TCS332, Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

Blockchain-Overview

- **Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.**
- A blockchain is a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.
- Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that **transaction is added to every participant's ledger.**

Blockchain-Overview

- The decentralized database managed by multiple participants is known as **Distributed Ledger Technology (DLT).**
- Blockchain is a type of DLT in which transactions are recorded with an **immutable cryptographic operation.**
- For example, information (records) will be added in the form of certain encrypted transactions (i.e., encryption with the public key of the owner).

Properties of blockchain

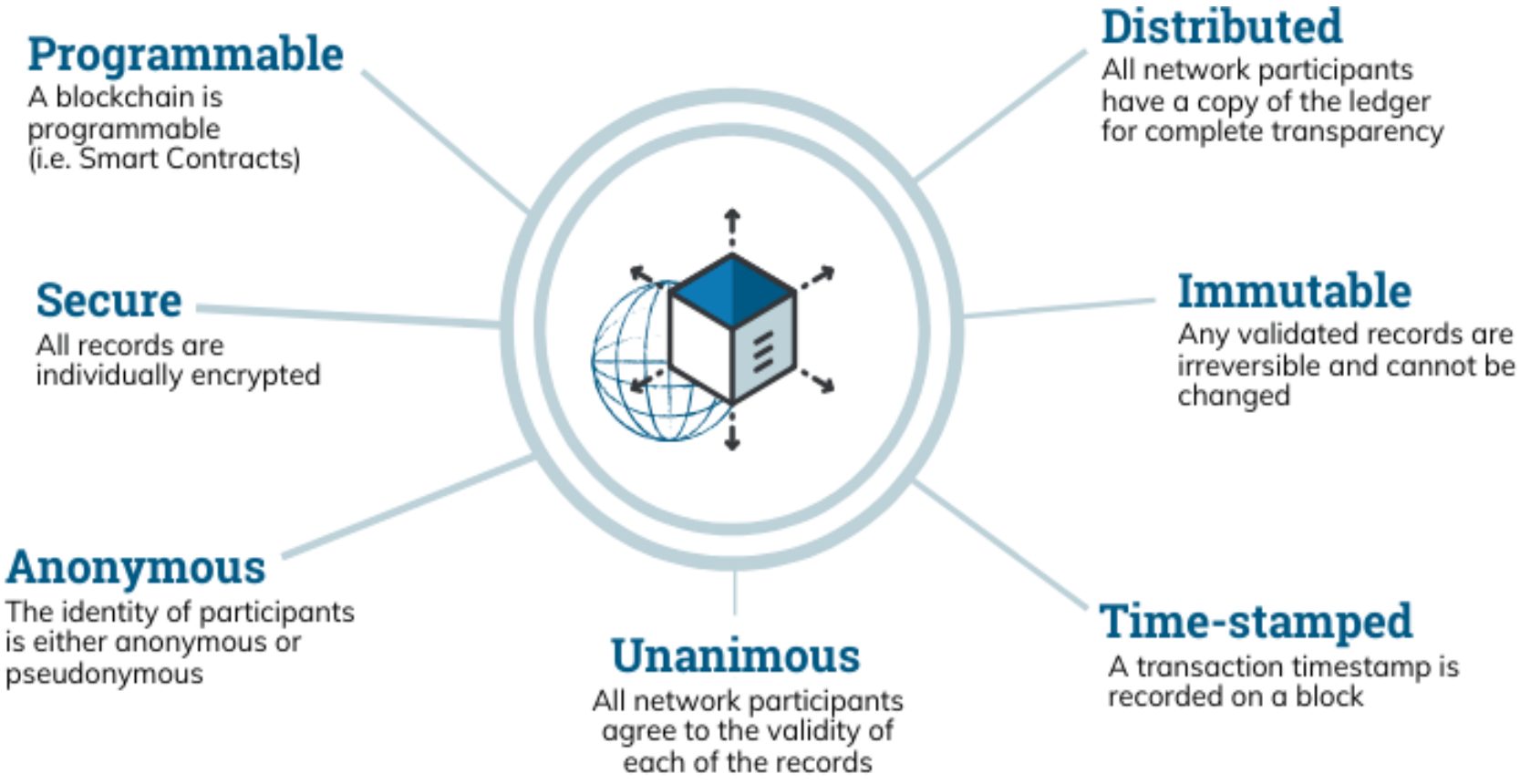


Fig. Properties of blockchain (DLT) (image source: https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

Security of blockchain

- Security of data is the foremost characteristics of blockchain.
- **Things we have to remember:**
- Whatever we store in the blockchain will be in the encrypted form.
- Hash of each block is also computed to preserve the integrity of data
- Signature of each block is also computed to provide the authenticity.
- Therefore, we achieve, secrecy, integrity and authentication at the same time.

