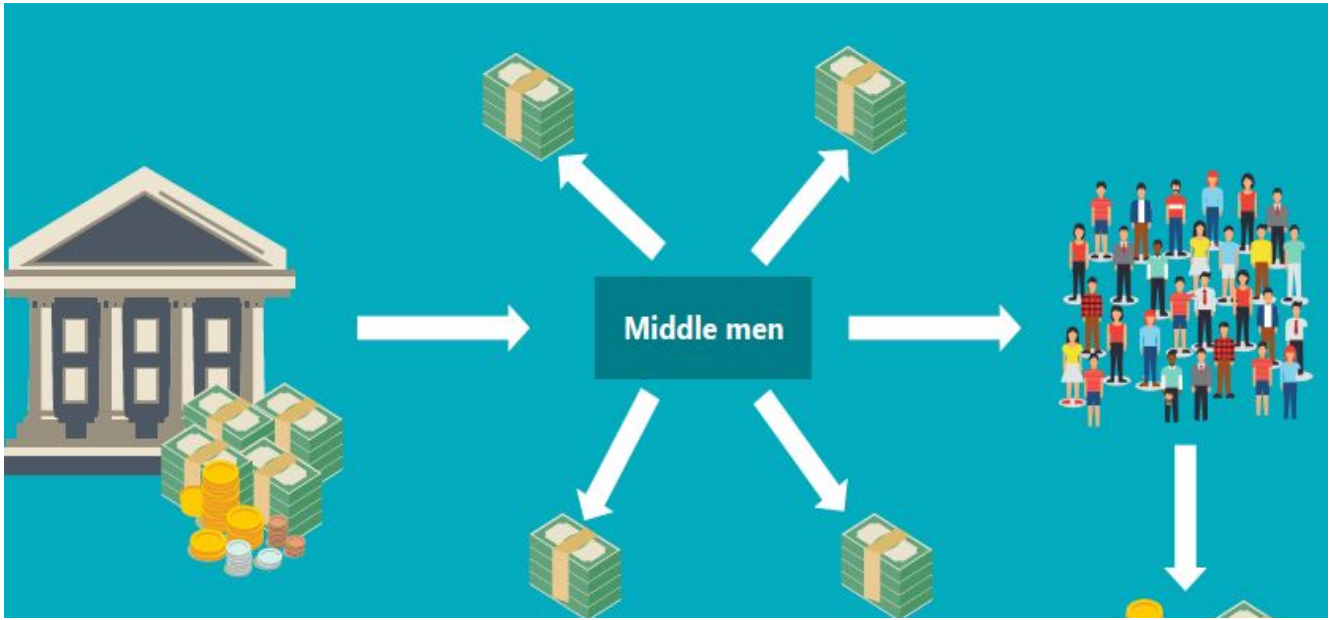
Efficient flow of data is of paramount importance

Edversity.

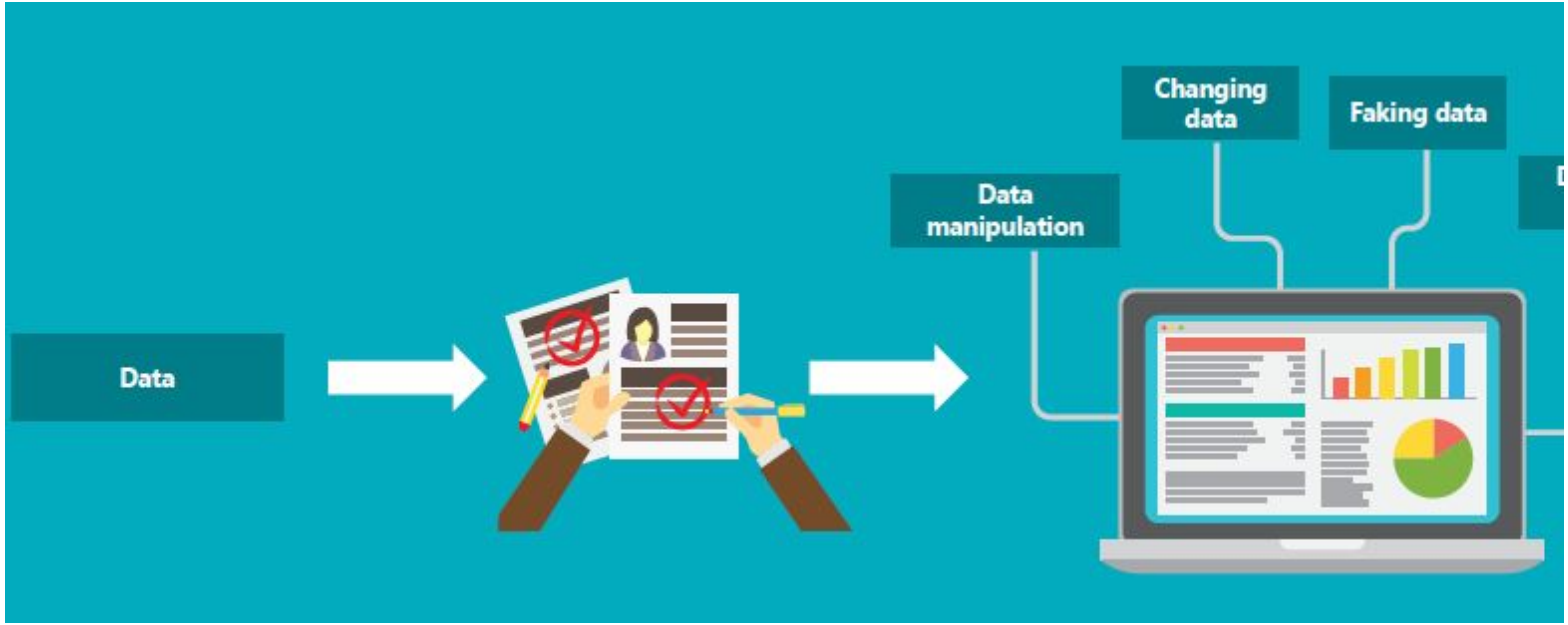
ISSUES IN TRADITIONAL SERVICES

- Middle Man
- Labor intensive paperwork
- Slow inter-bureaucratic communications

DATA STORED IN CENTRALISED



VERIFICATIONS



Edversity.

