22AIE203 DATA STRUCTURES & ALGORITHMS -2 (L-T-P-C:2-0-3-3)

BlockChain

February 14, 2024

Dr.Remya S
Assistant Professor
Department of Computer Science

AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY UNDER SECTION 3 OF UGC ACT, 1956

School of Computing
Amritapuri Campus, Clappana P.O., Kollam - 690525, Kerala, India. Ph: +91 (476) 280 2100 Email: csoffice@am.amrita.edu
www.amrita.edu/school/computing/amritapuri

Blockchain Technology-Background

- The theory behind Bitcoin was first explained in a **2008** white paper written under the pseudonym **"Satoshi Nakamoto"**
- Blockchain is a **list of records called blocks** that store data publicly and in chronological order. The information is encrypted using cryptography to ensure that the privacy of the user is not compromised and data cannot be altered
- Information on a Blockchain network is not controlled by a centralized authority, unlike modern financial institutions
- If you are a participant in the Blockchain network, you will have the same copy of the ledger, which all other participants have. Even if one node or data on one particular participant's computer gets corrupted, the other participants will be alerted immediately, and they can rectify it as soon as possible

- A blockchain is a **decentralized** database and **peer to peer** network that stores a registry of transactions secured with **cryptography**
- Blockchain is the ledger, or record keeping, side of the transaction and subsequent transactions
- Blockchain technology uses a distributed database (multiple devices not connected to a common processor) that organizes data into records, that have cryptographic validation, are timestamped, and are linked to previous records so that they can only be changed by those who own the encryption keys to write the files.
- Blockchain records the date, time, participants, and any other contractual or legal pieces of a Bitcoin transaction
- Blockchain is a key part of the infrastructure underlying Bitcoin and other cryptocurrencies

Features of Blockchain

- We have a **public distributed ledger**, which works using a **hashing encryption**
- Every block has a hash value, which is the **digital signature** of the block
- All the transactions are approved and verified on the Blockchain network using a proof of work consensus algorithm
- The Blockchain network utilizes the resources of the **miners**, who are there to validate the transactions for rewards

What is Blockchain Technology?

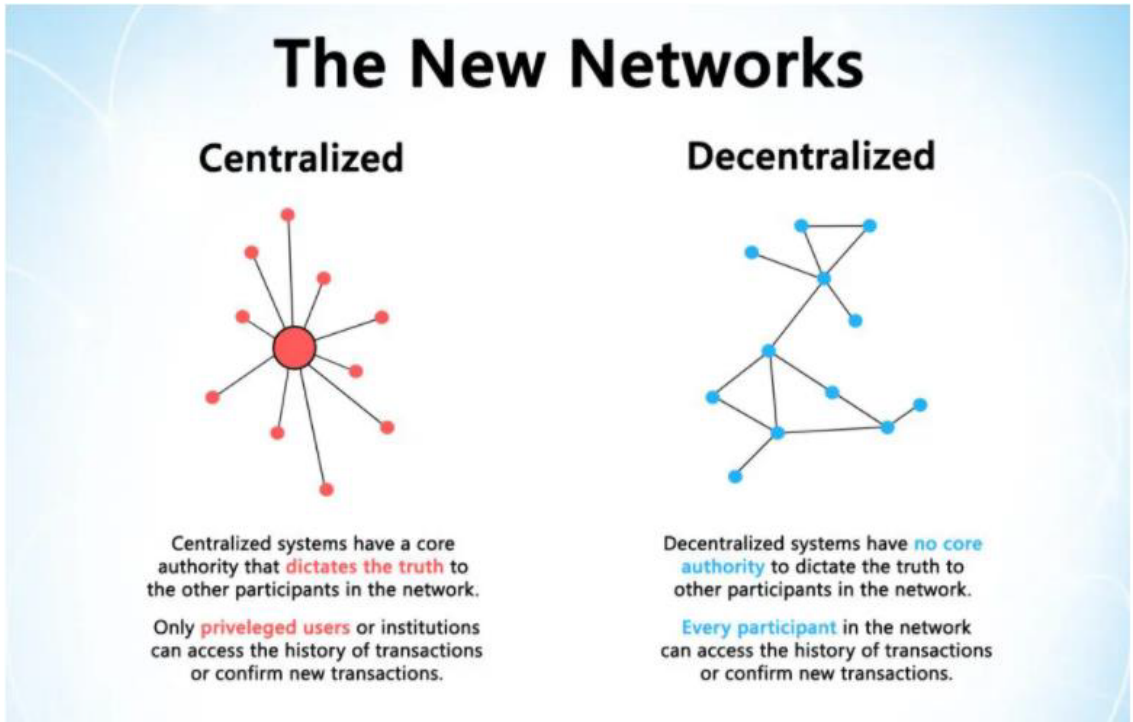
- Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the **"chain "** in a network connected through peer to peer nodes. Typically, this storage is referred to as a **'digital ledger'**
- Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering Hence, the information the digital ledger contains is highly secured
- The digital ledger is like a Google spreadsheet shared among numerous computers in a network, in which, the transactional records are stored based on actual purchases. **Anybody can see the data, but they can't corrupt it.**

The Three Pillars of Blockchain Technology. . .

- Decentralization
- Transparency
- Immutability

Decentralization

In a decentralized network, if you want to interact with your friend then you can do so directly without going through a third party. That was the main ideology behind Bitcoins. Only you alone are in charge of your money You can send your money to anyone you want without having to go through a bank.



Transparency

One of the most interesting and misunderstood concepts in blockchain is "transparency". **A person's identity is hidden** via complex cryptography and represented only by their public address. The following snapshot of Ethereum transactions depicts as what it actually shown.

TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...	→	0x2bdc9191de5c1b...	0.004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...	→	0xf14cb3acac7b230...	0.744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...	→	0x2d42ee86390c59...	0.016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...	→	0xd39681bb0586fb...	0.01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...	→	0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...	→	0x8a91cac422e55e...	0.029594 Ether	0.000294

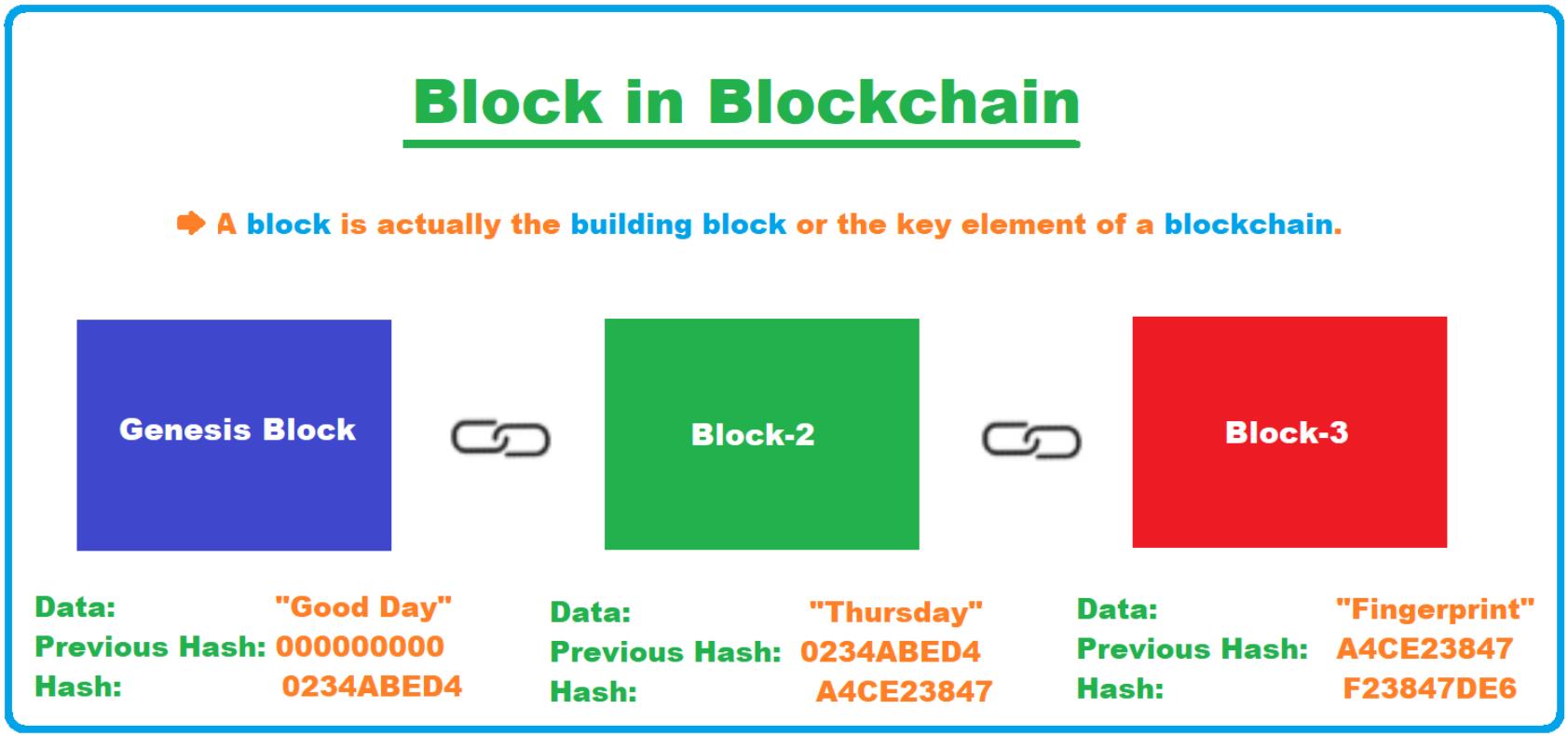
Immutability

Immutability, in the context of the blockchain means that once something has been entered into the blockchain it **cannot be tampered with**. The reason why the blockchain gets this property is that of the **cryptographic hash function takes an input string of any length and gives out an output of a fixed length.**

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

What is a Block??

With Blockchain technology, **each page in a ledger of transactions forms a block**. The block has an impact on the next block or page through cryptographic hashing. In other words, when a block is completed, it creates a unique secure code, which ties into the next page or block, creating a chain of blocks, or blockchain.



Why is Blockchain Popular?

