Blockchain V/S Database: A Comparative Study

Anuradha Mall, Dept of Computer Science, Institute of Science, Banaras Hindu University, Varanasi, India, anuradha1020@bhu.ac.in

ABSTRACT

Blockchain (BC) has recently drawn a lot of attention from both the business world and academic circles. A data structure that records network transactions is the basis of the Blockchain technology. It is a digital ledger that keeps track of information in blocks of data. Its unique characteristic that sets it apart from current technology is the immutability of the records that are stored. Tables are data structures used to store information in databases (DB). While many academics and industry professionals are embracing the blockchain craze, some of them are voicing concerns about the basic distinction between blockchain and conventional database. This paper provides an overview of database, and blockchain. Furthermore, it describes about the various limitation of database. It also compares the database with blockchain on the basis of various properties.

Keyword*s*---Conventional database, blockchain, immutability.

I. DATABASE

A. INTRODUCTION

It is a type of data structure for keeping data in the form of tables. By linking data from many databases together using a relational model, it made it possible to collect data in more complex ways. A DB management system can be used to arrange the data kept in databases. An administrator is a single user who has power over a database and can make changes to it. It is recursive, meaning you can repeat an action on a certain record to edit or delete it. From tiny offices and home offices to corporate settings, databases are deployed using client/server architecture. This is so that computers may access or store information from the database, which is hosted on a server [3].

DB are extremely centralised because they require a lot of control. It also requires user accounts from an administrator, who then establishes permissions—sometimes known as rights—on how users may access databases. A typical database's centralization establishes the system's security and confidence.

In order to handle complex queries easily and swiftly extract desired output from the database, SQL and other data mining algorithms have progressed. For accessing, obtaining, merging, sorting, editing, or removing data from a database, an initial credential is necessary.

Not every entry in a database is secure, and it is not intended to track back any earlier database transactions.

B. FEATURES OF DATABASE

- **User-Friendly Customizability***:* The administrator can alter conventional centralised databases in accordance with company needs. Additionally, it can be sent to other sites, where the data can then be integrated into a central database for searches and reports. They provide powerful capabilities that let programmers build programmes that give users a more standardised and user-friendly experience.[2]
- **Consistency***:* A database system can execute hundreds of transactions per second and handle massive amounts of data when it is administered appropriately. They are also quick because they are permissioned, allowing only a small number of users to do write operations, and since the data is stored on a small number of servers yet can be made accessible to many users. Hardware and other methods like sharding and downsizing can be used to improve database speed. An administrator can also undo modifications in the case of a catastrophe. The administrator, who oversees the entire system, supervises all updates and security.
- **Transaction Volume and Speed:** Databases of today are built for both data analytics and high-volume transaction processing. This indicates that they have been tried, tested, and proven to work for mission-critical operations in business production settings.
- **Saves money and storage space:** The cost of data entry and storage will be reduced if the data is managed appropriately.
- **Scalability***:* Millions of records and thousands of transactions every second can be managed by databases with ease.

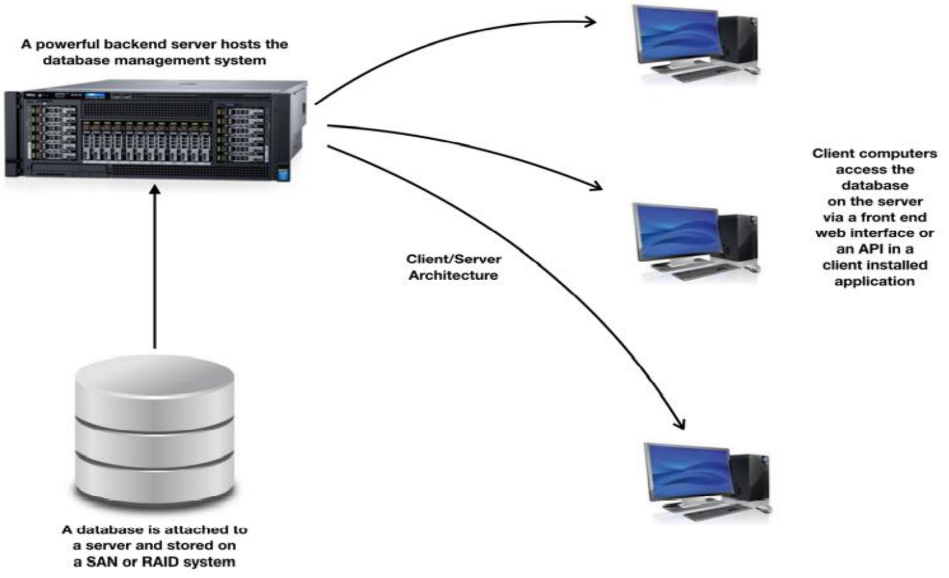
A powerful backend server hosts the database management system
Client/Server Architecture
Client computers access the database on the server via a front end web interface or an API in a client installed application
A database is attached to a server and stored on a SAN or RAID system

Figure 1: Database Topology: A Client Server architecture

C. DATABASE LIMITATIONS

- **Singular Point of Failure***:* There is a single point of failure because it is centralised. Information that is under the custody of one corporation can be made profitable for use by others, but this isn't always in the users' best interests. Another problem arises when a database is breached since the information of numerous users may be impacted. The entire system is impacted when a database server crashes. There is no way to recover important data if there is no backup of the data kept in the database. This is why redundancy and failover are crucial in centralised systems.
- **Administrator Account***:* Because a database needs an administrator, it becomes more difficult to recover a database if the password is forgotten. It becomes a very time-consuming operation to reset passwords and increase the authority of a new administrator when a database administrator departs the organisation.
- **Security Concerns***:* If the administrator of a centralised system neglects to install patches and updates, the system may be subject to hacker security attacks. Database breaches are more likely as a result. Although centralization is intended to simplify management, it can occasionally lead to serious issues that compromise a system's ability to maintain data integrity.
- **Transparency***:* No other node can track the transaction history or the transaction itself; only administration can do so.

II. BLOCKCHAIN RESOLVES DATABASE-RELATED PROBLEMS

A. Security

Not all database entries are secure, nor are they intended to reverse any earlier transactions. In contrast, every transaction on a blockchain is cryptographically protected, which ensures security and allows all participating nodes to share the ledger's current state.

B. Decentralised

Unlike databases, which are centrally controlled and each node is overseen by a single administrator, blockchain is decentralised, making it extremely fault tolerant. Since data held on one computer must be duplicated to every network node, decentralisation increases security.

C. Establishing Trust

One of the main features of BC technology is immutability. The decentralised consensus process creates immutability. Each participating node takes part in a consensus technique to assess if a certain transaction is legitimate or not. Each node in the system has equivalent access and capabilities (for instance, to the public blockchain). Due to the system's overall democratisation, this offers a strong platform for fostering trust. In a conventional DB, we must depend on one central authority to regulate system access. When the person in charge of the system is dependable and trustworthy, the system is good.

D. Transparency

A database is not transparent if only the administrator can follow a transaction's history; by contrast, every node and block in a blockchain can follow a transaction's history.

E. Robustness and Error Tolerance

Blockchain is a decentralised technology that makes use of distributed computing to offer reliability and fault tolerance. The blockchain uses distributed storage to store data. A copy of the blockchain is kept by each participating node. As a result, it is possible for all sorts of cyber threats to target isolated point of failure. The work can still be done by other nodes even if one of them fails or is compromised.

F. Redundancy

With a database, the copy of every transaction is owned by the central administrator, whereas in a blockchain, every participating node possesses the most recent copy of every transaction.

III. BLOCKCHAIN

A. Introduction

Blockchain technology promises to establish a decentralised ecosystem in which data and transactions are managed independently by all parties. Data that is organised into blocks is kept in a database. When data is added to a BC, it can only be read; once it has been added, it cannot be changed; and new data can be only uploaded at the blockchain's ending.

A ledger made up of consecutive blocks linked together in accordance with rigorous guidelines is known as a blockchain. The nodes of a Peer-to-peer network maintain and disseminate the ledger, in which each block is generated every specified length of time via a decentralised consensus process. The network's participating nodes can communicate with one another. There isn't a "master" in charge of all nodes. The BC allows any node to contribute in decision-making, making the system democratic and monopoly-resistant.

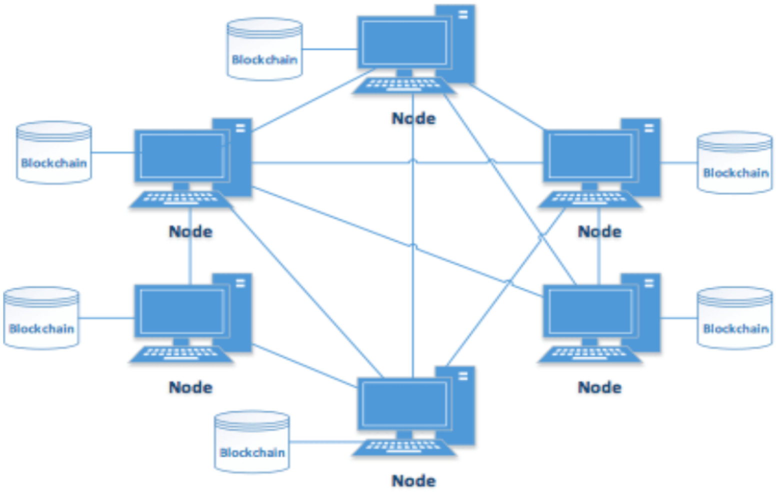

Figure 2: Blockchain Peer to Peer Network

B. CURRENT BLOCKCHAIN NETWORK NODE ARCHITECTURE

Traditional peer-to-peer networks and structured modular networks are the two categories used to describe the blockchain network architecture [6]. Most digital currencies, like Bitcoin, employ the former, whereas alliance chains use the latter.

- **Traditional Blockchain Architecture:** A community or cooperative group often updates unified wallet software, which is used by traditional digital currency systems as a node carrier and maintains a fair condition for all nodes. As a result, a node typically maintains the entire ledger database and is paid in digital money from nearby miners. The node also initiates a transaction, keeps the recipient's private key, acts as a gateway for someone else, and completes basic functions (consensus, encryption-decryption, and many more). As a result, while the architecture's nodes are all comprehensive, bespoke optimization is challenging. Users and businesses communicate through transactions, more specifically those from the Decentralised application contract. In a P2P network, the transaction is broadcast to the BC. This allows for the simultaneous independent processing of the same transaction request by several nodes. However, according to the consensus rules, only single node should utilise the billing opportunities during the course of a period. As a result, it is pointless for nodes to conduct this transaction without accounting.

The following problems with the standard digital currency proposed system are described in broad terms:

a) **Resource wastage on the node:** In order to start making money, the members first mortgage their computing resources. Their earnings obtained put toward enhancing system performance. However, since there is competition between the nodes, they are unable to work together and handle repeated transactions on their own. None of the resources may be used entirely.

b) **Lack of modularity***:* Authorized publishers carry out all of the integrated tasks of digital currencies. The participants must make use of official node software that is completely built. Due to the difficulty in allocating or modularizing node functions in accordance with the benefits of the computer resources at their disposal, decentralized techniques like micro services cannot be used. Efficiency, interoperability, and privacy might thus develop into unrecognised problems in the future.

c) The CDBC design philosophy is at odds with the competitiveness of transaction processing fees. Users must pay higher fees in a system with poor performance to guarantee that their transactions are given priority. This goes against the social justice that CDBC demands.

- **Modular Blockchain Architecture:** The nodes have higher trust among peers since the alliance network itself is employed in a somewhat centralised setting. Alliance chain architecture designs, such the Hyperledger Fabric [7], are more adaptable. Particularly, this design specifies various permissions for nodes and modularizes their operations. This allows for the repair of the defective part when a malfunction develops. If necessary, a particular type of node can have its processing capability increased by itself. The system's performance is enhanced by the design, which reduces repetitive processing labour and saves more resources.

This design still has a number of issues. At first, the alliance chain network now in use is primarily intended to allow data sharing between commercial companies from various industries. All chain operations, even basic transactions, are built on smart contracts to increase business richness. Despite the fact that we are able to carry out every one of CBDC's requirements using smart contracts, the program's speed and agility are inferior to those of performing fundamental functions specifically. