ETHEREUM 2.0 MASTERY PROGRAM

Instructor: Raja Rizwan Saleem

MODULE-2

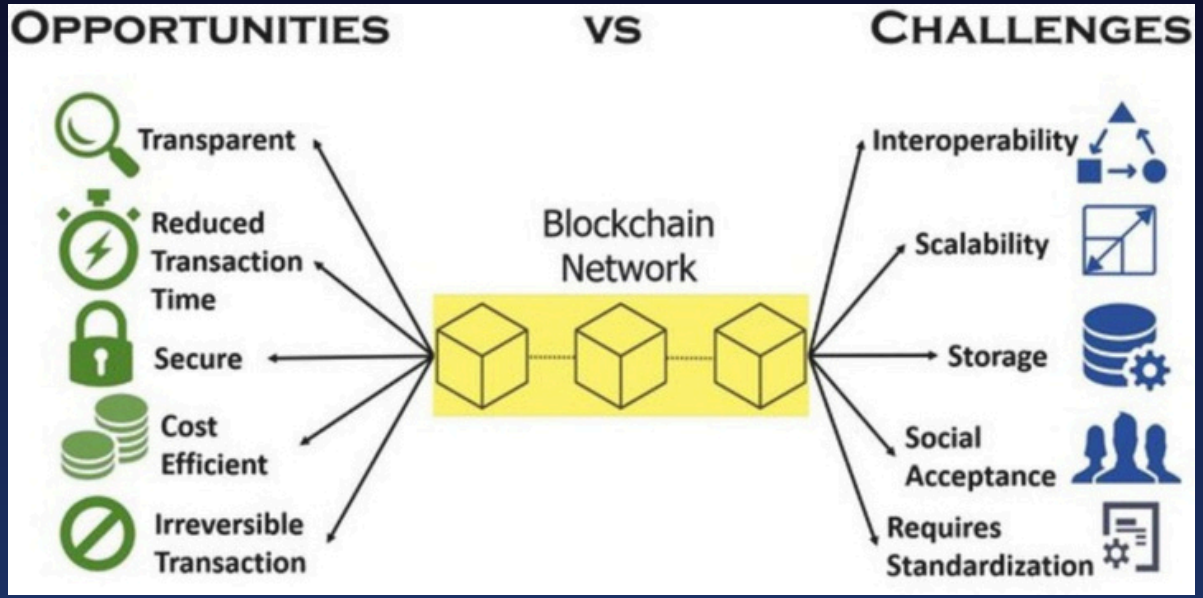
BLOCKCHAIN AND SMART CONTRACT BASICS

Raja Rizwan Saleem
Lead Blockchain Trainer

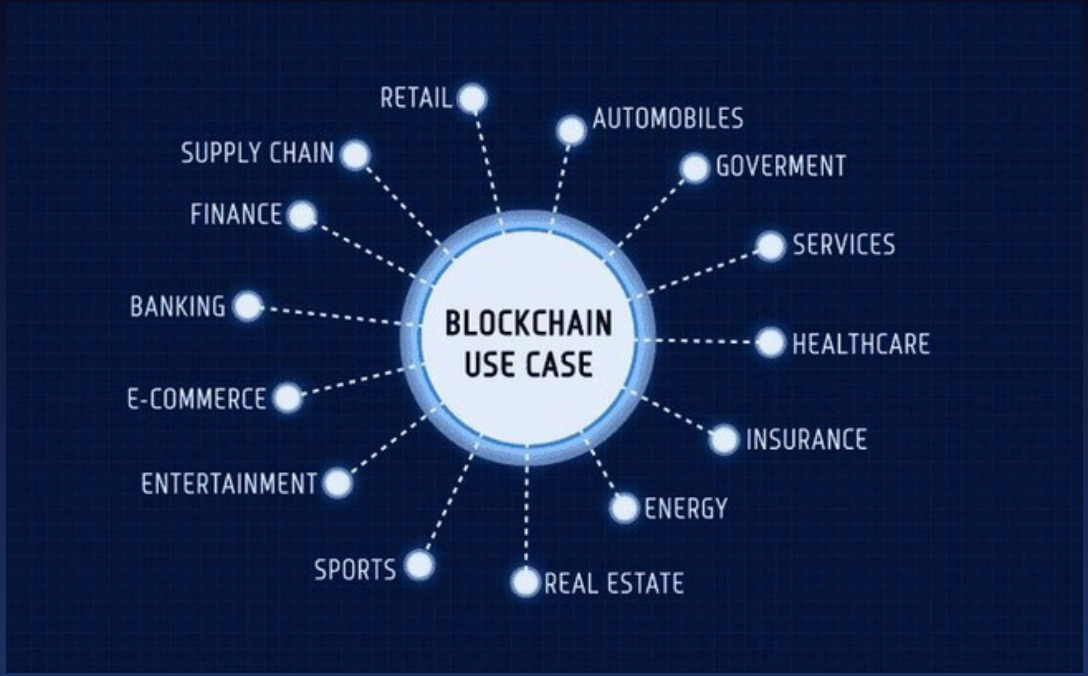
Class-02

BLOCKCHAIN USE CASES

Advantages and challenges related to the application of blockchain.

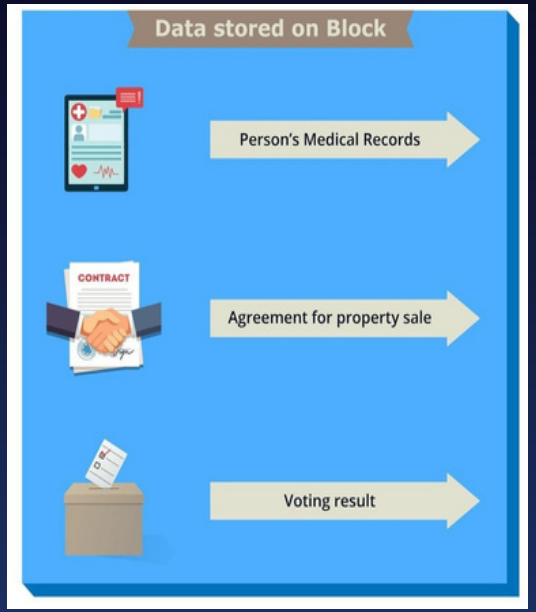


WHAT IF;


BLOCKCHAIN
USE CASE
RETAIL
AUTOMOBILES
SUPPLY CHAIN
GOVERMENT
FINANCE
SERVICES
BANKING
HEALTHCARE
E-COMMERCE
INSURANCE
ENTERTAINMENT
ENERGY
SPORTS
REAL ESTATE

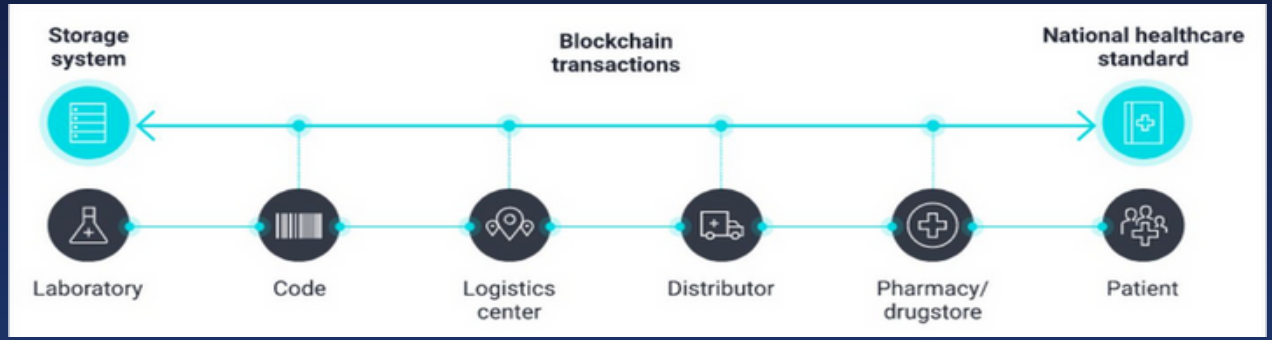
RECORD MANAGEMENT

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



Blockchain in 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



Blockchain in PHARMA

The global pharmaceutical industry is massive, worth around $1.2 trillion, but it still faces significant problems with inefficiency. Surprisingly, using blockchain technology could potentially save over $100 billion for pharmaceutical companies each year. It's clear that blockchain has the power to disrupt and greatly impact the pharmaceutical sector.

So, how does blockchain benefit the pharmaceutical industry?

Blockchain in pharmaceuticals improves drug authenticity, tracking, and data integrity, and secures data, reducing counterfeit drug risks. It simplifies supply chain management, automates compliance with smart contracts, and enables safe data sharing.

Blockchain in PHARMA

Counterfeit Drug Prevention

- Provides a secure and unchangeable record of transactions.
- Enhances traceability from manufacturing to the end consumer.
- Helps verify drug authenticity and prevent counterfeit distribution.
- Protects public health and pharmaceutical companies from fraud.

Blockchain in PHARMA

Supply Chain Management

- Offers real-time visibility and traceability across the supply chain.
- Ensures compliance with safety and regulatory standards.
- Enables efficient recalls by quickly identifying affected drugs.
- Enhances monitoring of production, shipment, and distribution.

Blockchain in PHARMA

Clinical Trials and Research Data Management

- Provides a tamper-proof ledger for clinical trial records.
- Ensures data authenticity and regulatory compliance.
- Improves transparency and collaboration between researchers.
- Reduces the risk of data manipulation or fraud.

Blockchain in PHARMA

Regulatory Compliance and Quality Control

- Creates an immutable audit trail for regulatory review.
- Simplifies compliance with industry standards.
- Reduces the risk of compliance violations and fines.
- Enhances quality control in drug manufacturing.

Blockchain in PHARMA

Patient Data Security and Privacy

- Ensures decentralized and secure medical data storage.
- Gives patients control over data access and sharing.
- Complies with data protection regulations (e.g., GDPR, HIPAA).
- Enhances trust and security in healthcare data exchange.

General Data Protection Regulation

Health Insurance Portability and Accountability Act

Blockchain in PHARMA

Smart Contracts for Automatic Transactions

- Automates payments, licensing, and supply agreements.
- Reduces administrative costs and manual intervention.
- Ensures secure and transparent contract execution.
- Eliminates the need for third-party intermediaries.

Blockchain in PHARMA

Streamlined Payments and Billing

- Provides a transparent and efficient billing system.
- Reduces delays and costs in transactions between stakeholders.
- Enhances trust and efficiency in financial operations.
- Facilitates faster reimbursement for healthcare services.

Blockchain in PHARMA

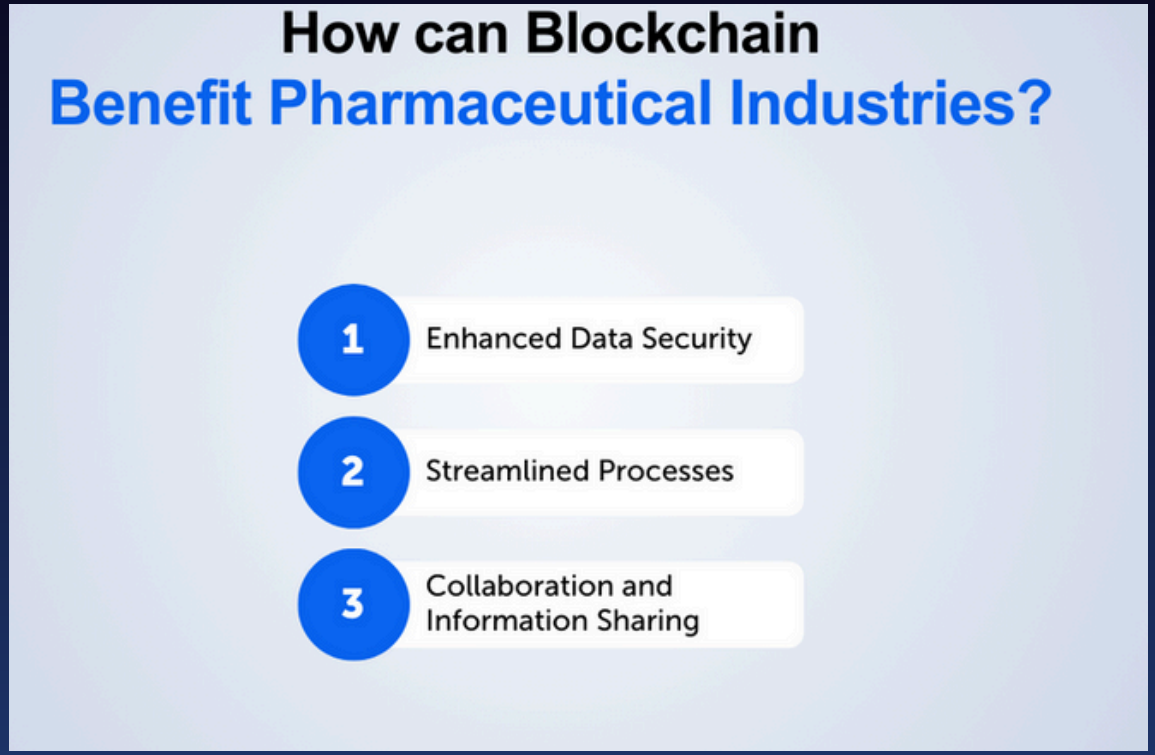
Enhanced Collaboration and Innovation

- Enables secure and transparent data sharing.
- Facilitates cross-industry collaboration (pharma, research, healthcare).
- Accelerates the development of new drugs and therapies.
- Encourages innovation in pharmaceutical technologies.

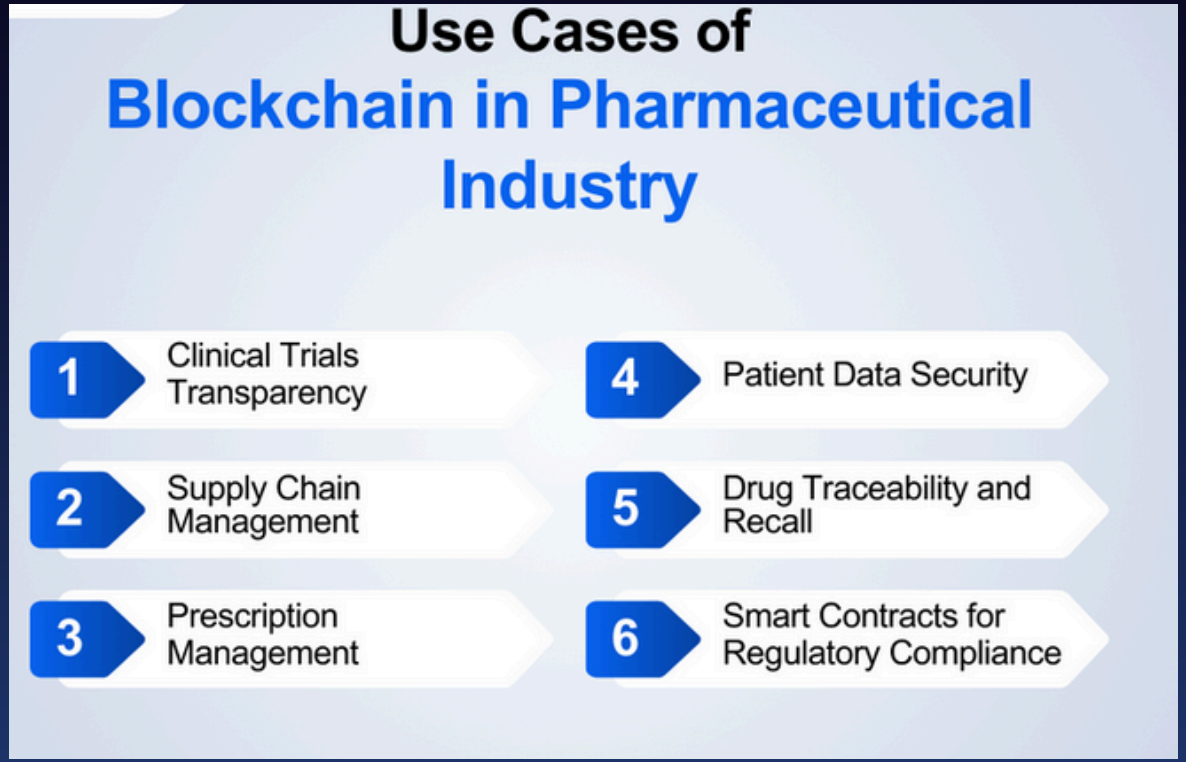
Blockchain in PHARMA

Blockchain in PHARMA

PHARMA


How can Blockchain
Benefit Pharmaceutical Industries?
1
Enhanced Data Security
2
Streamlined Processes
3
Collaboration and
Information Sharing

PHARMA


Use Cases of
Blockchain in Pharmaceutical Industry
1
Clinical Trials Transparency
2
Supply Chain Management
3
Prescription Management
4
Patient Data Security
5
Drug Traceability and Recall
6
Smart Contracts for Regulatory Compliance

REAL TIME USE-CASES

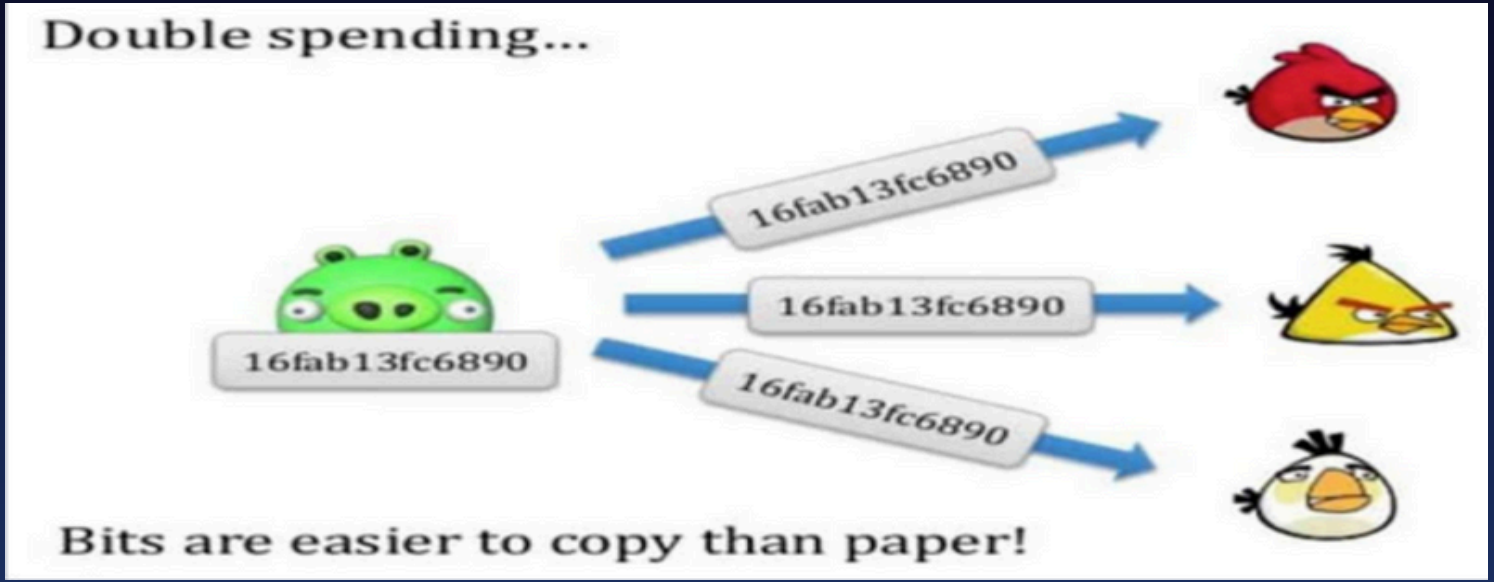
REAL TIME CASE-STUDIES

- Bitcoin
- Crypto Kitties
- Walmart

WHAT IS BITCOIN?

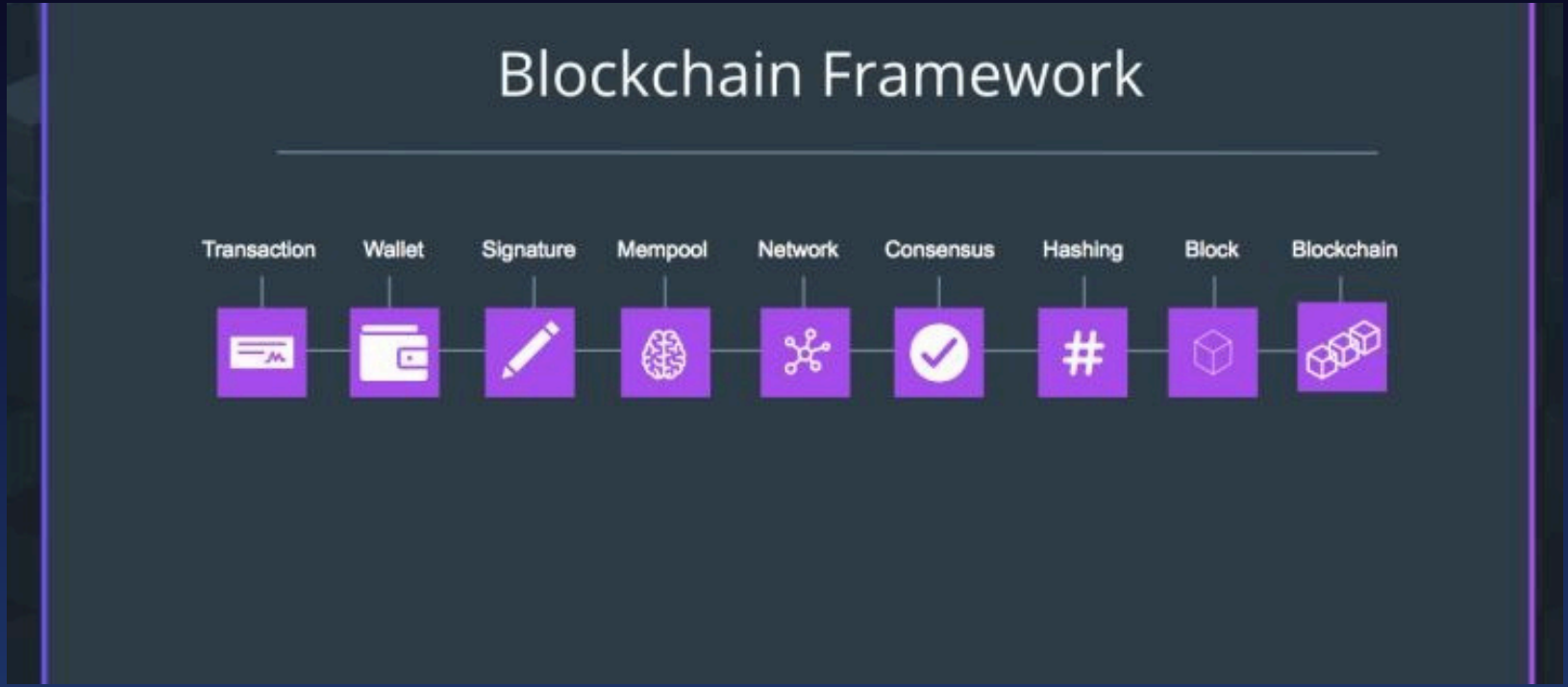
- White Paper was published in 2008.
- White Paper was written by Satoshi Nakamoto (No one knows whether it's a single person or a group).
- Bitcoin is a peer-to-peer cash system:
- Created to bring a common global currency.
- However, it is not being used as originally intended.
- It does not meet the definition of currency as per Google.
- It is more like a Prize Bond, Saving Certificate, or Lottery Ticket.
- Total supply of Bitcoin is 21 million, which will be fully mined by the year 2140.

WHAT PROBLEM IT SOLVED?



HOW BITCOIN WORKS?

Blockchain Framework



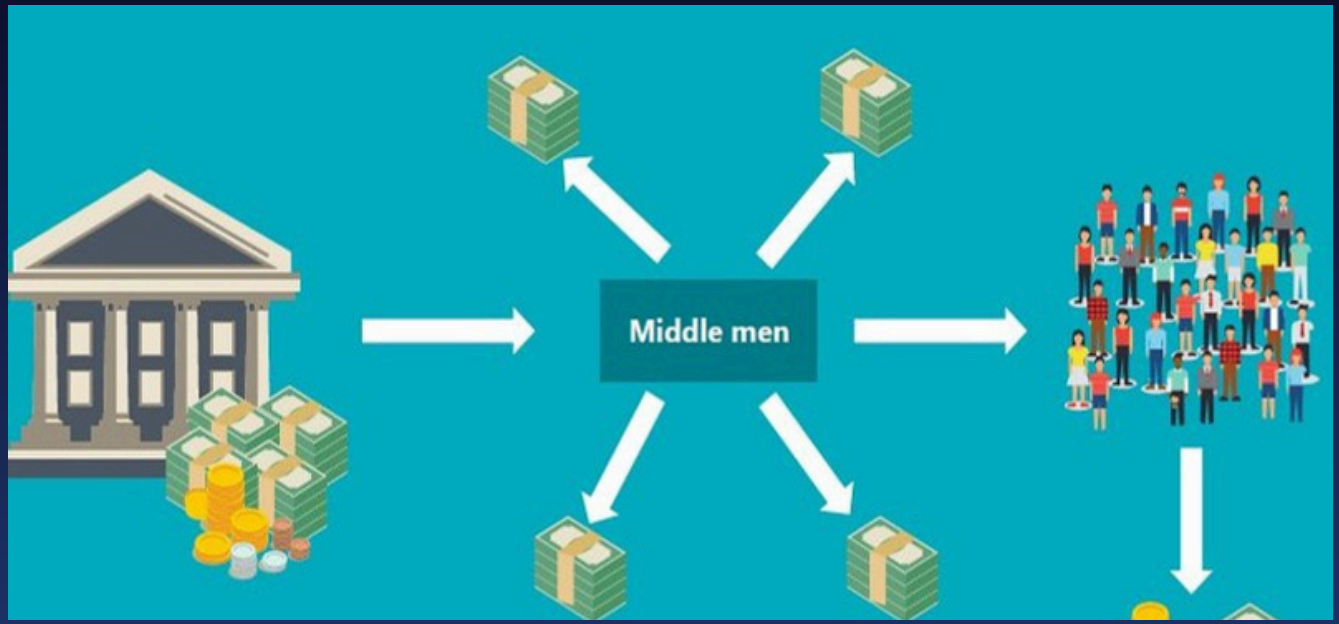
PEOPLE ARE IMPORTANT

Efficient flow of data is of paramount importance

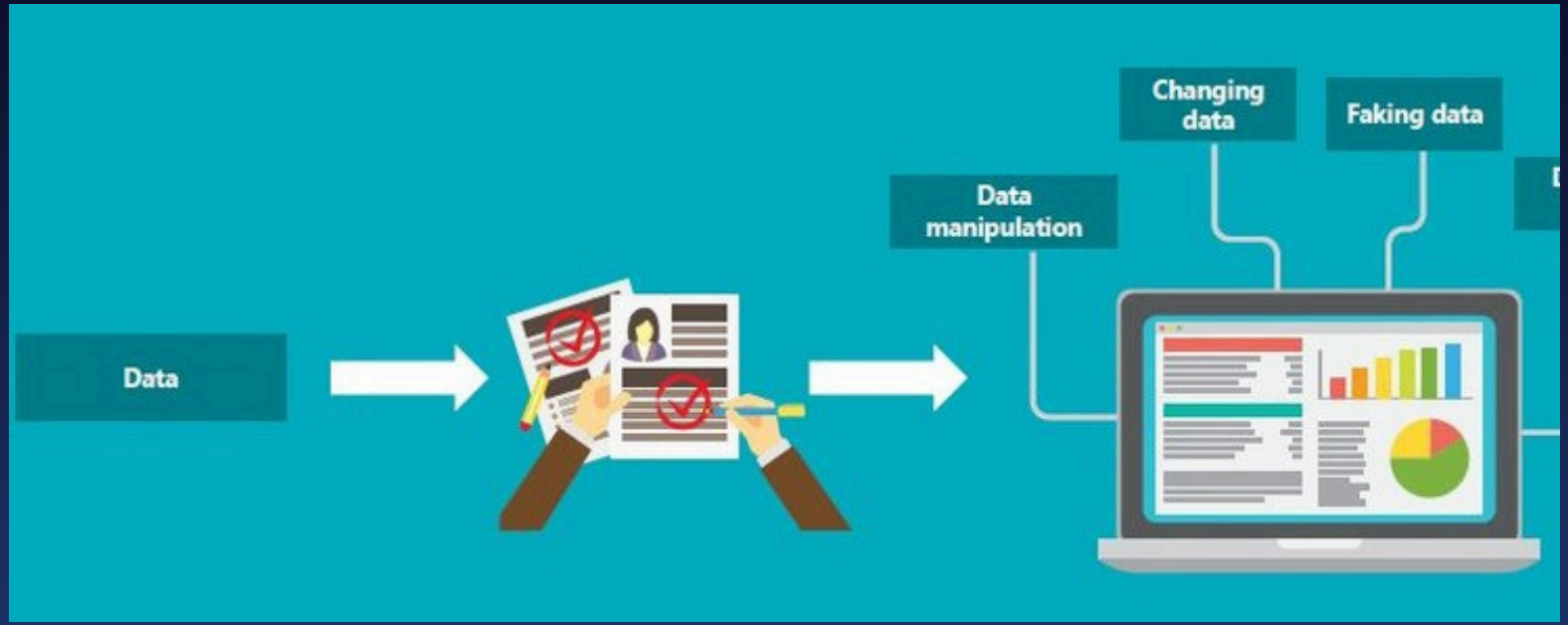
ISSUES IN TRADITIONAL SERVICES

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

DATA STORED IN CENTRALISED



VERIFICATION



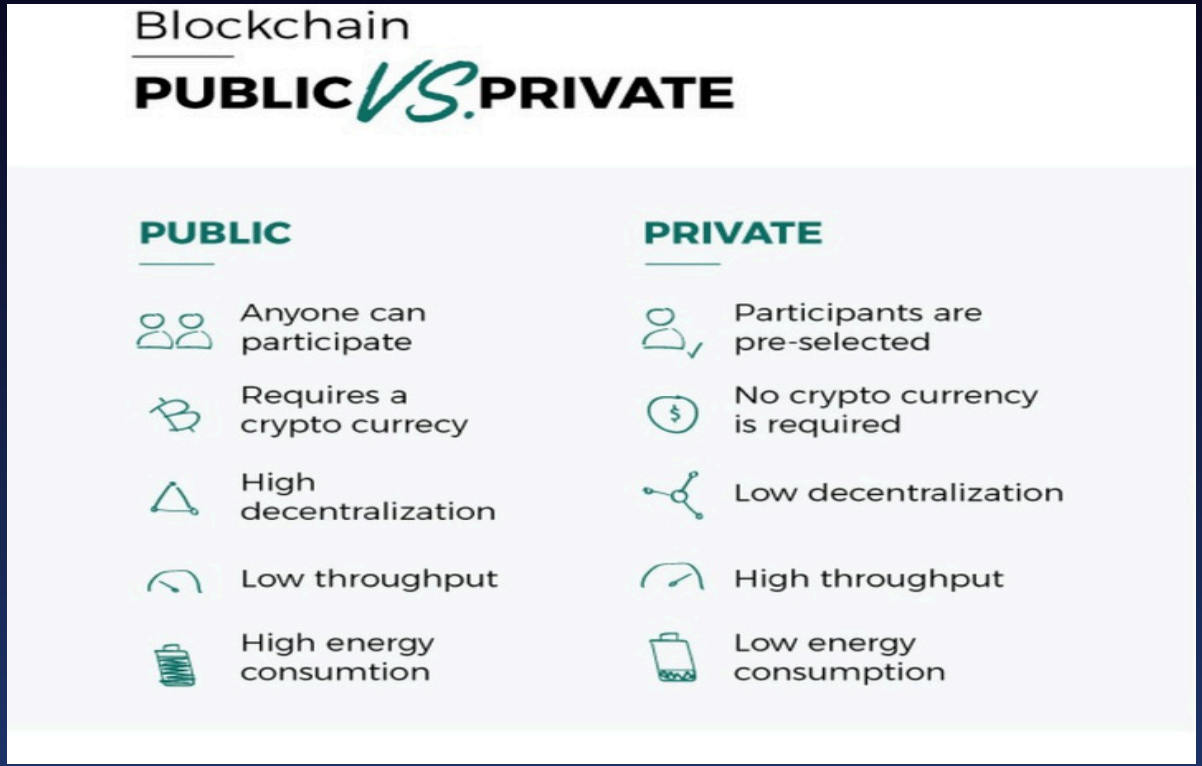
GOOD GOVERNANCE

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

BLOCKCHAIN FRAMEWORKS

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

Performance Vs Privacy Vs Security

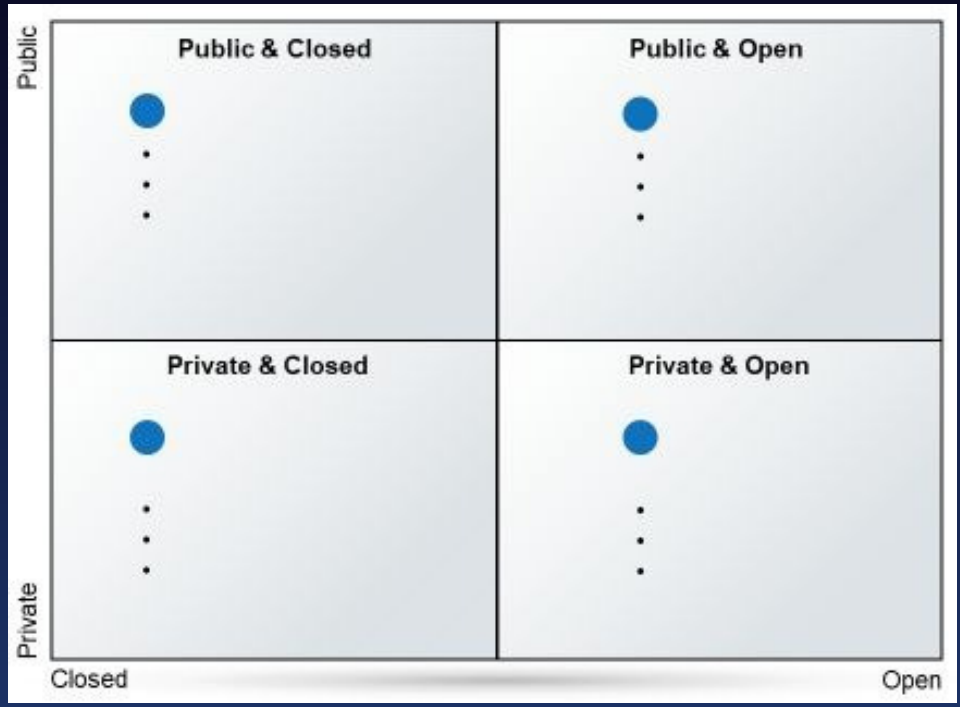
	Private blockchain	Public blockchain	Consortium blockchain
Access	Private	Public	Public/Private
Consensus	Organization based	Public	Selected nodes
Efficiency	High	Low	High
Centralization	Yes	No	Partial
Consensus Process	Permission based	Permissioned based	Permissionless
Immutability	Not completely tamper-proof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

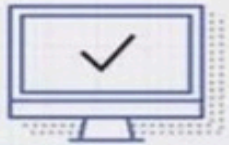


BLOCKCHAIN DECISION MATRIX

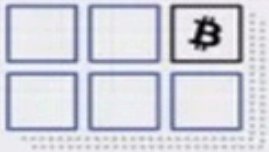
Transaction Life Cycle

A new transaction is entered.

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



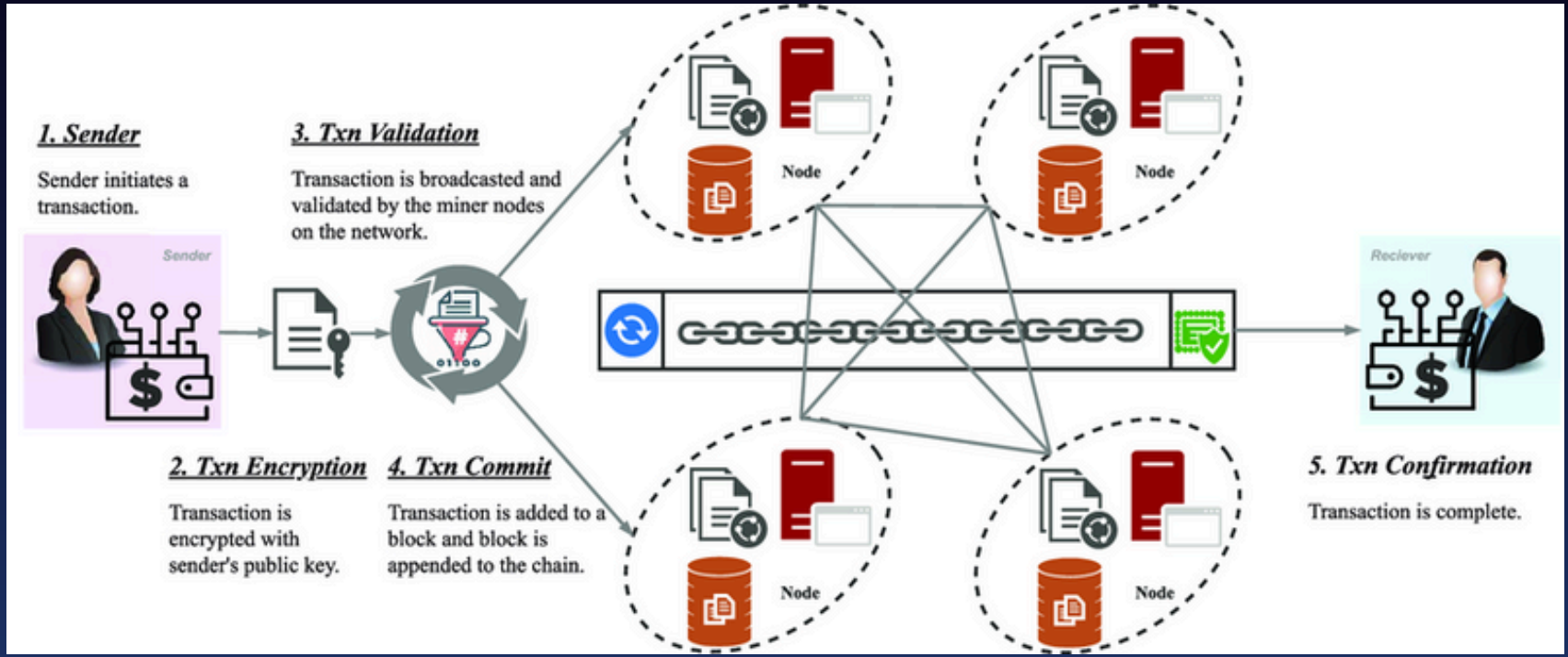
This network of computers then solves equations to confirm the validity of the transaction.



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

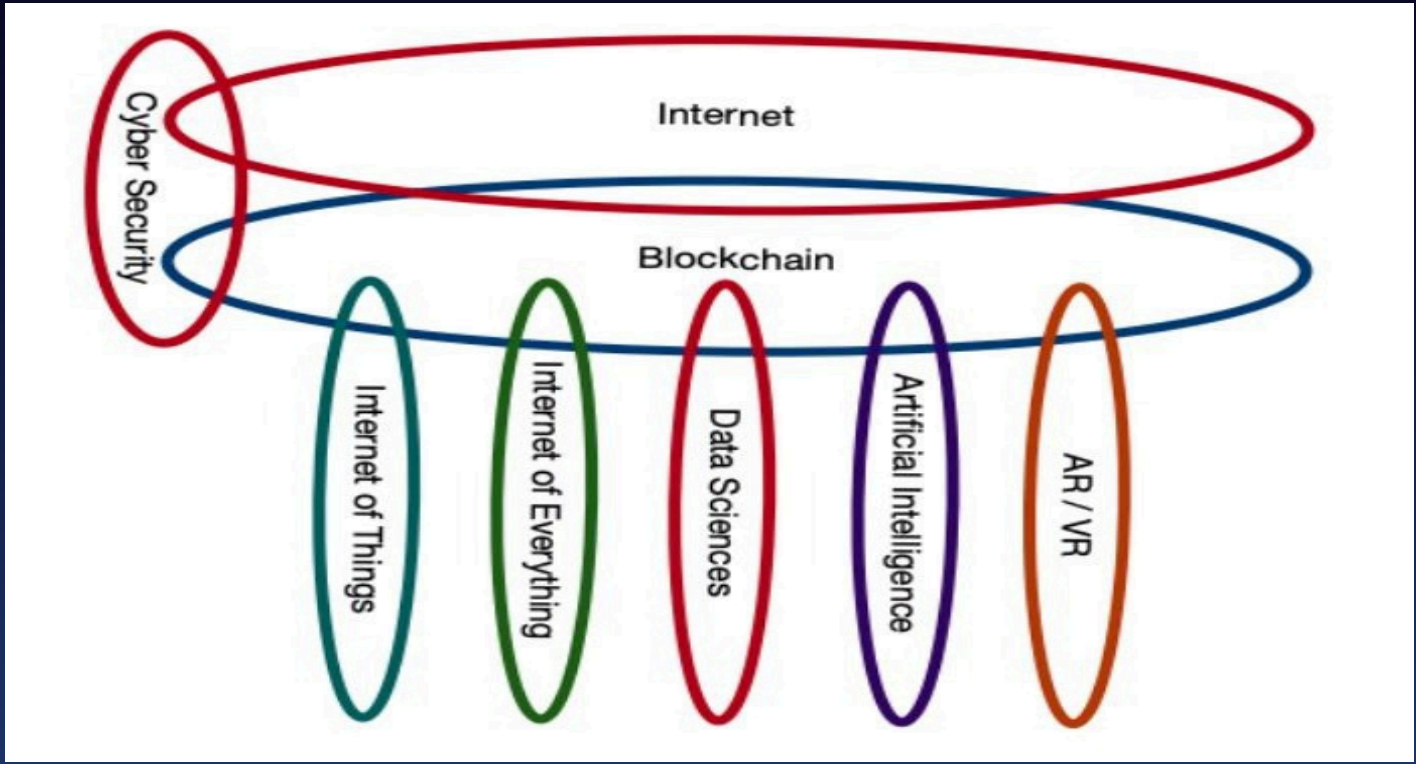
These blocks are then chained together creating a long history of all transactions that are permanent.

The transaction is complete.

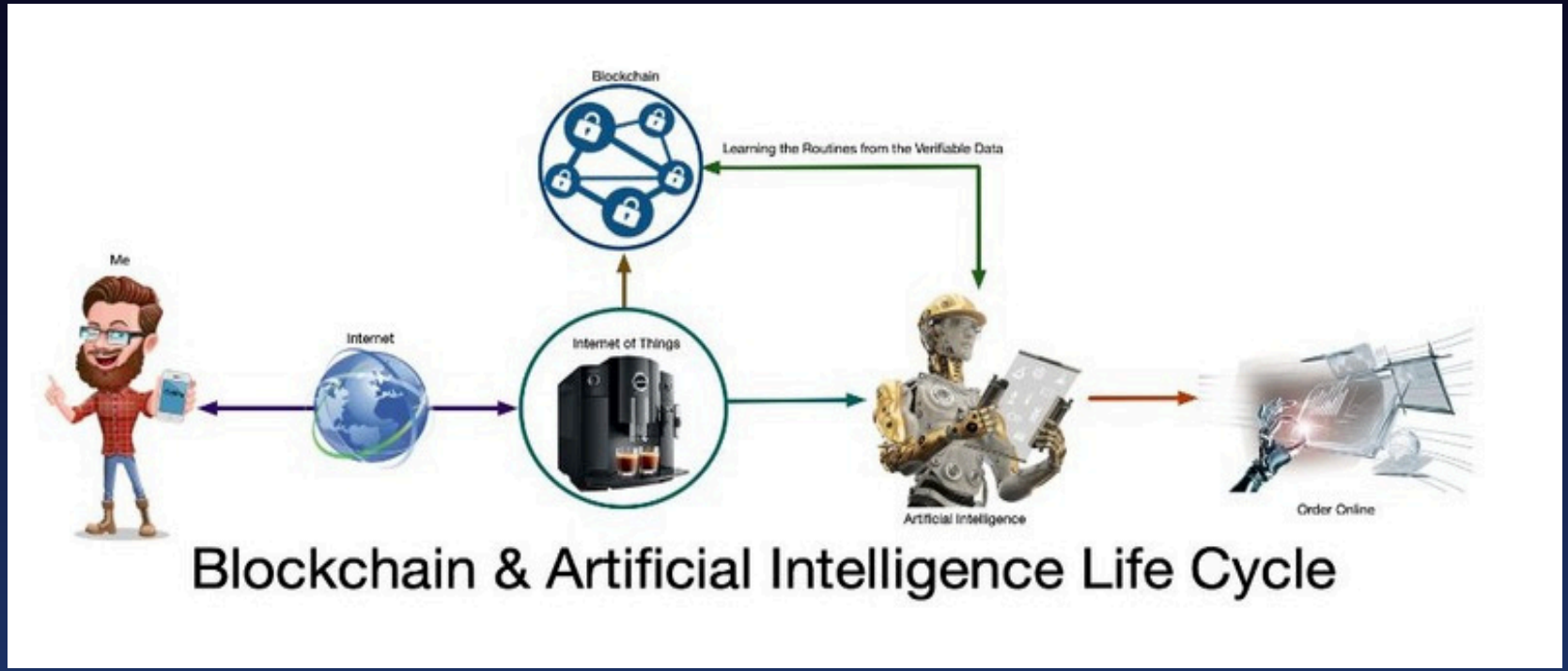

1. Sender
Sender initiates a transaction.
3. Txn Validation
Transaction is broadcasted and validated by the miner nodes on the network.
Sender
Node
Node
Node
Node
Reciever
2. Txn Encryption
Transaction is encrypted with sender's public key.
4. Txn Commit
Transaction is added to a block and block is appended to the chain.
5. Txn Confirmation
Transaction is complete.