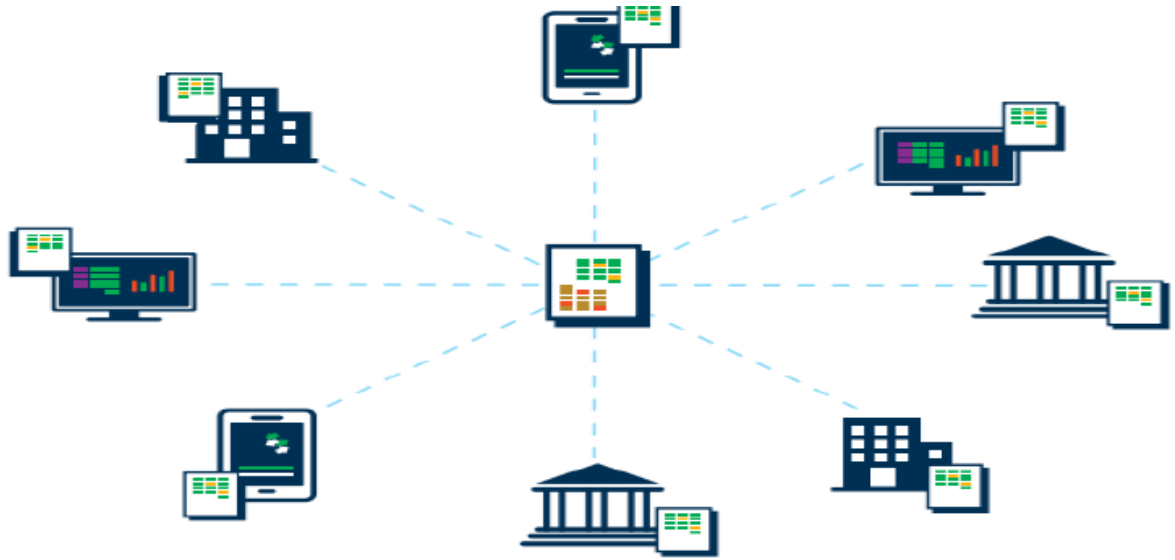
- **Highly Secure:** Blockchain technology uses a digital signature feature to conduct fraud free transactions making it impossible to corrupt or change the data of an individual by the other user without a specific digital signature
- **Decentralized System:** Conventionally, you need the approval of regulatory authorities like a government or bank for transactions however, with Blockchain transactions are done with the mutual consensus of users resulting in smoother, safer, and faster transactions
- **Automation Capability:** Blockchain technology is programmable and can generate systematic actions, events, and payments automatically when the criteria of the trigger are met

What is a Cryptocurrency?

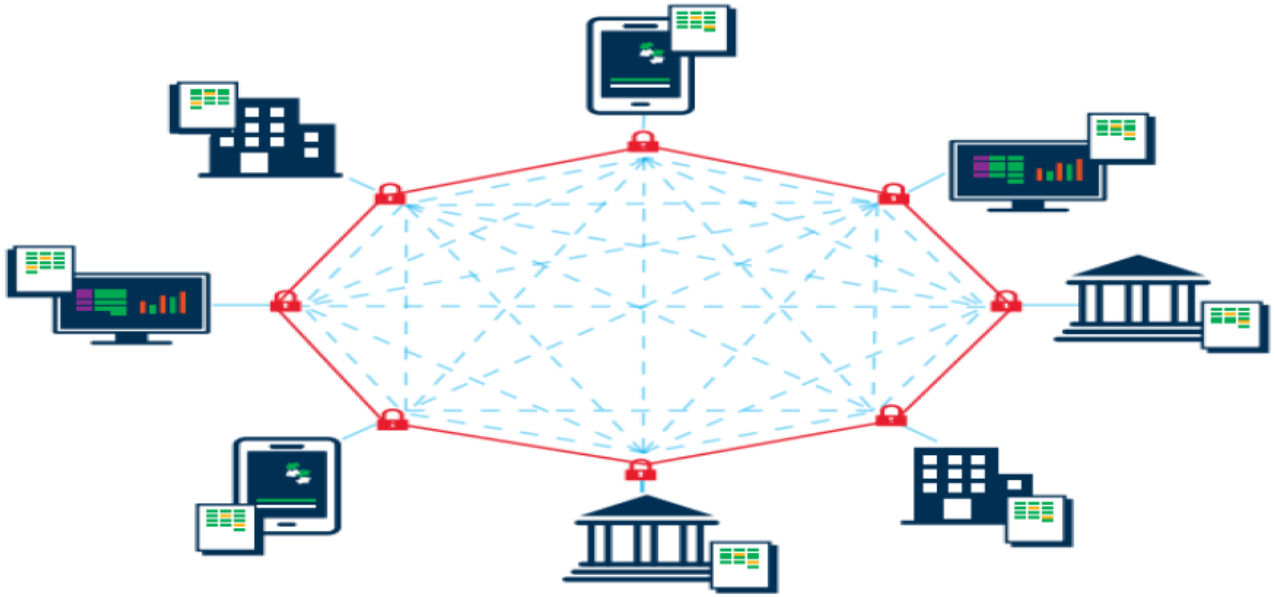
- A cryptocurrency is a form of digital currency that can be used to verify the transfer of assets, control the addition of new units, and secure financial transactions using cryptography
- One of cryptocurrencies' most important advantages over normal currencies is that they are **not controlled by any central authority**.
- The shared and distributed nature of cryptocurrencies keeps everyone on the same page. Therefore, the transparency and distributed nature of Blockchain technology is what makes cryptocurrencies secure
- Some of the more popular cryptocurrencies are Bitcoin, Litecoin, Ethereum, Stellar, Ripple, etc

What is Distributed Ledger?

1. Distributed Ledger **(Permissionless)**: Each node in a P-2-P network owns a full and up-to-date copy of the entire ledger. Every proposed local addition to the ledger by a network participant is communicated across the network to all nodes. Nodes collectively validate the change through an algorithmic consensus mechanism(general agreement). After validation is accepted, the new addition is added to all respective ledgers to ensure data consistency across the entire network.
2. Distributed Ledger**(Permissioned):** In a permissioned system, nodes need permission from a central entity to access the network and make changes to the ledger. Access controls can include identity verification.



Distributed Ledger (Permissionless)

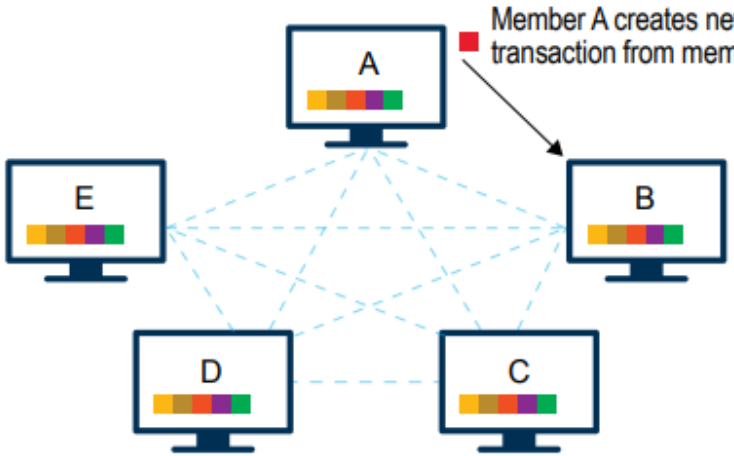


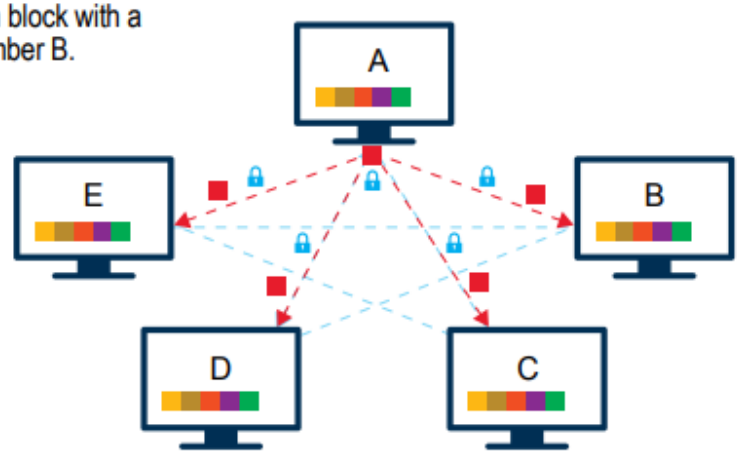
Distributed Ledger (Permissioned)

How does Blockchain Based DLT Work?

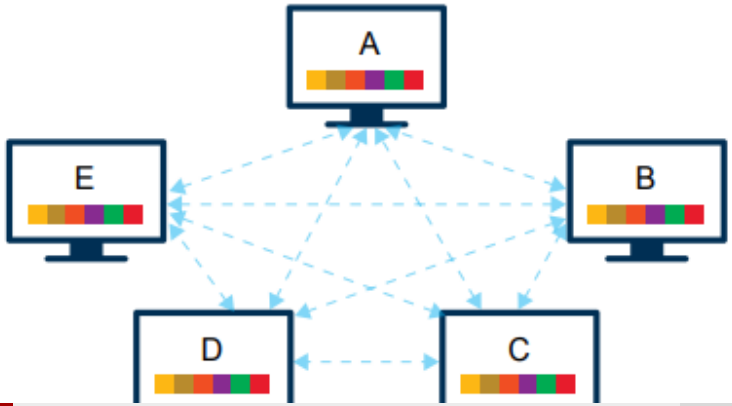
1. Blockchain-based DLT systems take the form of an append-only chain of data 'blocks'. New additions to the database are initiated by one of the members (nodes), who creates a new "block" of data containing several transaction records.

2. Information about this new data block is then shared across the entire network, containing encrypted data so transaction details are not made public.





3. All network participants collectively determine the block's validity according to a pre-defined algorithmic validation method ('consensus mechanism'). Only after validation, all participants add the new block to their respective ledgers. Through this mechanism each change to the ledger is replicated across the entire network and each network member has a full, identical copy of the entire ledger at any point in time.



How Does Blockchain Work?

Blockchain consists of three important concepts Blocks, Nodes and Miners.