Security of blockchain

- If one block in one chain was changed, it would be immediately apparent that it had been tampered/changed with.
- **If hackers want to corrupt the data of blockchain, then they would have to change every block in the chain, across all of the distributed versions of the chain.**

Security of blockchain

- Some blockchain based cryptocurrency frameworks like, Bitcoin and Ethereum are constantly growing as blocks are being added to the chain, which significantly adds to the security of the ledger.

Working of blockchain

- **Diagram shows that how blockchain processes actually execute in the form of a digital wallet.**

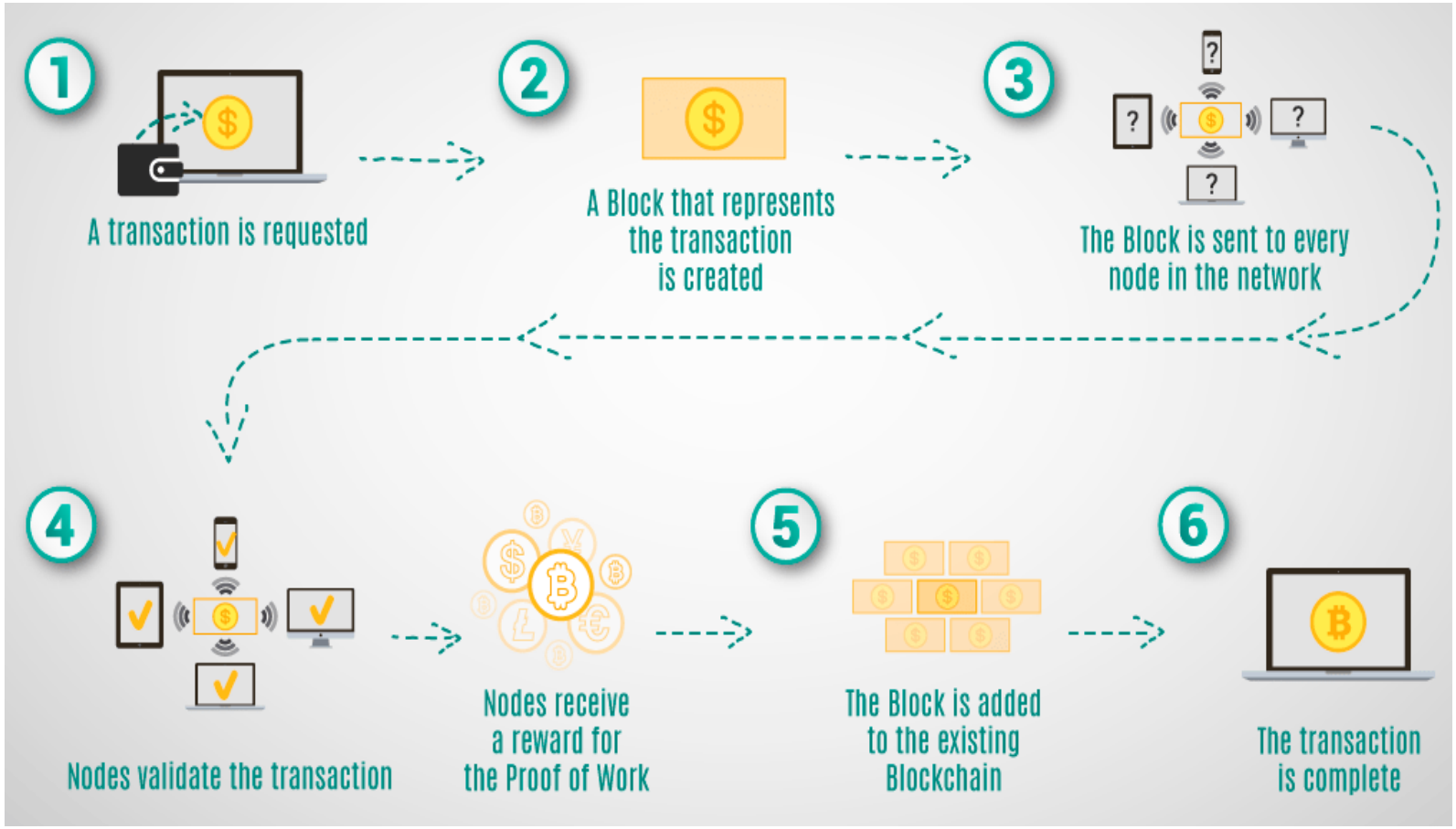


Fig. Working of blockchain (image source: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

Working of blockchain

- Any new record or transaction within the blockchain implies the building of a new block.
- Each record is then proven and digitally signed to ensure its genuineness.
- Before this block is added to the network, it should be verified by the majority of nodes in the system.

Core components of blockchain

- **Node:** User or computer within the blockchain architecture (each has an independent copy of the entire distributed ledger)
- **Transaction:** Smallest building block of a blockchain system (i.e., encrypted records) 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

Core components of blockchain

- **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/algorithm):** A set of rules and arrangements to carry out blockchain operations

Benefits of use of blockchain

- **Cost reduction:**
- Lots of money is spent on sustaining centrally held databases (i.e., banking database) by keeping data secure from cyber crimes and other corrupt intentions.

Benefits of use of blockchain

- **History of data:**
- Within a blockchain structure, it is possible to check the history of any transaction at any moment in time.
- This is a **ever-growing archive**, while a centralized database is more of a snapshot of **information at a specific point**.

Benefits of use of blockchain

- **Data validity and security**:
- Once entered, the **data is hard to tamper** with due to the typical characteristics of blockchain.
- It **takes time to proceed with record validation** since the process occurs in each independent network rather than via compound processing power.
- This means that the **system sacrifices performance speed, but instead guarantees high data security and validity.**

Issues with blockchain

- **Effect on the communication environment**
- The blockchain-based environment relies on encryption techniques for security when establishing a consensus over a distributed network.
- If a party wants to add something to the chain, that party has to prove he/she has permission to add a block to the chain. The procedure executes a complex algorithm and, in turn, demands excessive use of computing power.
- For instance, **in the Bitcoin network over the last year, it is said that the computing power needed for the execution of networking tasks dissipated the same amount of energy needed by 159 countries.**
- Therefore, it is important to consider the energy requirement factor in the deployment of blockchain.

Issues with blockchain

- **Cost factor:**
- Apart from the above implementation cost is another challenge for the blockchain.
- Blockchain schemes are not that efficient in terms of execution of transactions and the related energy requirements.
- For example, the bitcoin scheme executes **3-5 transactions** per second and consumes a lot of energy in that work. If we compare its performance with other platforms, such as Visa, it seems worse because **Visa performs about 1,667 transactions** per second.

Issues with blockchain

- **Cost factor:**
- Therefore, to fulfill the requirements of a blockchain-based environment, we must accept a country's very high budget to secure some computing infrastructure.
- Only a few countries have the budget to support such kinds of communication schemes. **We need to invent efficient methods that can be deployed in the blockchain.**
- Therefore, this is another issue for people in the same domain.

Issues with blockchain

- **Loads from blockchain technology:**
- Blockchain is deployed with a distributed ledger and through cryptographic algorithms.
- Blockchain transactions require extra time and resources to process a transaction.
- The main objective of the blockchain-based environment is secure information exchange, which can be achieved through deployment of the blockchain mechanism. But **transactions in a blockchain may require extra hours to finalize.**

Issues with blockchain

- **Loads from blockchain technology:**
- Quick information exchange is a primary requirement in some domains (for example, battlefields, healthcare, and rescue operations).
- If the processing and exchange of information consumes extra time, then the intended recipient will not get the information within the required time.
- The concerned authority will not be able to make a decision within the desired reaction time.
- These issues can be sorted out by the **use of lightweight cryptographic operations,** because they need low computation, communications, and storage costs to process the transactions.

Issues with blockchain

- **Jurisdictional problems**
- Nodes of a decentralized ledger can span multiple locations around the world, it is often difficult to establish which jurisdictions' laws and regulations apply to a given application.
- There is a risk that transactions performed by an organization could fall under every jurisdiction in which a node in the blockchain network is situated, resulting in an overwhelming number of laws and regulations that might apply to transactions in a blockchain based system.