BLOCKCHAIN WITH OTHER TECHNOLOGIES

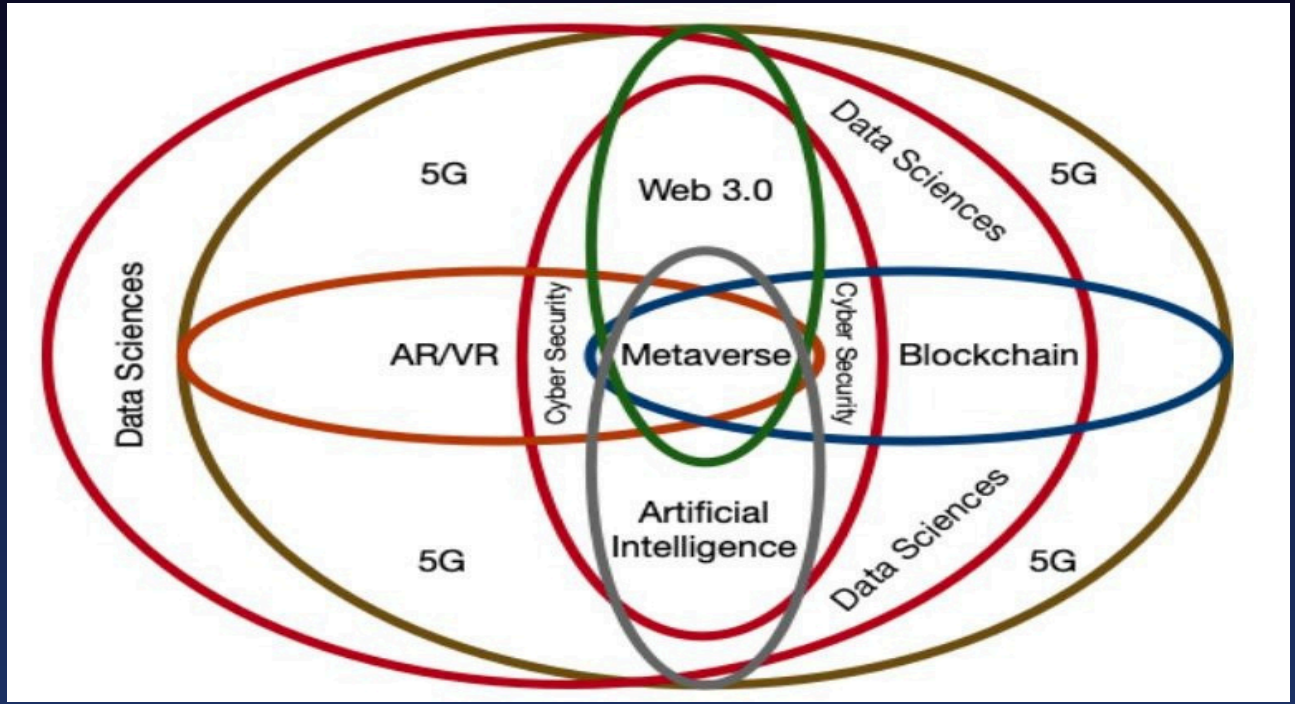
BLOCKCHAIN WITH OTHER TECHNOLOGIES



ROLE OF BLOCKCHAIN IN COMMUNITY



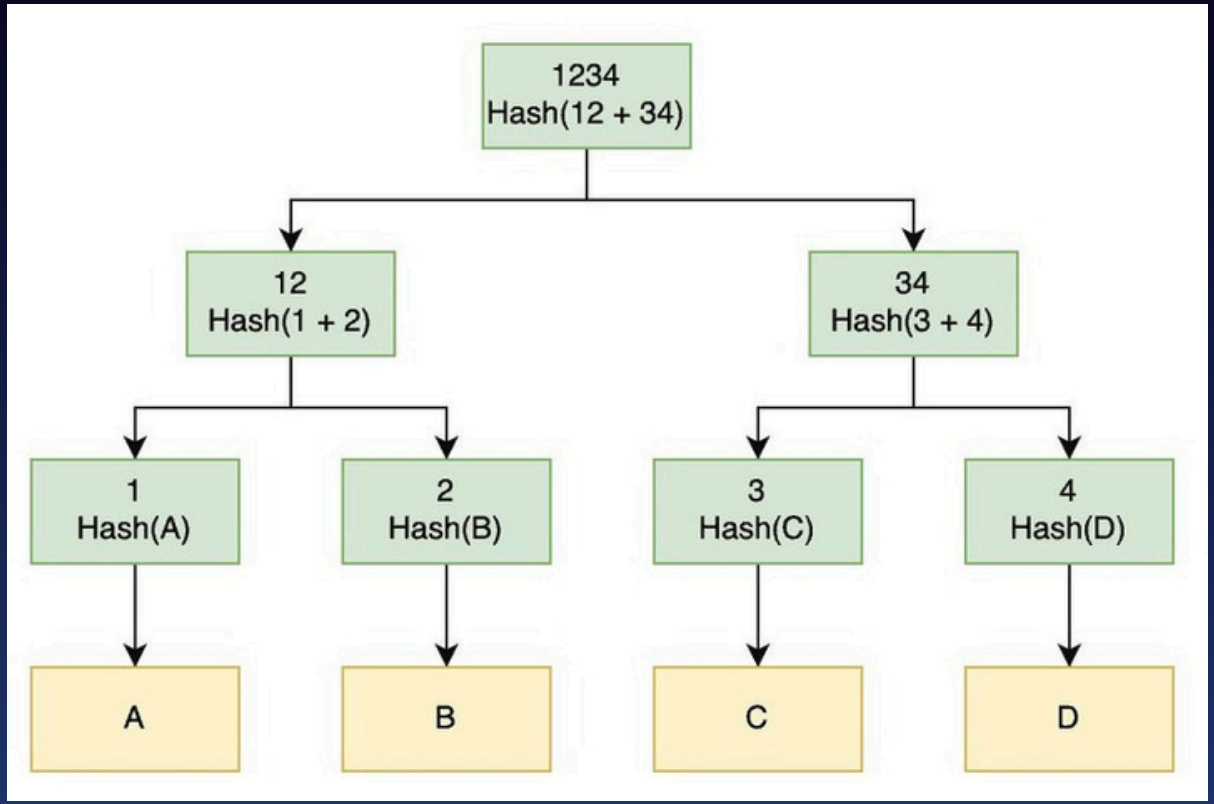
ALL TECHNOLOGIES CONNECTED



BLOCKCHAIN ADOPTION

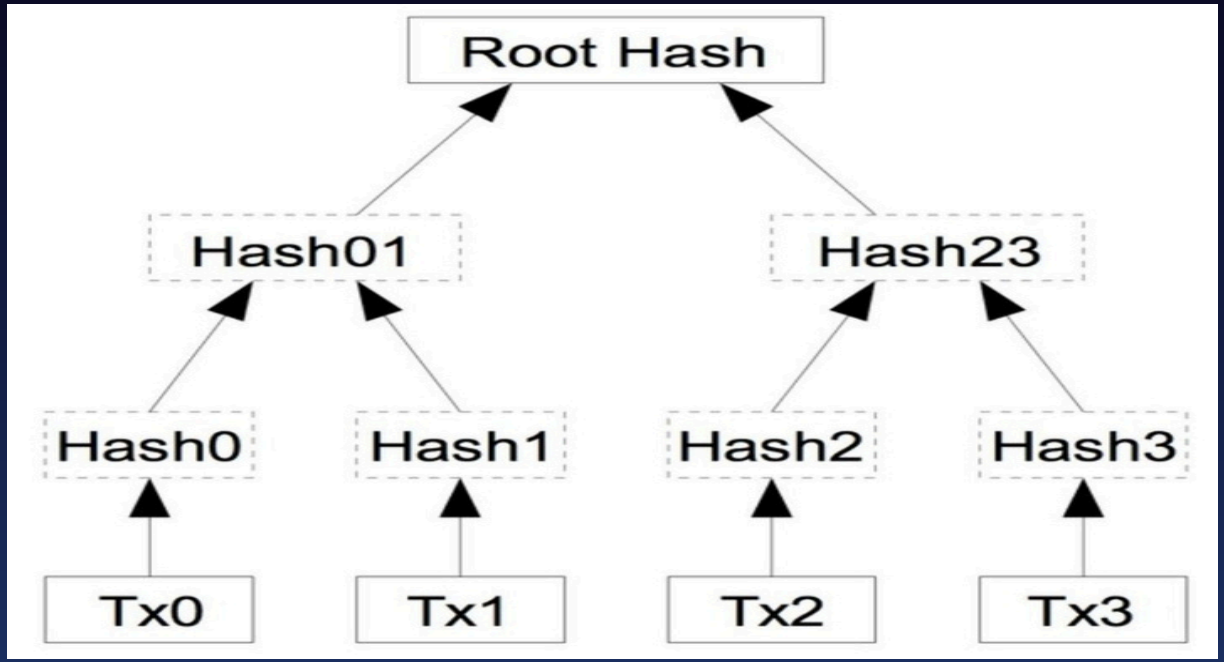
THE FUTURE OF BLOCKCHAIN

Markle Tree

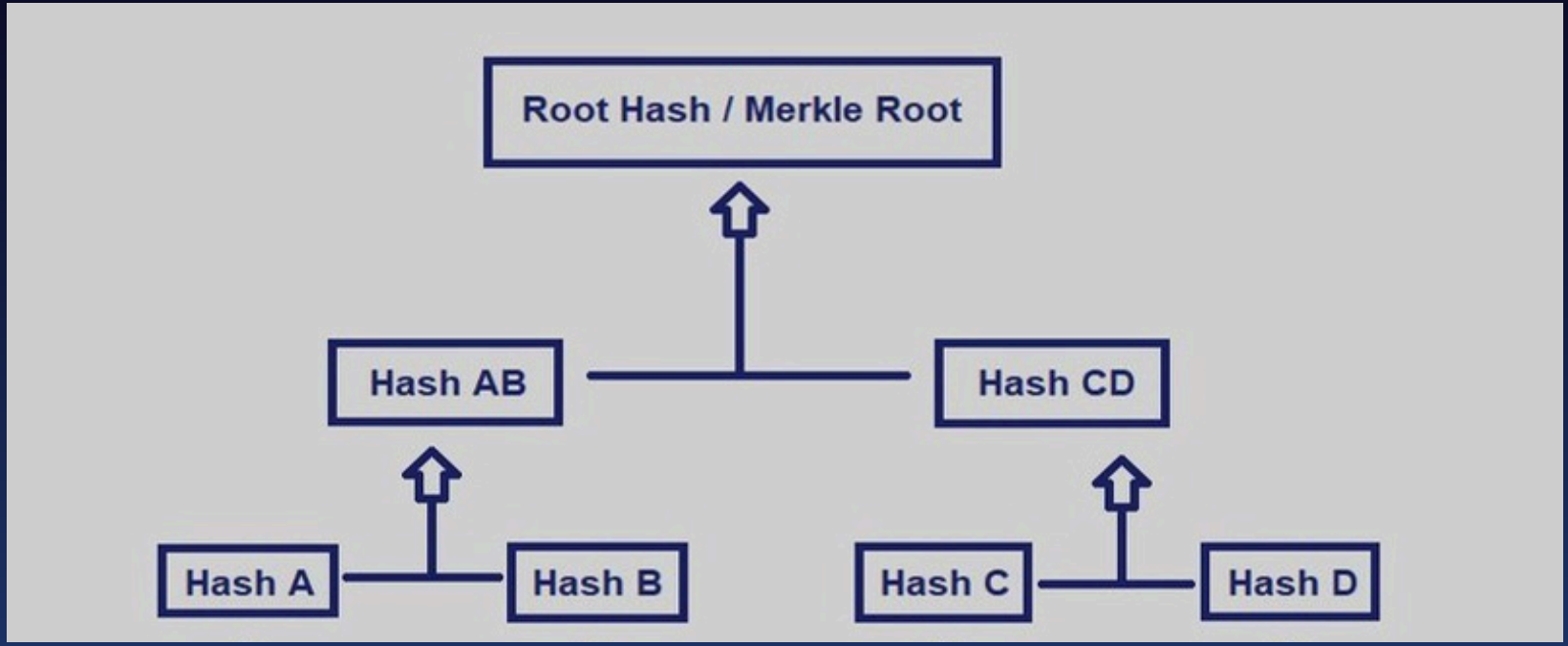

1234
Hash(12 + 34)
12
Hash(1 + 2)
34
Hash(3 + 4)
1
Hash(A)
2
Hash(B)
3
Hash(C)
4
Hash(D)
A
B
C
D

Features of Markle Tree

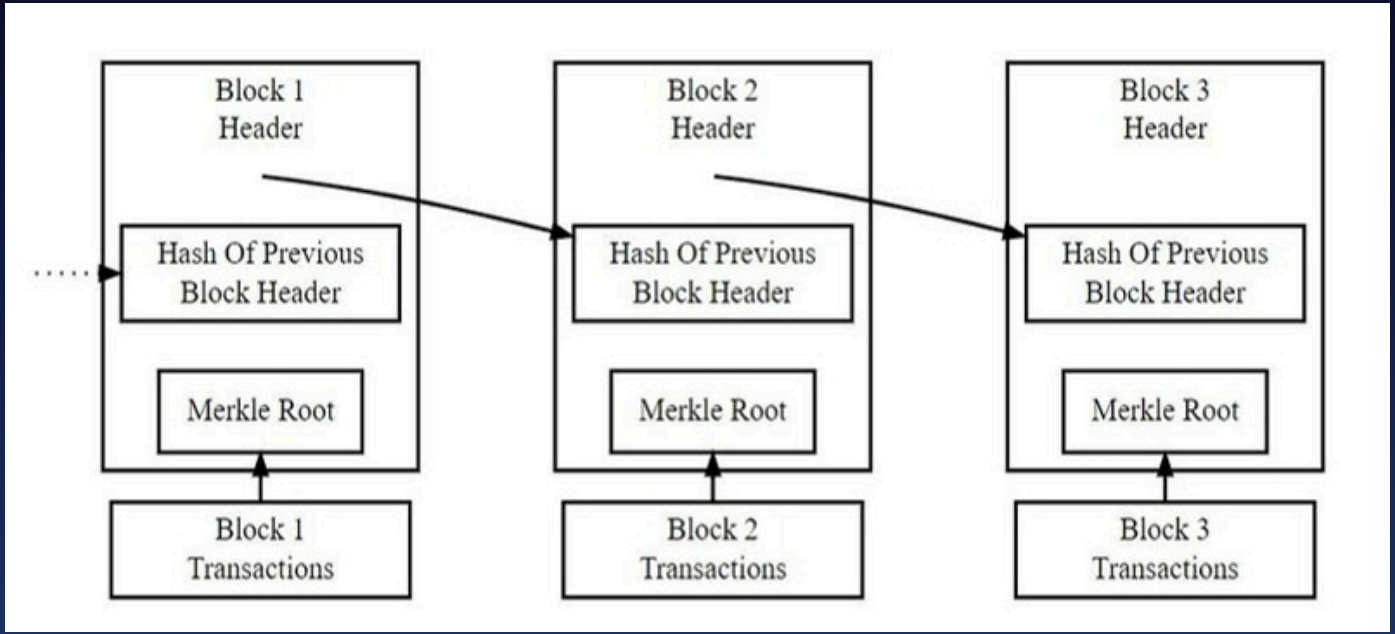
Markle Tree


Root Hash
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Markle Tree


Root Hash / Merkle Root
Hash AB
Hash CD
Hash A
Hash B
Hash C
Hash D

Merkle Tree


Block 1
Header
Hash Of Previous
Block Header
Merkle Root
Block 1
Transactions
Block 2