Blocks

- Every chain consists of multiple blocks and each block has three basic elements
  1. The data in the block
  2. A **32 bit** whole number called a **NONCE**. The nonce is randomly generated when a block is created, which then generates a block header hash
  3. The hash is a **256 bit number**.
- When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

Nodes

- One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain
- Nodes can be any kind of electronic device that maintains copies of the blockchain and keeps the network functioning
- Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified
- Each participant is given a unique alphanumeric identification number that shows their transactions
- Combining public information with a system of checks and balances helps the blockchain maintain integrity and creates trust among users

Miners

- Miners create new blocks on the chain through a process called mining
- In a blockchain, every block has its own unique nonce and hash, but also references the hash of the previous block in the chain
- Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256 there are roughly four billion possible nonce hash combinations that must be mined before the right one is found
- Making a change to any block earlier in the chain requires remaining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology
- When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially

Cryptography

- **Cryptography** is the science of using mathematics to encrypt and decrypt data-**Phil Zimmermann**
- A **cryptosystem** is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system.
- The various components of a basic cryptosystem are as follows : **Plaintext, Encryption Algorithm, Ciphertext, Decryption Algorithm, Encryption Key, Decryption Key**

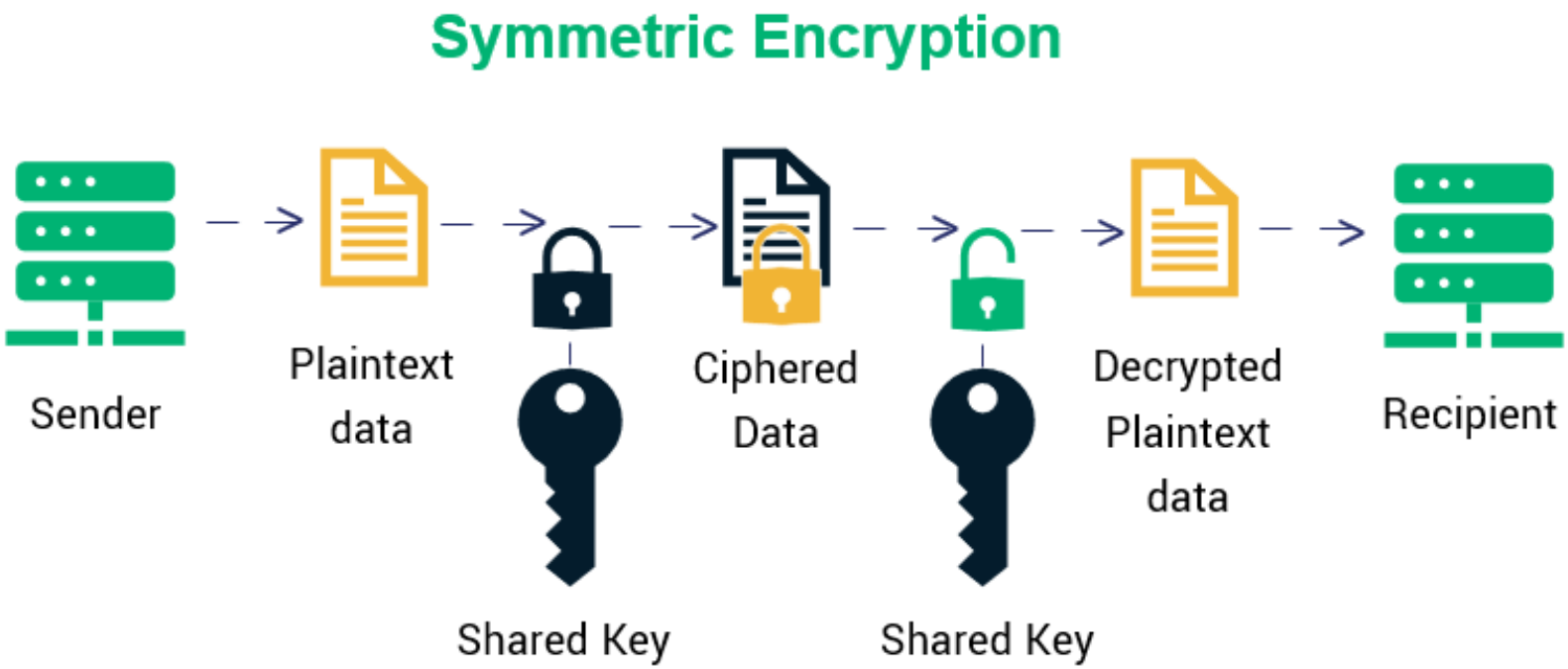
- Cryptography can provide the following services:
  1. **Confidentiality** (secrecy)
     - Ensuring that no one can read the message except the intended receiver
     - Data is kept secret from those without the proper credentials, even if that data travels through an insecure medium
  2. **Integrity** (anti-tampering)
     - Assuring the receiver that the received message has not been altered in any way from the original.
  3. **Authentication**
  4. **Non-repudiation:** A mechanism to prove that the sender really sent this message

Types of Cryptography

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Functions

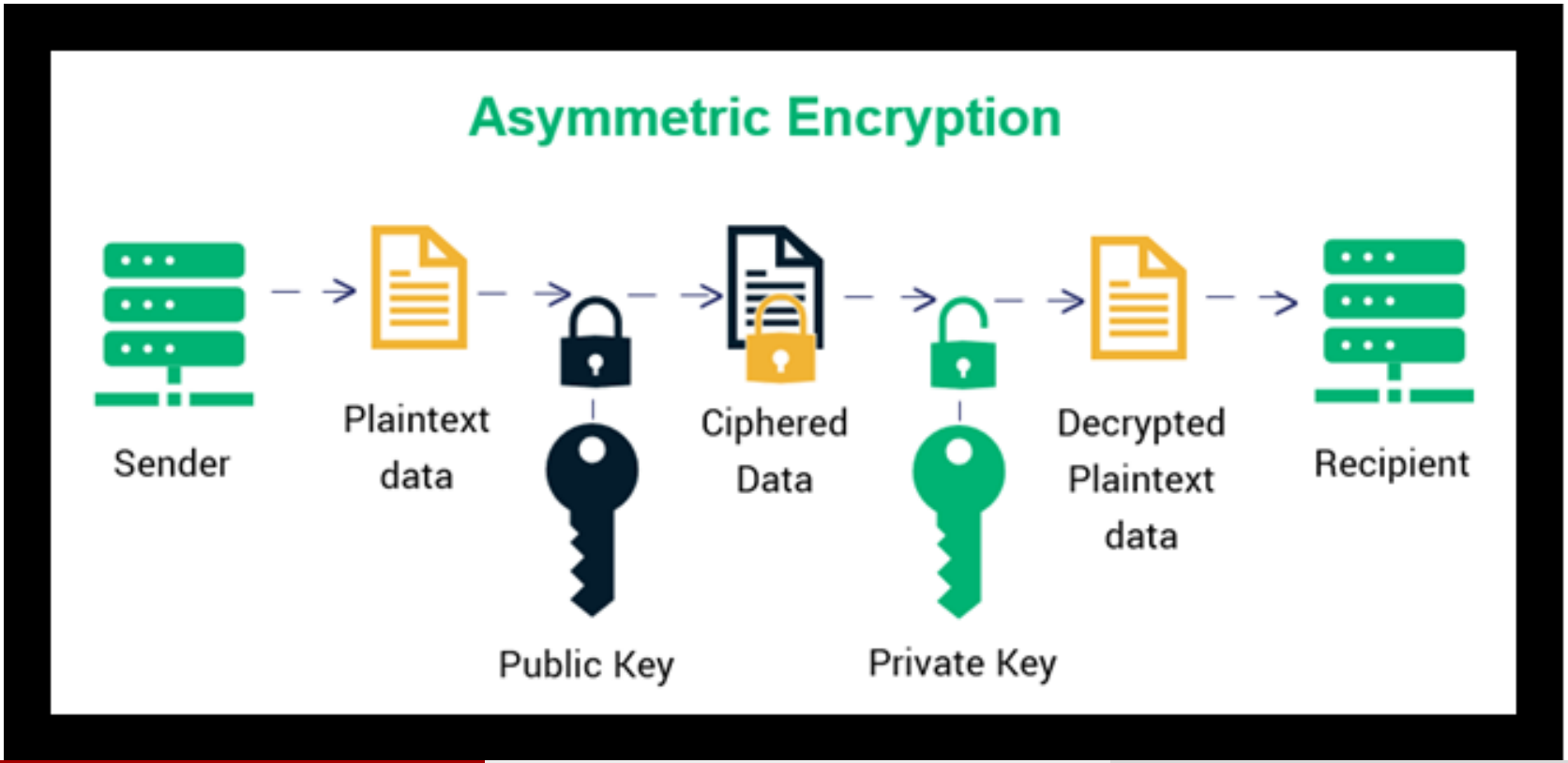
Symmetric Key Cryptography

- Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a **single, common key** that is used to encrypt and decrypt the message.
- Also known as **Secret Key Cryptography or Conventional Cryptography**
- Problems with Conventional Cryptography: **Key Management**



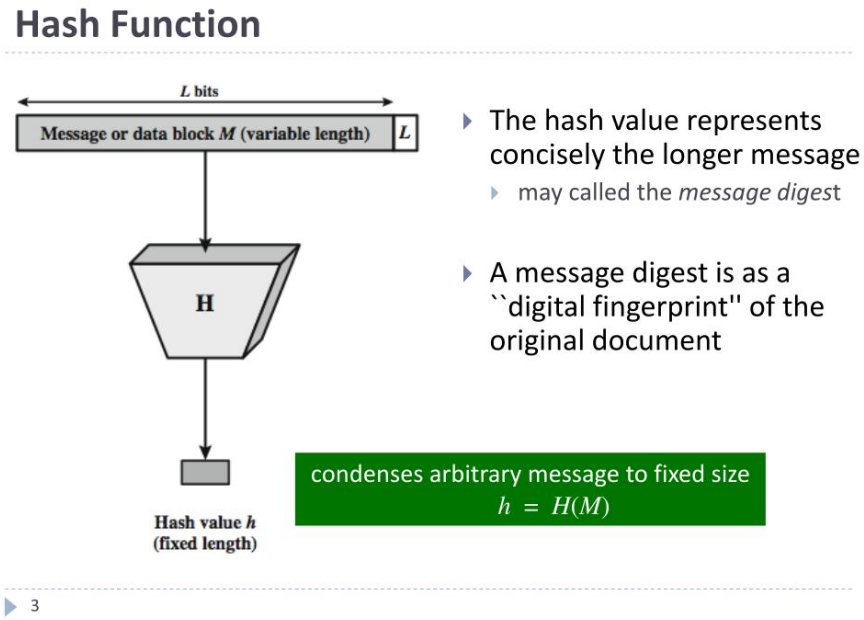
Asymmetric cryptography

- Asymmetric cryptography , also known as **Public-key cryptography**, refers to a cryptographic algorithm which requires two separate keys, one of which is **private and one of which is public**. The public key is used to encrypt the message and the private one is used to decrypt the message.



Hash Functions

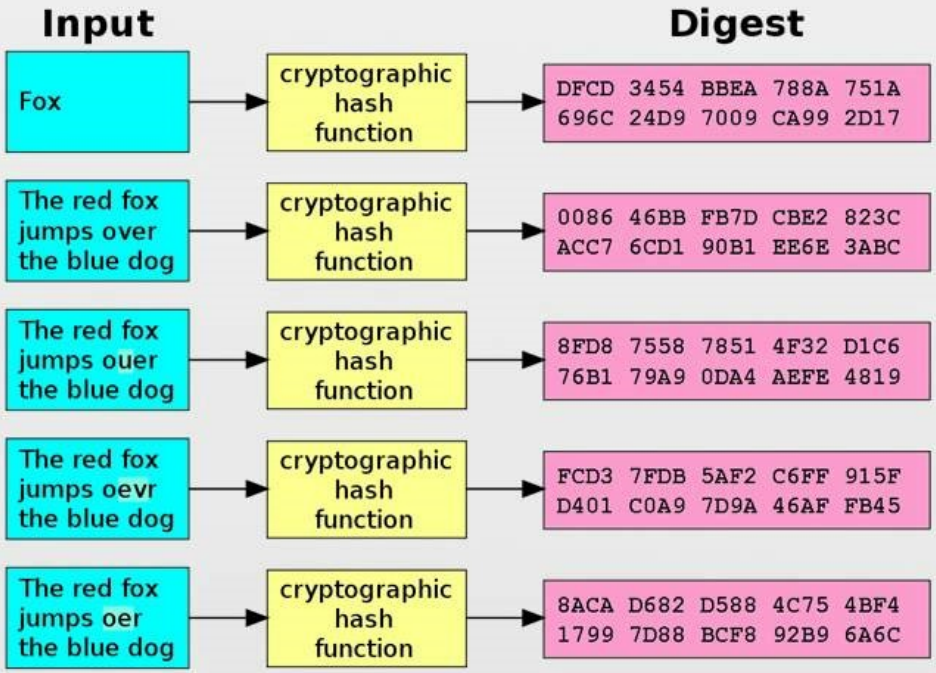
A cryptographic hash function is a hash function that **takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value**, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest



The ideal cryptographic hash function has four main properties:

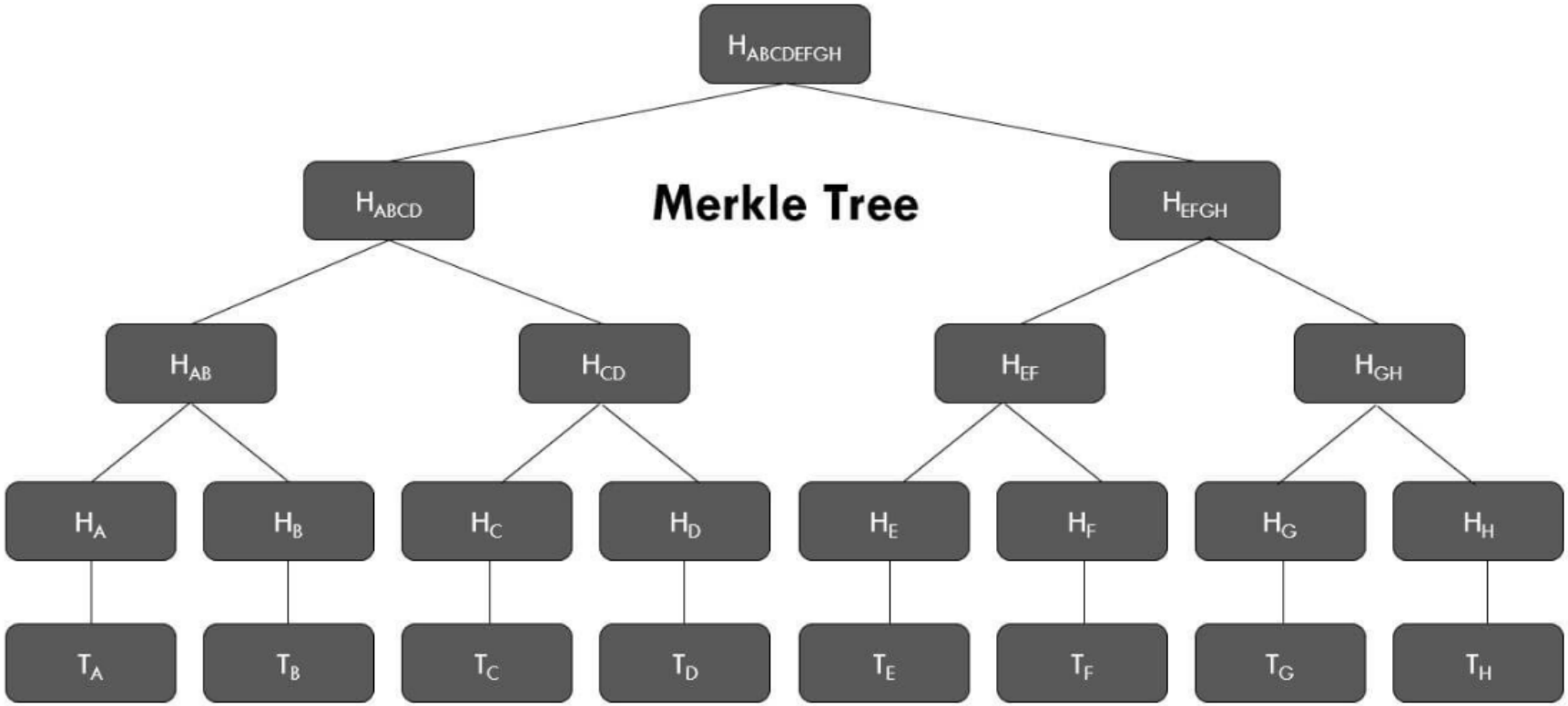
- It is easy to compute the hash value for any given message
- It is infeasible to generate a message that has a given hash
- It is infeasible to modify a message without changing the hash
- It is infeasible to find two different messages with the same hash.

Cryptographic hash function



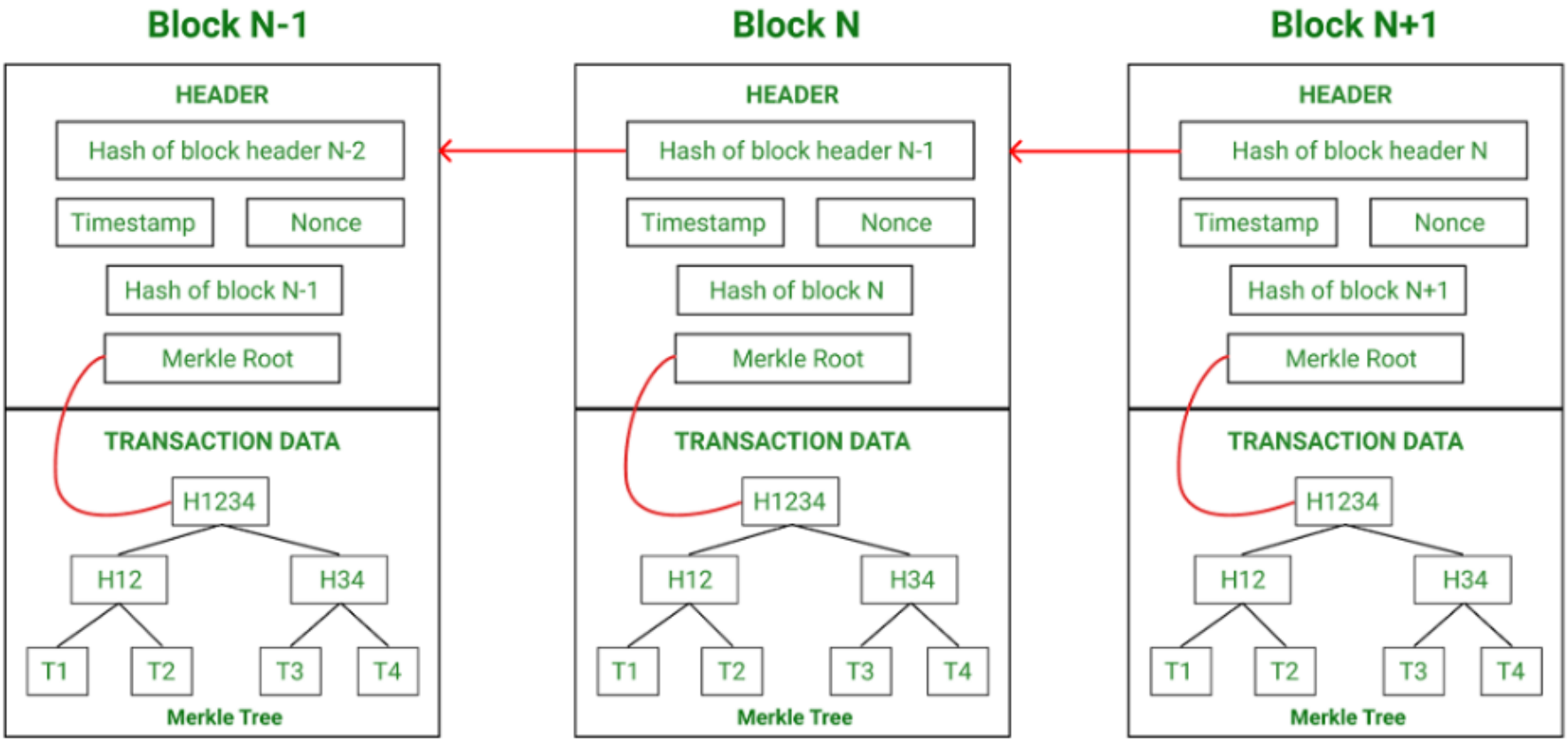
Merkle Trees

- Merkle tree (also known as hash tree) is a data structure used for data verification and synchronization.
- It is a tree data structure where each non-leaf node is a hash of it's child nodes.
- It maintains data integrity and uses hash functions for this purpose.


Merkle Tree
$H_{ABCDEFGH}$
H_{ABCD}
H_{EFGH}
H_{AB}
H_{CD}
H_{EF}
H_{GH}
H_A
H_B
H_C
H_D
H_E
H_F
H_G
H_H
T_A
T_B
T_C
T_D
T_E
T_F
T_G
T_H

Steps involved:

1. **Pairing Leaves:** Take two consecutive leaves and hash them together to create a new hash.
2. **Creating Intermediate Nodes:** Move up the tree, pairing and hashing the newly created hashes, until you have a single hash at the top.
3. **Root Hash:** The resulting top hash, known as the Merkle root, represents the entire dataset's integrity. This single hash encapsulates the essence of all the data below it. Any change in the underlying data would lead to a completely different Merkle root, making tampering evident.



Each block comprises of block header + Merkle tree