Blockchain architectures

- Three categories:
- **1. Public blockchain architecture**
- A public blockchain architecture means that the data and access to the system is available to **anyone who is willing to participate** (i.e., Bitcoin, Ethereum, and Litecoin).

Blockchain architectures

- **2. Private blockchain architecture**
- As opposed to public blockchain architecture, the private system is controlled only by users from a specific organization or authorized users who have an invitation for the participation (i.e., blockchain of a healthcare monitoring system)

Blockchain architectures

- **3. Consortium blockchain architecture**
- This blockchain structure can consist of a few organizations. In a consortium, procedures are set up and controlled by the preliminary assigned users (i.e., blockchain of a smart transportation system).

Blockchain architectures (differences)

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	impossible	possible	possible
Efficiency (use of resources)	Low	High	High
Centralization	No	Partial	Yes
Consensus process	Permissionless	Needs permission	Needs permission

Blockchain architectures (differences)

- A private blockchain is considered more centralized since it is controlled by a particular group with increased privacy.
- On the contrary, a public blockchain is open-ended and thus can be called as decentralized.
- In a public blockchain, all records are visible to the public and anyone could take part in the agreement (consensus) process.

Blockchain architectures (differences)

- On the other hand, this is less efficient since it takes a considerable amount of time to accept each new record into the blockchain architecture **(drawback of public blockchain).**
- In terms of efficiency, the time for each transaction in a public blockchain is less eco-friendly since it requires a huge amount of computation power compared to private blockchain architecture.

Blockchain architectures (differences)

- **Validator node:** These nodes can initiate, receive and validate the transactions **(i.e., miner nodes).**

- **Member node:** These nodes can only initiate and receive the transactions. They can not validate the transactions.

Blockchain architectures (differences)