GOOD GOVERNANCE

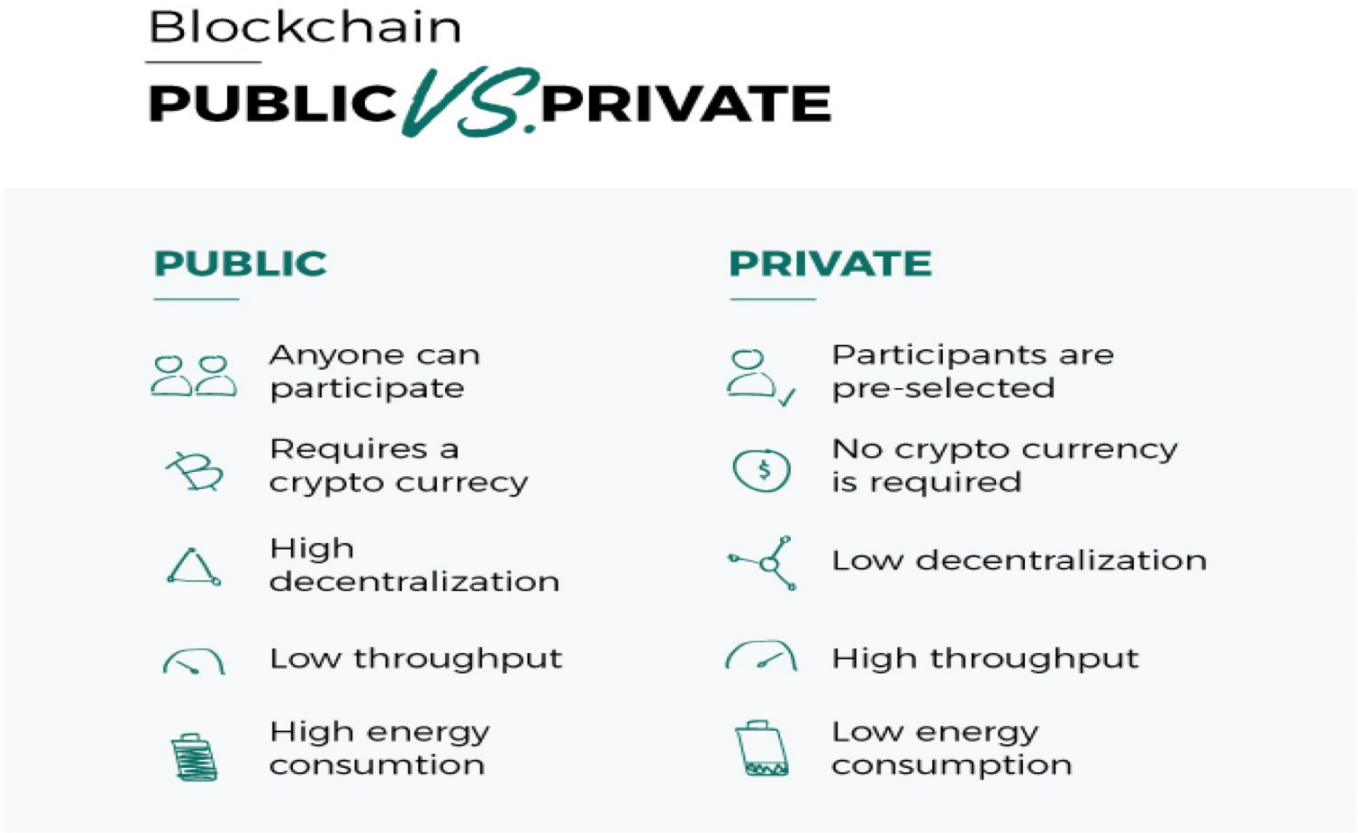
- In my view Blockchain will stop
  - Money laundering
  - Certificate Forgery
  - Fraud
  - Identity Theft
  - Corruption
  - Forge Health Records

BLOCKCHAIN FRAMEWORKS

Edversity.

BLOCKCHAIN FRAMEWORKS

- Private
- Public



Performance Vs Privacy Vs Security

	Public	Private
Access	Anyone	Single Organization
Participants	Permissionless & Anonymous	Known Identities
Security	Consensus Mechanism	Pre-approved Participants
Consensus	Proof-of-Work (PoW) Proof-of-Stake (PoS)	Voting Consensus
Transaction Speed	Slow	Lighter and faster

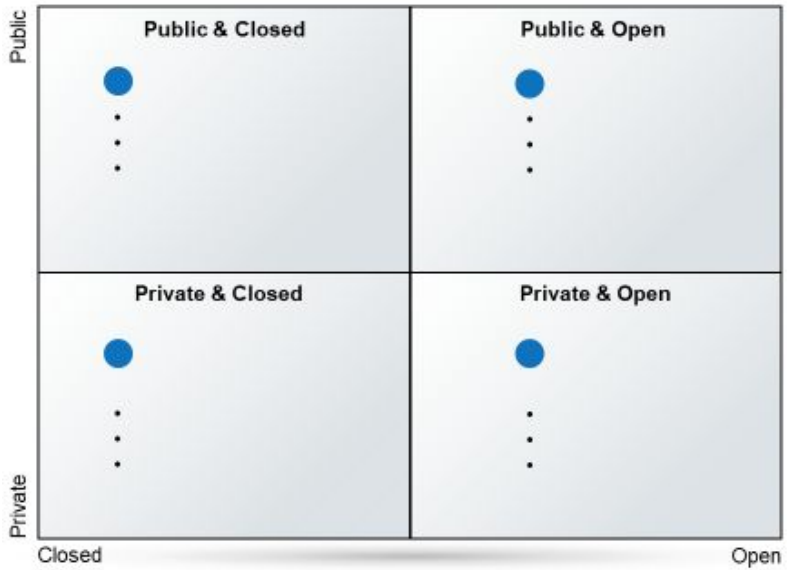
	Private blockchain	Public blockchain	Consortium blockchain
Access	Private	Public	Public/Private
Consensus	Organization based	Public	Selected nodes
Efficiency	High	Low	High
Centralization	Yes	No	Partial
Consensus Process	Permission based	Permissioned based	Permissionless
Immutability	Not completely tamper-proof	Completely tamper-proof	Not completely tamper-proof

TYPES OF BLOCKCHAIN

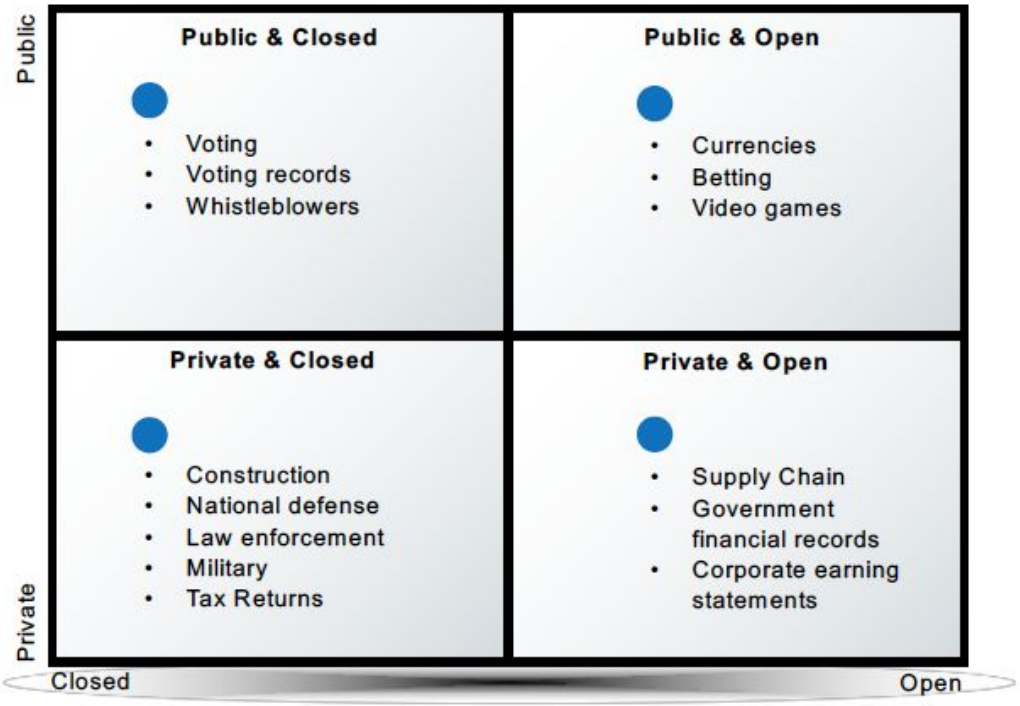
- Public vs Private
  - Who can write data to the Blockchain?
  - Public – everyone can add a record
  - Private – only certain participants can write data
- Open vs Closed
  - Who can read data from the Blockchain?
  - Open – everyone can read Blockchain data
  - Closed – only certain participants can read data

BLOCKCHAIN DECISION

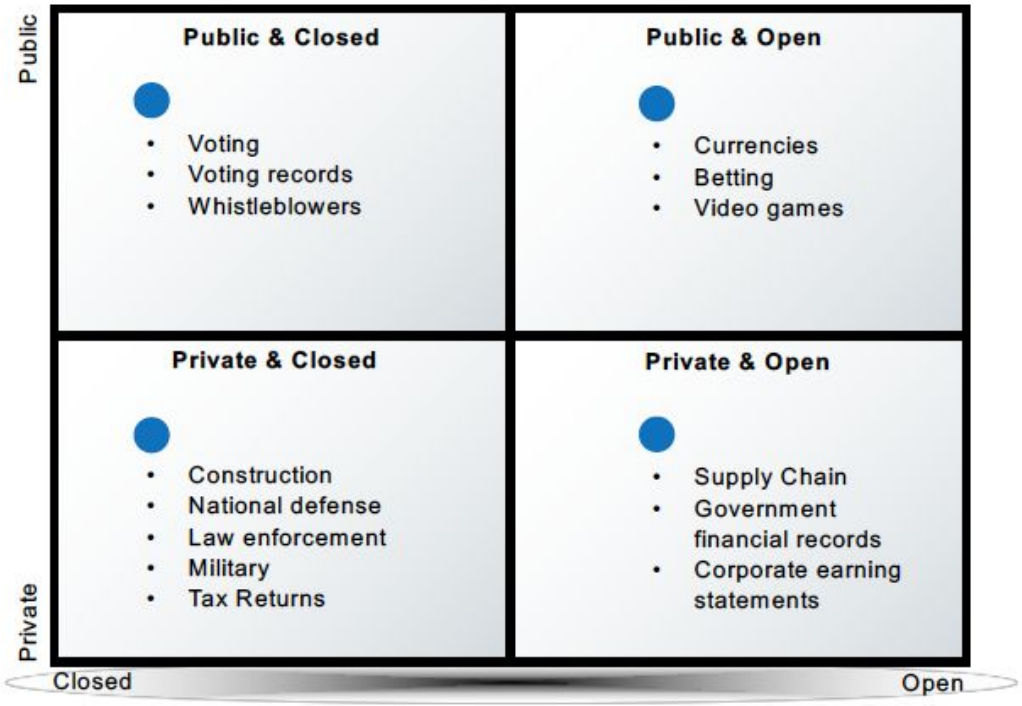
- Currency
- Securities exchange
- Video game
- Voting records
- Supply chain data
- Government financial records
- Corporate earnings statements
- Construction tracking
- Defense programs
- Law enforcement agencies
- Others?



BLOCKCHAIN DECISION MATRIX



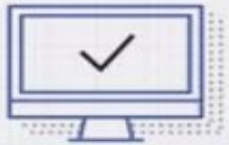
BLOCKCHAIN DECISION MATRIX



Transaction Life Cycle

A new transaction is entered.

The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.



This network of computers then solves equations to confirm the validity of the transaction.

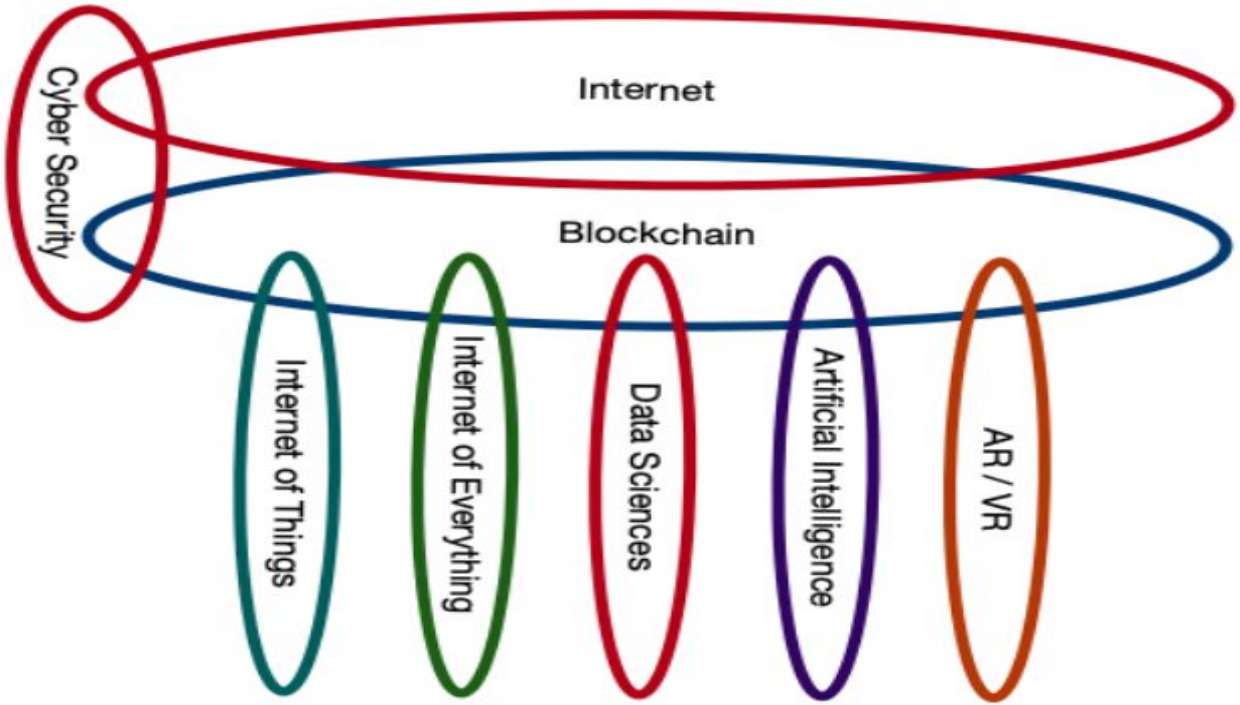
Once confirmed to be legitimate transactions, they are clustered together into blocks.

These blocks are then chained together creating a long history of all transactions that are permanent.

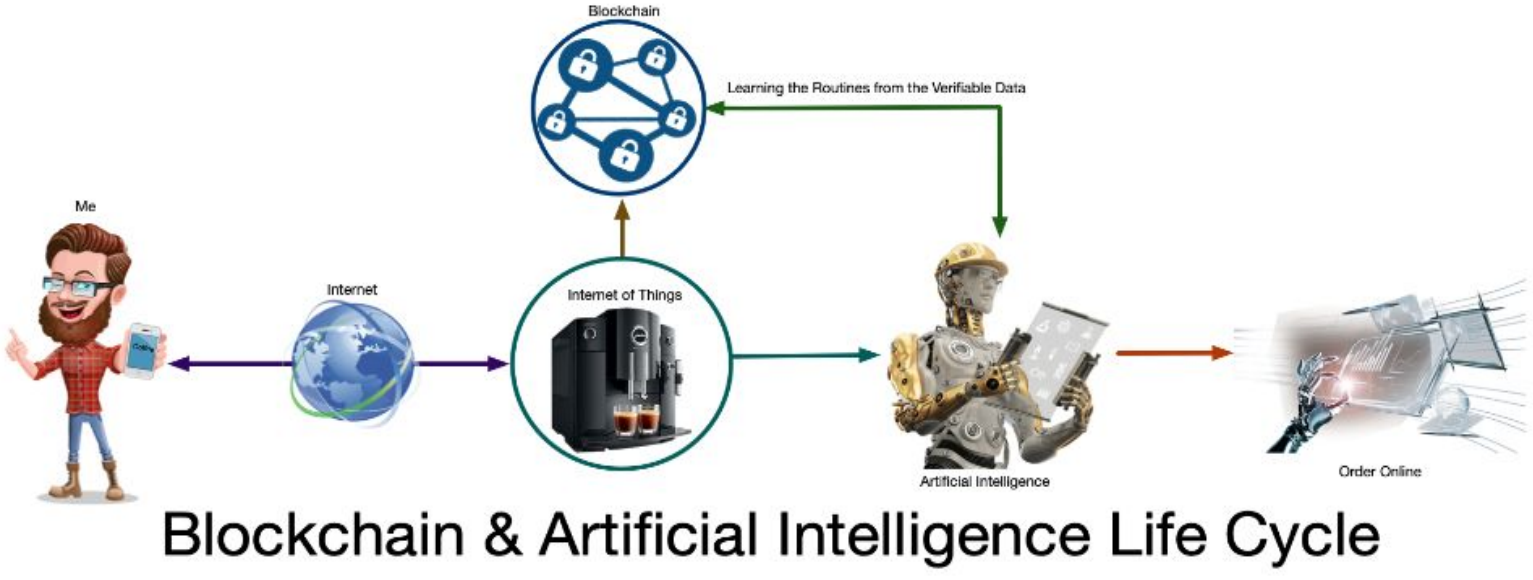
The transaction is complete.

BLOCKCHAIN WITH OTHER TECHNOLOGIES

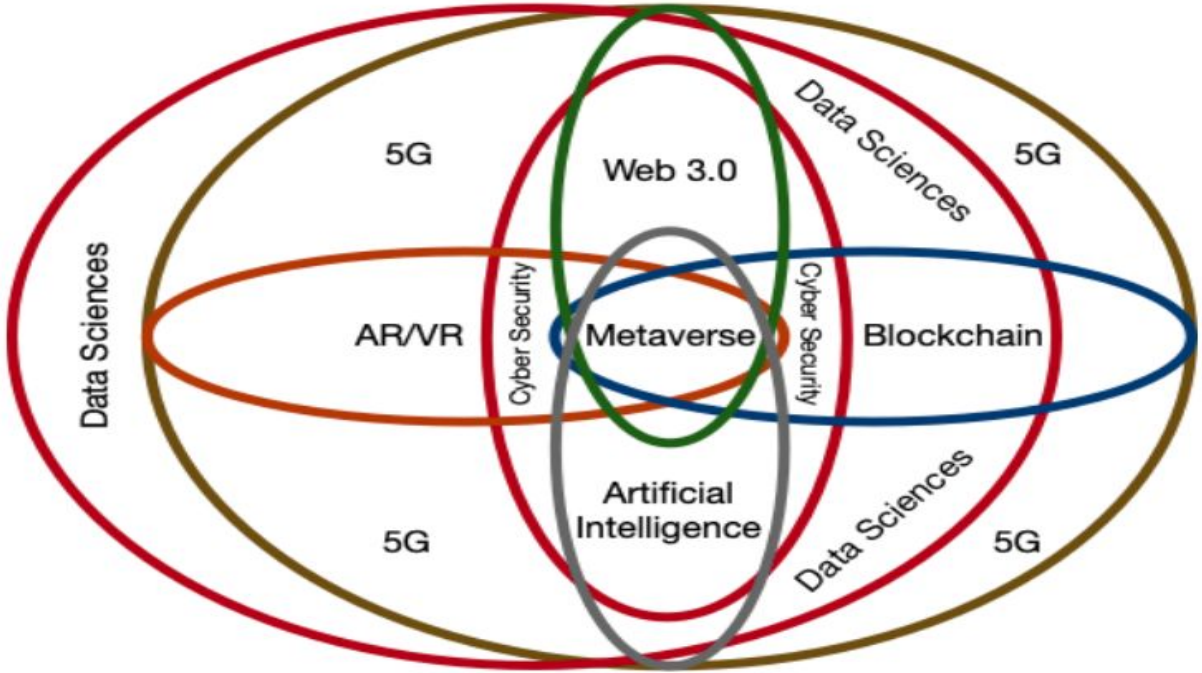
BLOCKCHAIN WITH OTHER TECHNOLOGIES



ROLE OF BLOCKCHAIN IN COMMUNITY



ALL TECHNOLOGIES CONNECTED



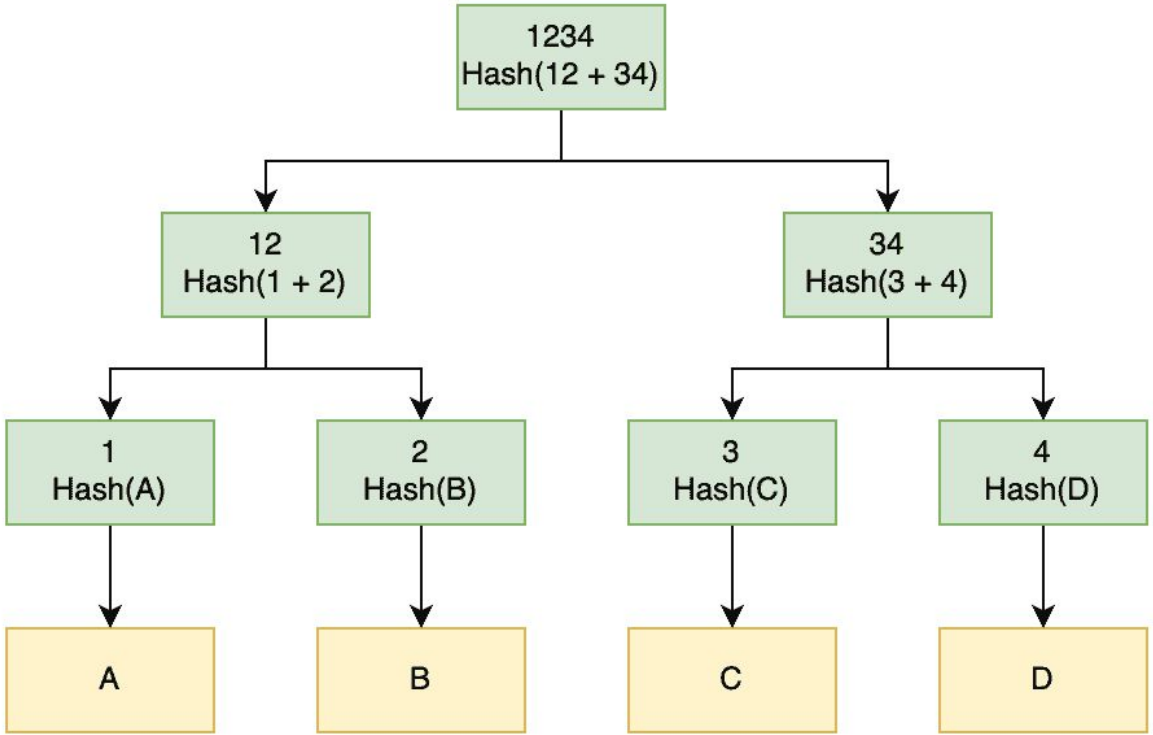
Edversity.

BLOCKCHAIN ADOPTION

THE FUTURE OF BLOCKCHAIN

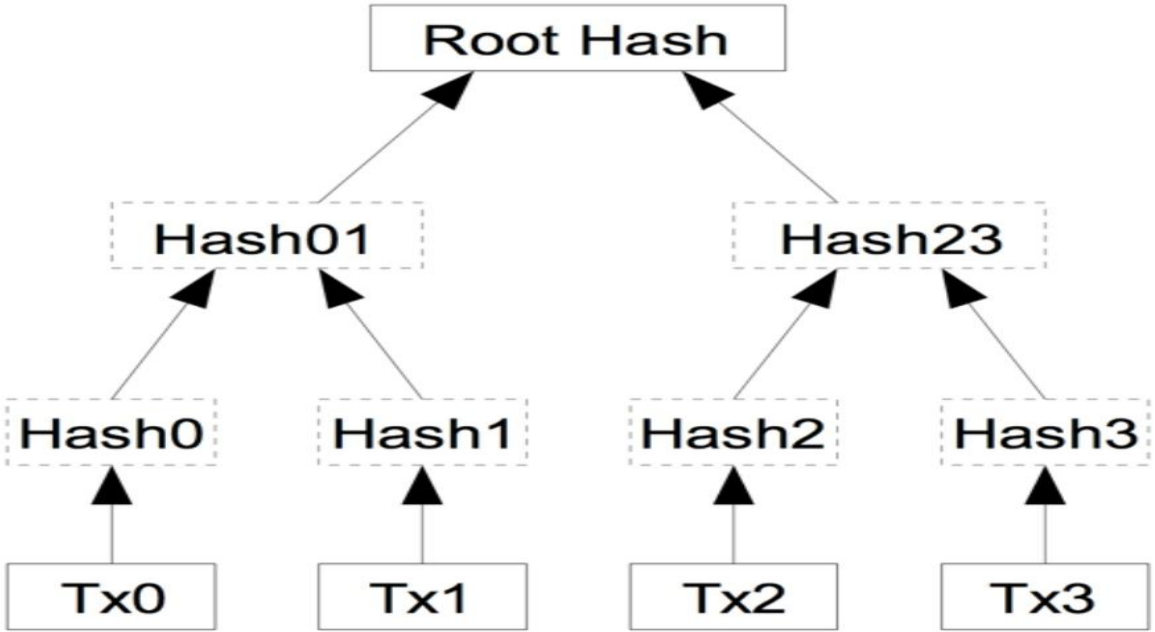
Edversity.

Markle Tree

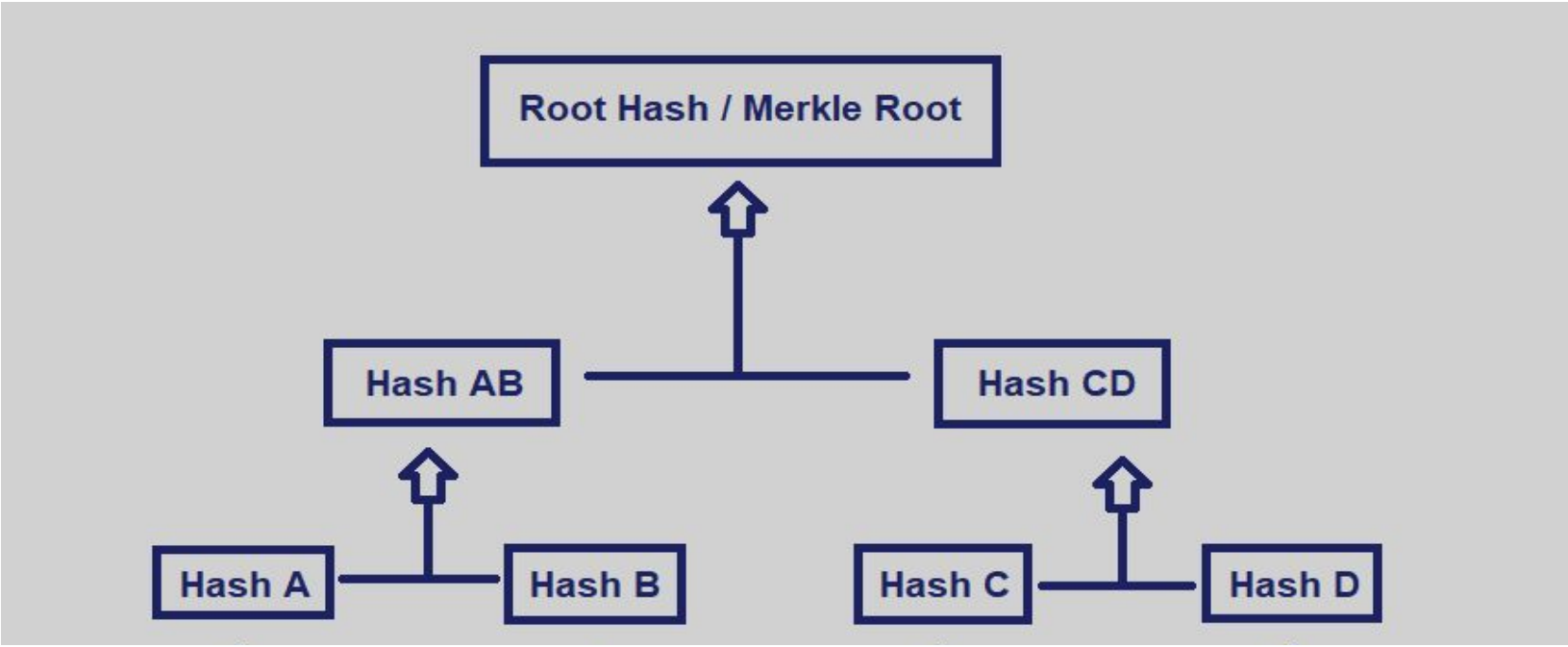


Features of Markle Tree

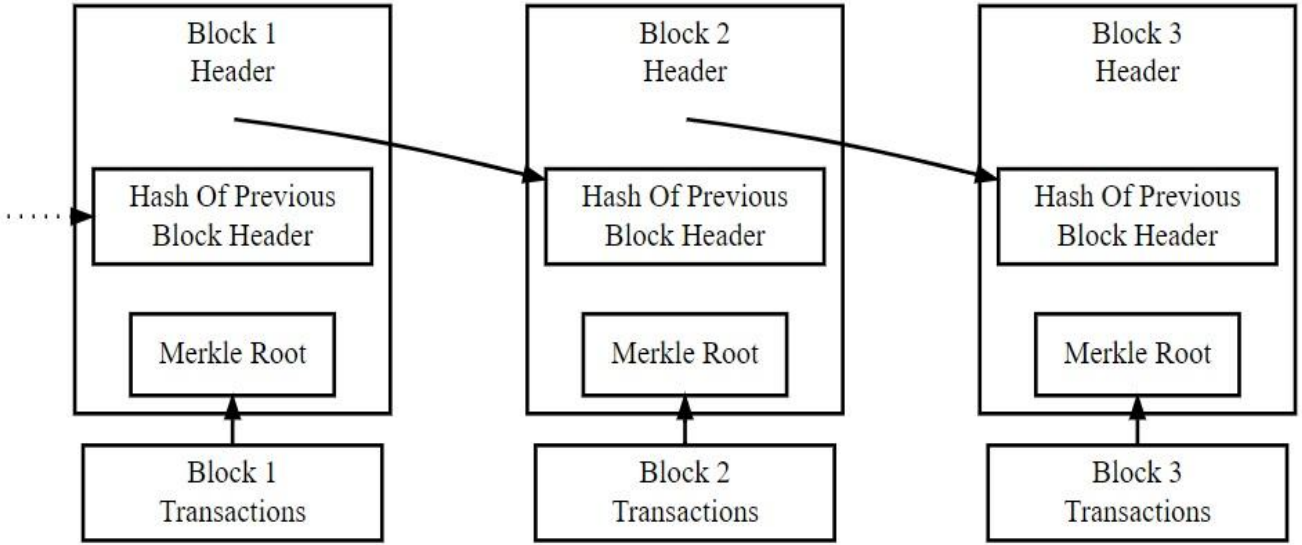
Markle Tree



Markle Tree



Merkle Tree



Merkle Tree Benefits

- **Efficient Verification**: Merkle trees offer efficient data integrity and validity verification and significantly reduce the amount of memory required for verification. Proof of verification does not require transferring large amounts of data over the blockchain network. Enable trusted cryptocurrency transfer in a peer-to-peer distributed system by quickly verifying transactions.
- **No Delay**: There is no delay when data is transferred over the network. Merkle trees are widely used in the calculations that keep cryptocurrencies working.
- **Less Disk Space:** Merkle trees take up less disk space compared to other data structures.

Merkle Tree Benefits

- **Tampering Detection:** The Merkle Tree offers an amazing advantage to miners in checking whether any transactions have been tampered with.
- Since transactions are stored in a Merkle tree, which stores the hash of each node in the top parent node, any changes to the transaction details, such as the amount to be debited or the address to which payment must be made, will propagate to the hashes in the upper levels and finally to the Merkle root.
- A miner can compare the Merkle root in the header with the Merkle root stored in the data part of the block and easily detect this manipulation.

What is Cryptography in Blockchain

What is Cryptography in Blockchain

Cryptography is a technique or protocol that secures information from any third party during communication. The word is composed of two Greek terms, the term Kryptos meaning “hidden,” and Graphein, meaning “to write”.

Terminologies related to Cryptography

Cryptography and Encryption Terms to Know

Cryptography: The practice of writing and solving codes

Key: A secret string of characters

Encryption: The mathematical process of creating and sharing an encoded message

Encryption algorithm: A set of algorithms that carry out the encryption

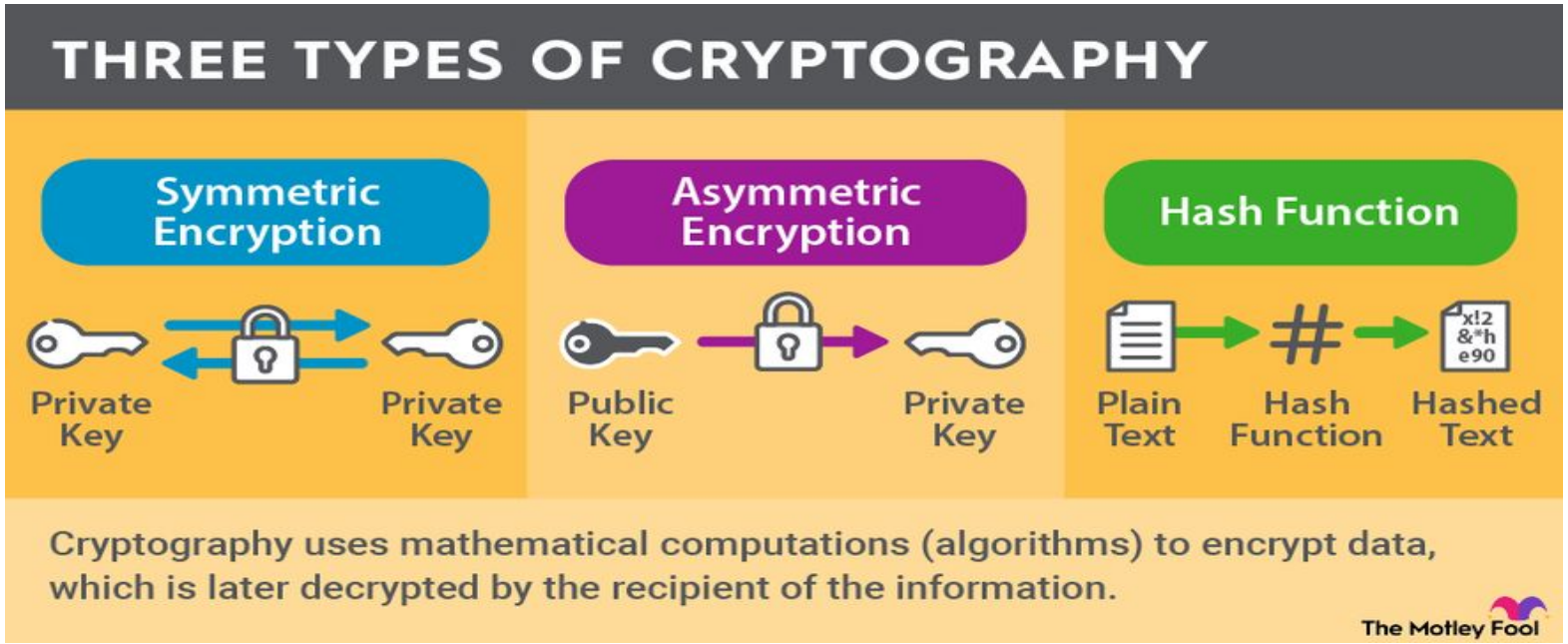
Ciphertext: The illegible form of an encoded message

Plaintext: The decoded message

Features of Cryptography

- The intended recipient and no one else can only access the information on a blockchain.
- Information cannot be changed while being stored or sent between a sender and the intended recipient without the addition of new information being noticed.
- The information creator/sender cannot later retract his desire to send information.
- The sender’s and receiver’s identities are verified. Additionally, the information’s origin and destination are verified.

Types of Cryptography



Edversity.

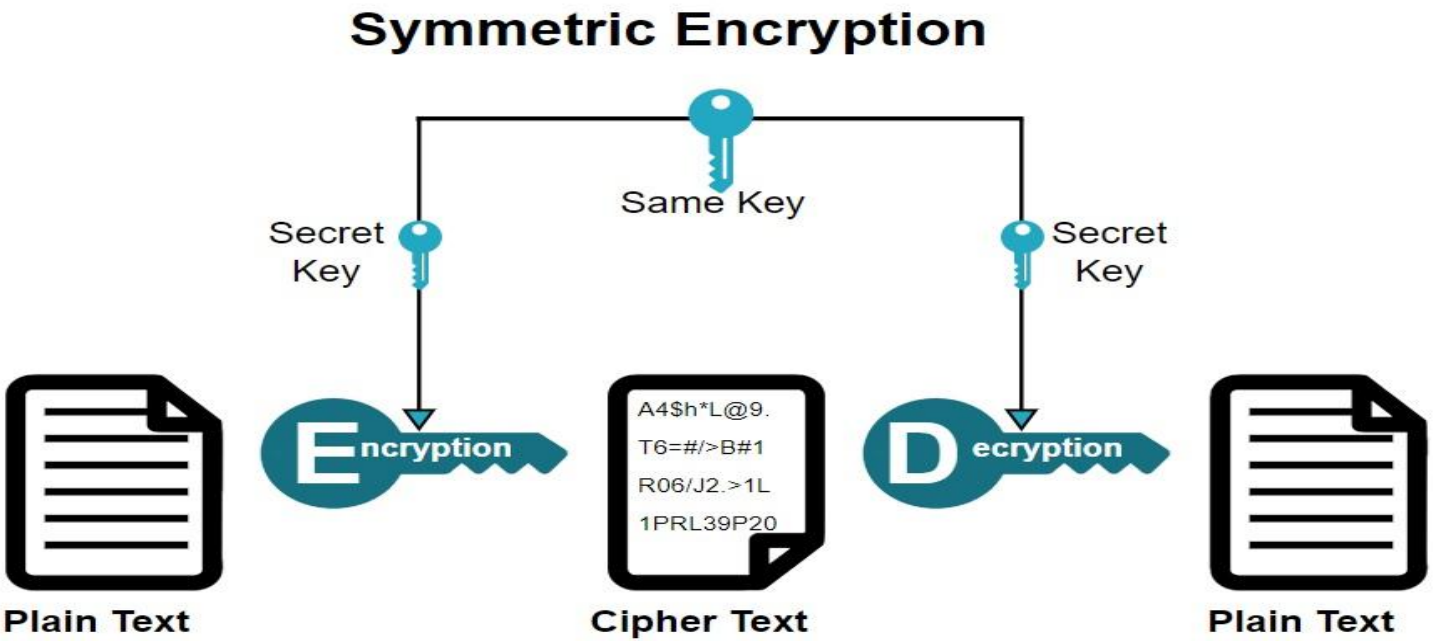
Types of Cryptography - Symmetric Encryption

This type of cryptography focuses on a similar key for encryption and decryption. Most importantly, the symmetric key encryption method is also applicable for secure website connections or data encryption. Also referred to as secret key cryptography. The only problem is that the sender and receiver exchange keys securely. The Data Encryption System (DES) is a popular symmetric key cryptographic system. A cryptographic algorithm uses an encryption key to encrypt data, which must be made available. The person entrusted with the secret key can decrypt the data. Examples: AES, DES, etc.

Features of Symmetric Encryption

- It is also described as secret key cryptography.
- Both parties have the same key to keep the secret.
- It is suitable for bulk encryption.
- It requires less processing power and faster transfer.

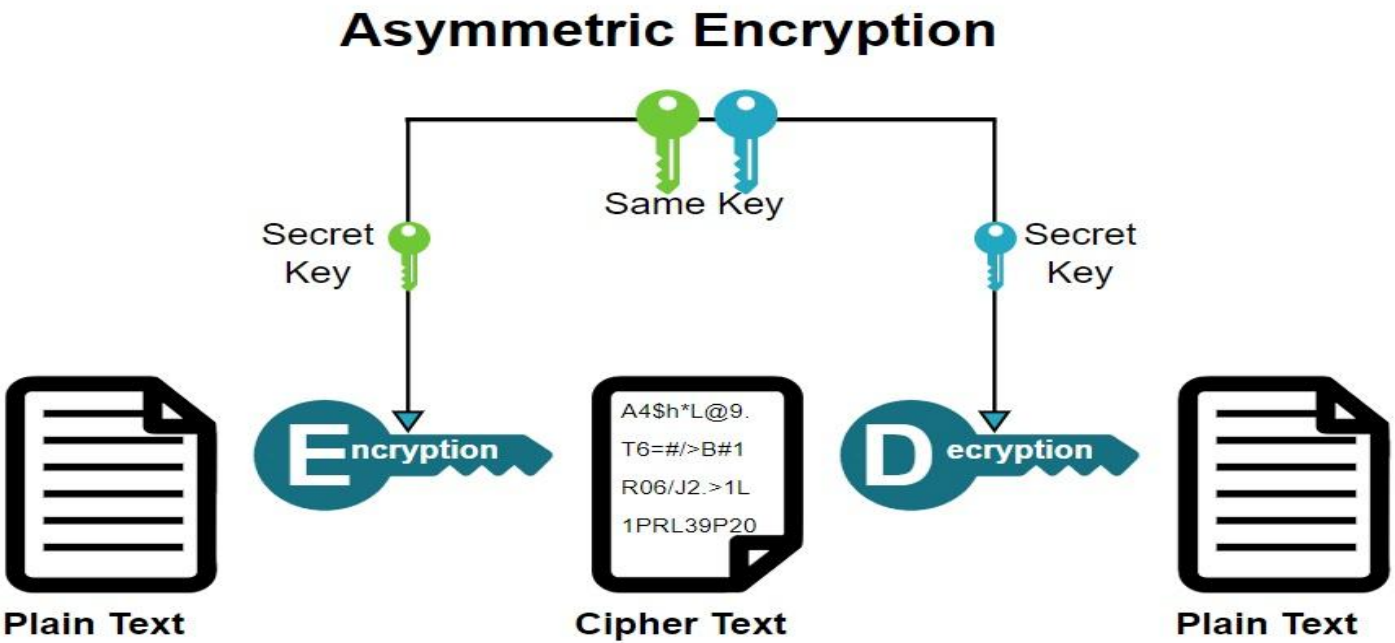
Types of Cryptography - Symmetric Encryption



Features of Asymmetric-Key Cryptography

- It is described as public key cryptography.
- It is often used for symmetric cryptography secret key sharing.
- It requires a long processing time to execute.
- It plays a significant role in the authenticity of the web server.

Asymmetric Encryption



Asymmetric vs. Symmetric Encryption

Asymmetric Encryption

- Two keys
- More secure
- Slower
- Newer technique

Symmetric Encryption

- One key
- Less secure
- Faster
- Older technique

Benefits of Encryption

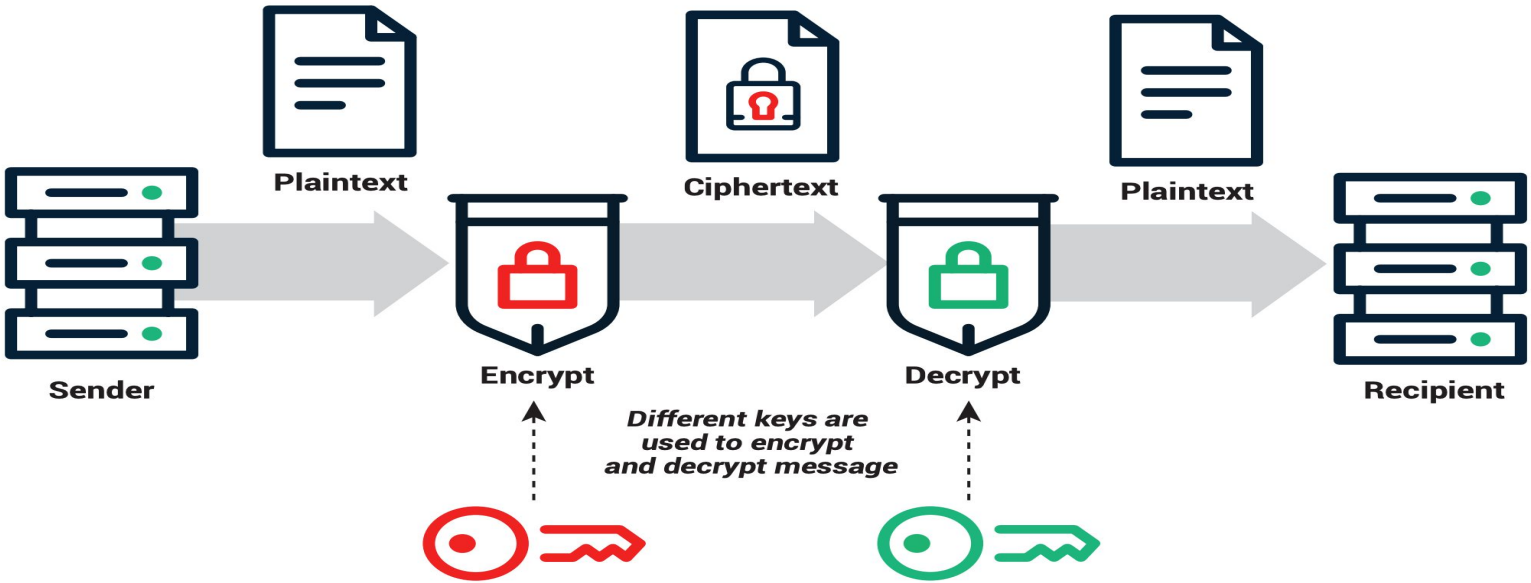
Security

Authentication

Privacy

Integrity

Encryption & Decryption



Thanks

End of Module-2 (Class-2)