Header
Hash Of Previous
Block Header
Merkle Root
Block 2
Transactions
Block 3
Header
Hash Of Previous
Block Header
Merkle Root
Block 3
Transactions

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

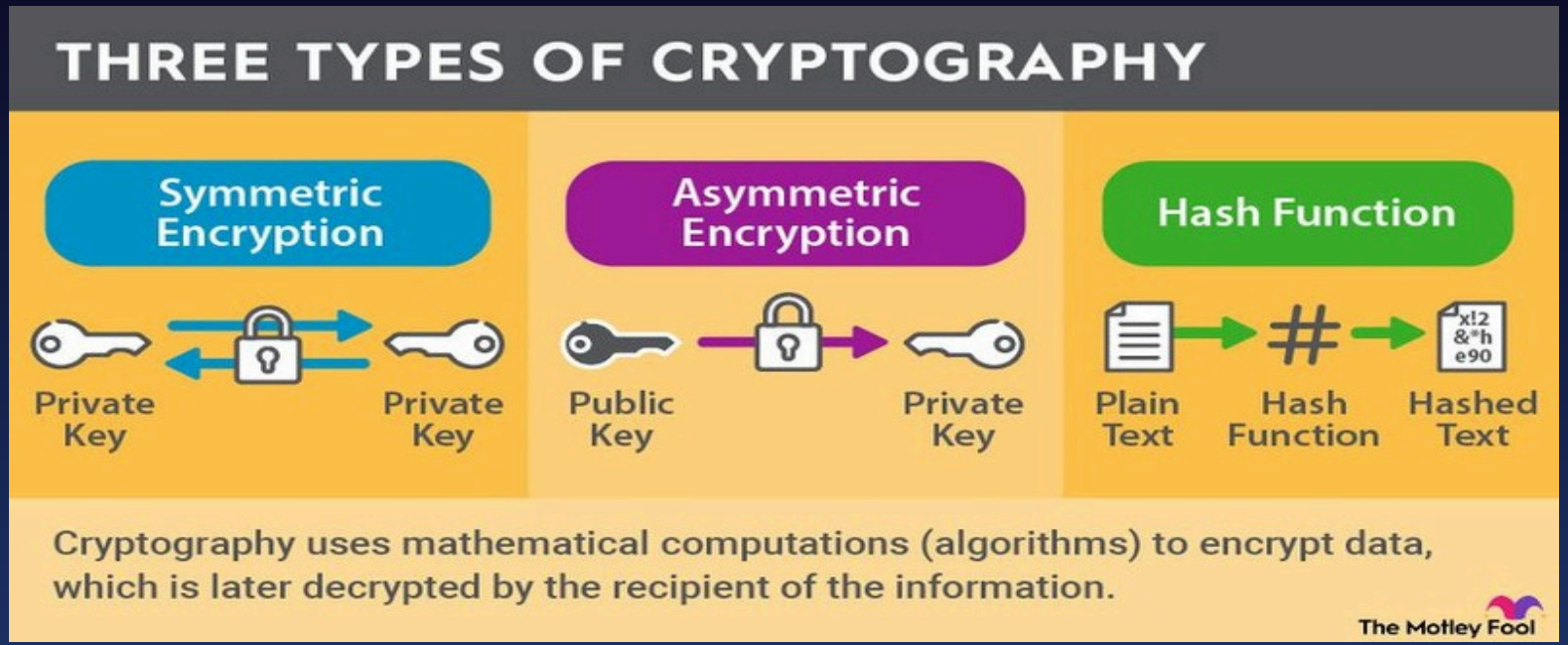
Ciphertext: The illegible form of an encoded message

Plaintext: The decoded message

Features of Cryptography

- Only the intended recipient can access the information on a blockchain.
- Information is immutable – it cannot be changed during storage or transmission without new modifications being noticed.
- No retraction – the sender cannot later deny or revoke their intent to send information.
- Identity verification – both the sender and receiver's identities, along with the information's origin and destination, are authenticated.

Types of Cryptography



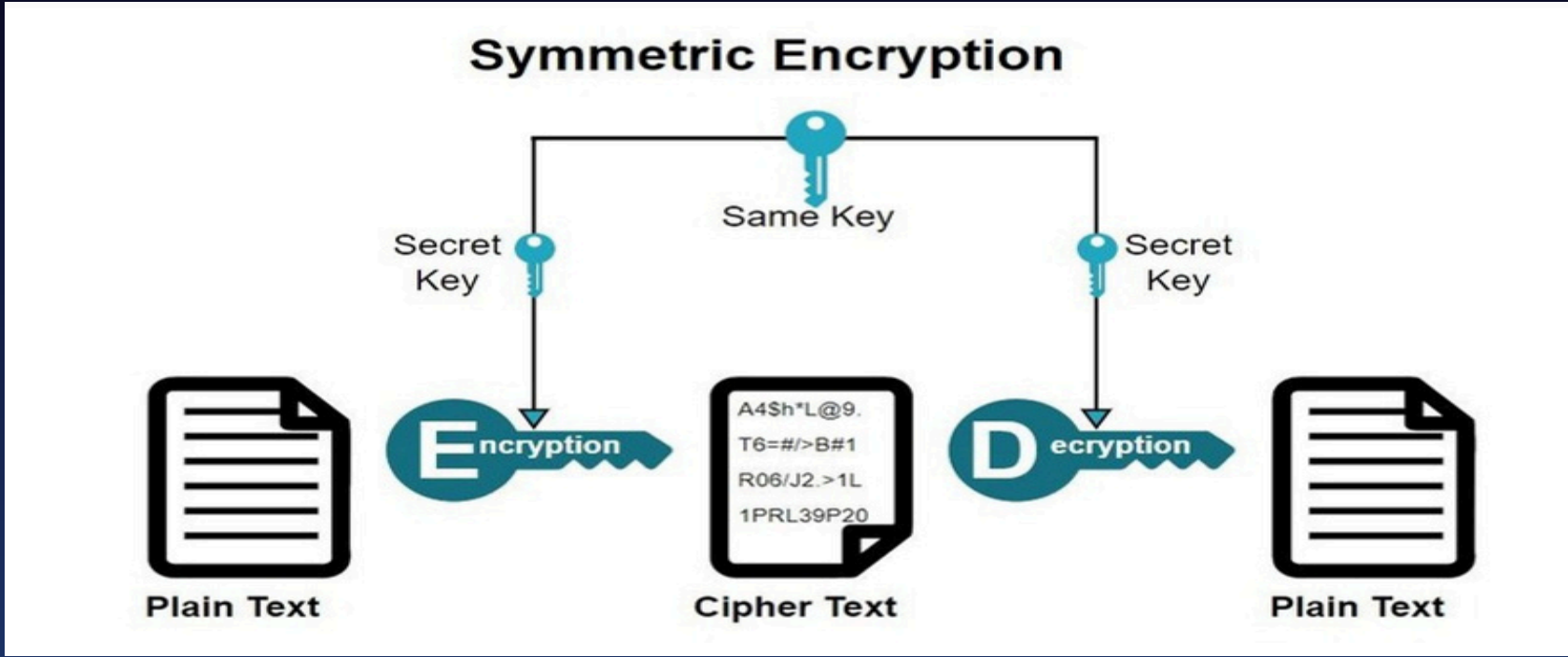
Types of Cryptography - Symmetric Encryption

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.

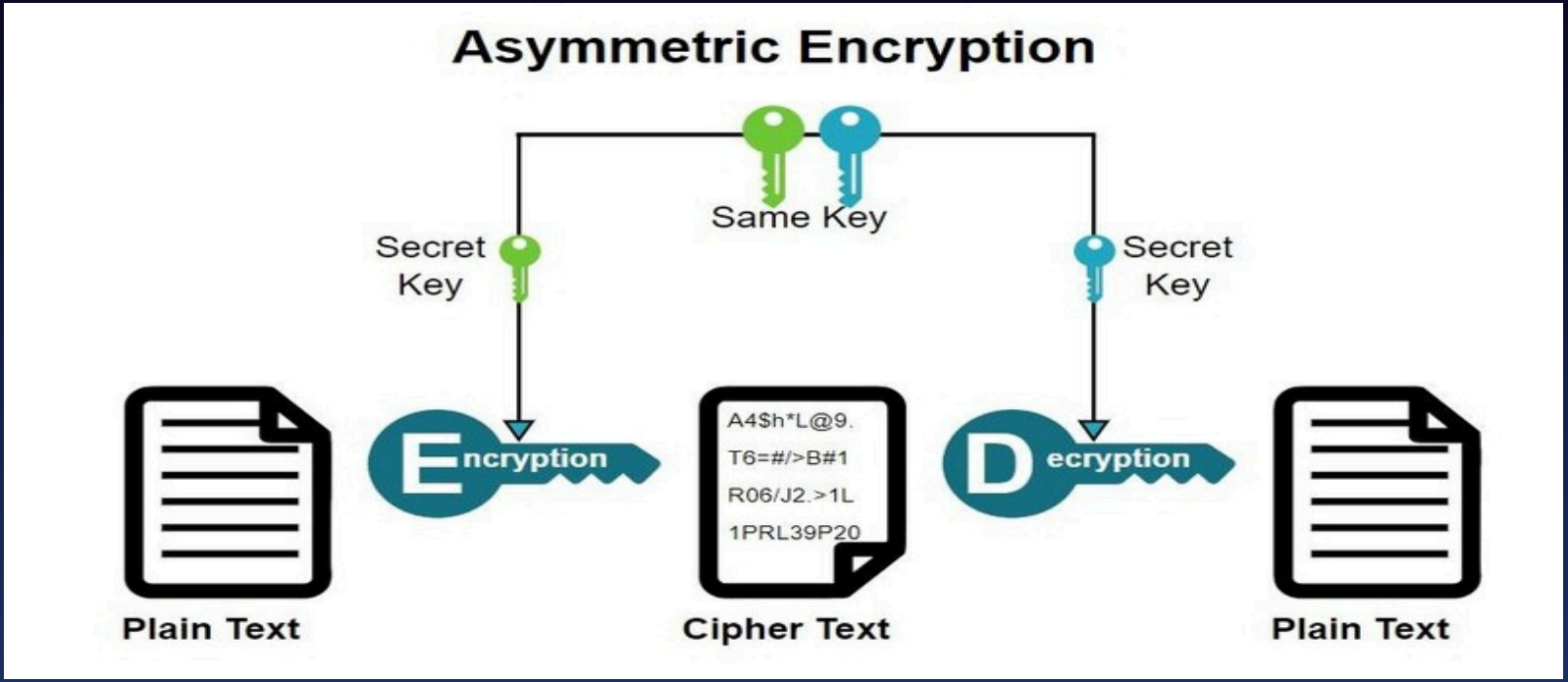
Types of Cryptography - Symmetric Encryption



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

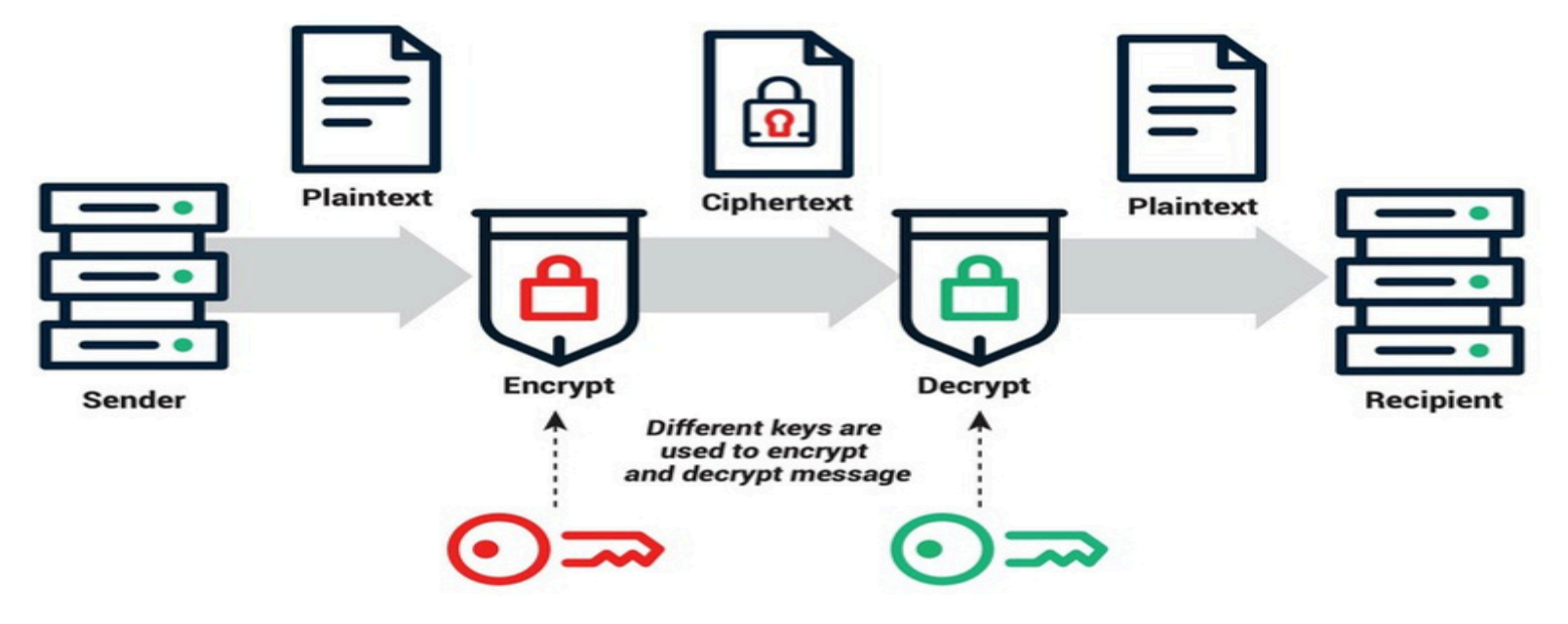
Security

Authentication

Privacy

Integrity

Encryption & Decryption



THANK-YOU