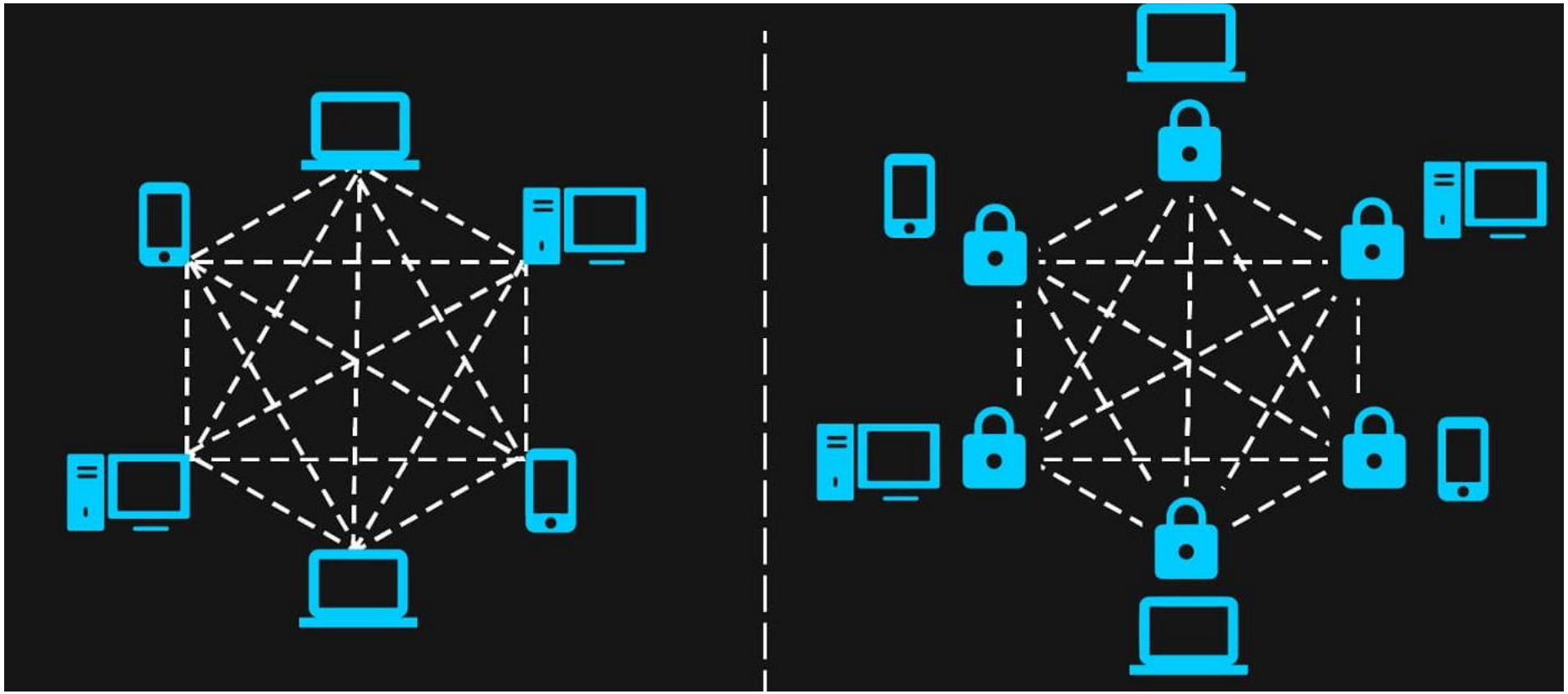


Fig. Differences between public blockchain and private blockchain (image source: https://101blockchains.com/permissioned-blockchain/)

Blockchain architectures (differences)

- **Public blockchain is a permission less network**. All entities (nodes) can freely access it without any kind of permission. The ledger is shared among the entities and transparent to all.
- **Private blockchain is a permissioned network**. A user (node) has to be permitted by the blockchain authority before his/her access to the network. User can only join if he/she gets the invitation.

Blocks and arrangements of blocks in a blockchain

- Genesis block is the very first block of the blockchain. Therefore, its hash value will be like 0000.
- Hash of current block will be connected to the hash of previous block field in the next block

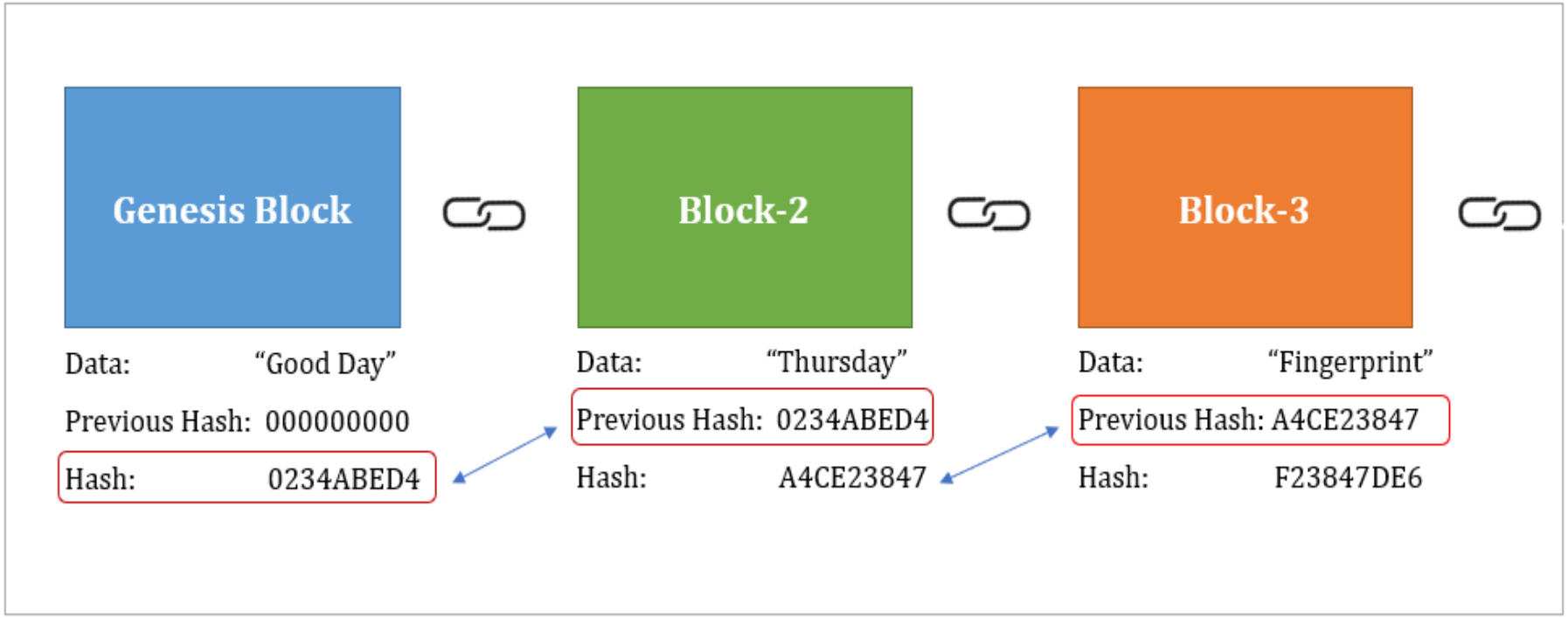


Fig. Arrangements of blocks in a blockchain (image source: https://medium.com/swlh/blockchain-characteristics-and-its-suitability-as-a-technical-solution-bd65fc2c1ad1

Blocks and arrangements of blocks in a blockchain

- Blocks are files where data pertaining to the network are permanently recorded.
- A **block records some or all of the most recent transactions** that have not yet entered any prior blocks.
- Thus, a block is like a page of a ledger or record book.
- Each time a block is ‘completed’, it gives way to the next block in the blockchain.
- A block is thus a permanent store of records which, once written, cannot be altered or removed.

Blocks and arrangements of blocks in a blockchain

- Blockchain is called an immutable ledger because it stores a record of transactions in blocks which cannot be changed, once created.
- **New blocks can be added to the block chain but data in the existing blocks cannot be changed.**
- **If a malicious actor alters the data in a block, the hash of that block gets changed and it does not match with the previous hash value of the next block.**
- The blockchain system realizes this and makes the change in the data invalid.

Structure of a block

Block Header	
Block Version	$BVer$
Previous Block Hash	$PBHash$
Merkle Tree Root	MR
Timestamp	TR
Owner of Block	OB
Public Key of Owner	Pub_{CS_j}
Block Payload (Encrypted Transactions)	
Encrypted Transaction #1	$E_{Pub_{CS_j}}(Tx_1)$
Encrypted Transaction #2	$E_{Pub_{CS_j}}(Tx_2)$
$\vdots$	$\vdots$
Encrypted Transaction $\#n_t$	$E_{Pub_{CS_j}}(Tx_{n_t})$
Current Block Hash	$CBHash$
Signature on Block using ECDSA	$BSign$

Structure of a block

The various fields utilized in a block of the blockchain are as follows:

Block Version:

It denotes the version of a block. The size of this field can be assumed as 32 bits.

Hash of previous block:

It consists the hash value of the previous block. The size of this field can be considered as 256-bits (if ``SHA256 hash algorithm" is taken).

Merkle Tree Root:

It is the Merkle tree root on the encrypted transactions, whose size is 256-bits as ``SHA-256 hash algorithm" is used.

Merkle Tree Root (MTR):

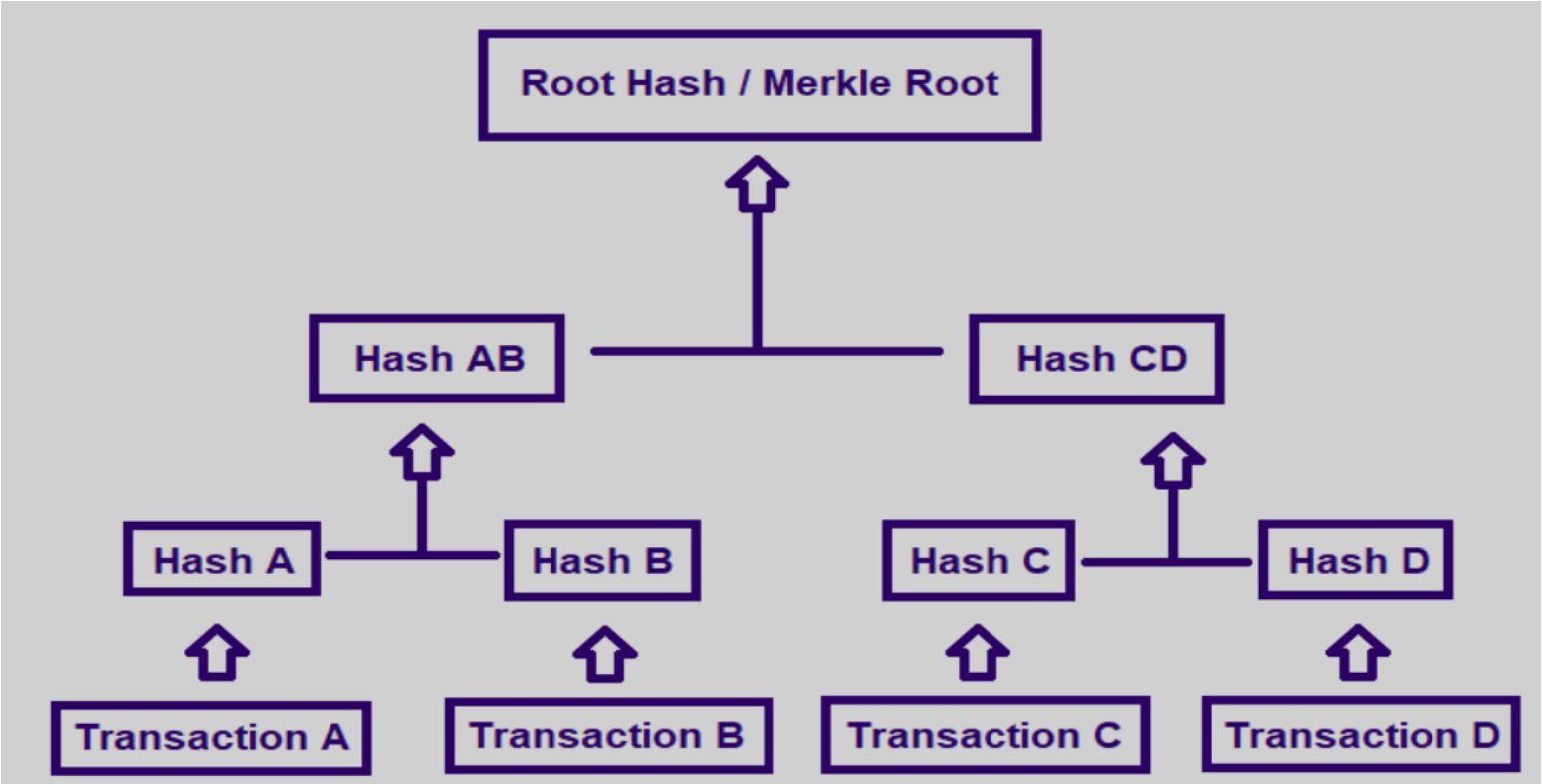


Fig. Computation of MTR (image source: https://nitk.acm.org/blog/2019/02/17/merkle-trees-and-their-application-in-blockchain/

Merkle Tree Root (MTR):

- Merkle tree root is used to reduce the volume of data and enable efficient validation of data on the blockchain.
- A merkle tree root is stored in each block and created by hashing transactional data that are included as part of the block. In the diagram below, there are four transactions (Tx).
- Each of these transactions are represented by a hash A-D. Each pair of hashes are further hashed (Hash AB and Hash CD), which are finally represented in the parent block as the merkle tree root (final hash value of all transactions).

Merkle Tree Root (MTR):

- Merkle tree root is used for the validation of transactions and it is more efficient.
- Rather than having to validate all of the data in a block, data for a single transaction can be sent along with the relevant hash values.
- The validating node can calculate the hash values for the given data and confirm that the transaction is valid without needing all of the data in the block.

Merkle Tree Root (MTR):

- **Zero-Knowledge Proof**
- Zero-knowledge proof enables a system to prove a condition of the message without revealing the actual contents of the message.
- For example, **if currency is being sent from one user to another, the blockchain can verify that the sender has enough money without needing to know who the user is or the total amount that the user has.**

Structure of a block

Timestamp:

It is the value of timestamp for a particular block. The size of this field can be considered as 32-bits.

Owner of Block:

It represents the identity of block owner. The size of this field can be considered as 160-bits.

Owner’s public key:

This field have the information of ``public key of the owner (miner) node". The size of this field is considered as 320-bits (since the ``Elliptic Curve Cryptography (ECC) algorithm" is considered).

Structure of a block

Encrypted transaction details:

It comprises the information about the ``ongoing transactions". For example, which entity (communicating party) is sending ``which information" and for ``what reason". The size of each encrypted transaction is ECC-based ciphertext. Thus, it requires (320 + 320)= 640 bits. If we consider 100 encrypted transactions, the payload of the block becomes (100 x 640) =64,000 bits.

Structure of a block

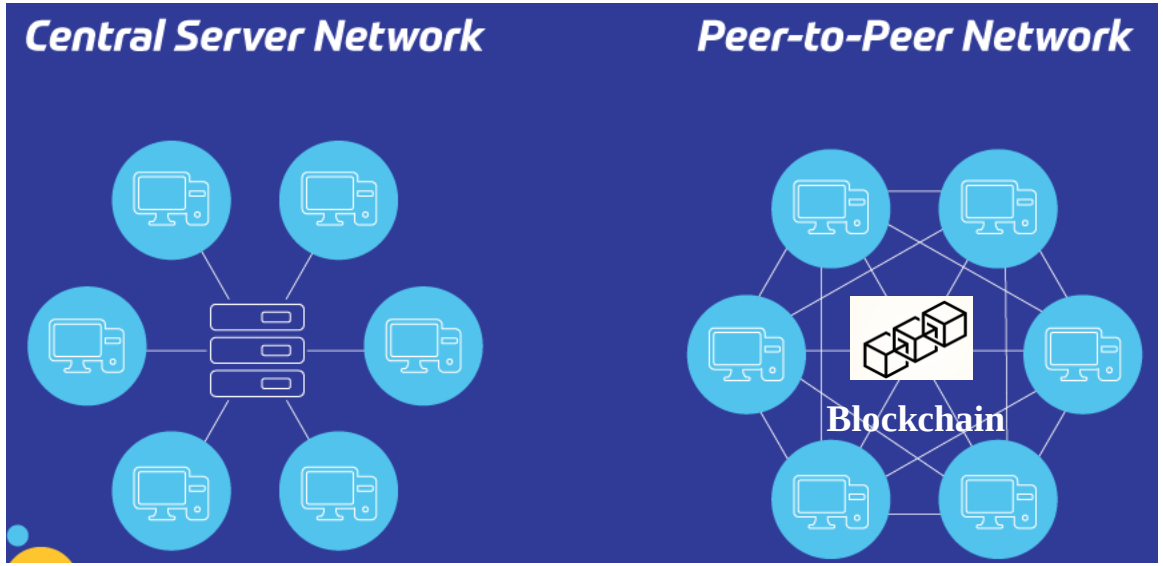
Hash of current block:

It contains the hash value of the current block. The size of this field is 256-bits (if ``SHA-256 algorithm'' is taken).

Block's signature:

It contains the ``signature information of a particular block''. The size of this field requires 320-bits (if ECC algorithm is applied).

Peer-to-peer cloud server (P2PCS) network



There is a central authority

There is no central authority

Fig. Differences between central server network and p2p network (image source: https://www.himss.org/resources/blockchain-healthcare

Peer-to-peer cloud server (P2PCS) network

- It is used for the implementation of a blockchain.
- The term “distributed” in distributed ledger technology (DLT) refers to the idea that it uses a peer-to-peer (P2P) network structure.
- Compared to a central server network, nodes on a P2P network are connected directly to each other rather than to a central server.
- There are no intermediaries (i.e., bank) to process the transaction.

Peer-to-peer cloud server (P2PCS) network

- This data distribution model is a defining characteristic of the technology.
- Here centralized authorities do not communicate updates to records.
- Instead, each node executes P2P communication to achieve consensus among the nodes and trigger updates in the form of blocks appended to the shared ledger.

References:

- William Stallings, “Cryptography and Network Security: Principles and Practice”, Pearson publication, 2020.
- George Icahn, “Blockchain: the complete guide to understanding blockchain technology”, 2020.
- Antony lewis, “The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them” 2020.
- Blockchain information available at: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture
- Blockchain information available at: https://www.euromoney.com/ learning/blockchain-explained/what-is-blockchain
- N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park. "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," in IEEE Access, DOI: 10.1109/ACCESS.2020.2995917.2020, Online. (2018 SCI Impact Factor: 4.098)
- M. Wazid, A. K. Das, S. Shetty, and M. Jo. "A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things," in IEEE Access, Vol. 8, No. 1, pp. 88700-88716, 2020, DOI: 10.1109/ACCESS.2020.2992467. (2018 SCI Impact Factor: 4.098)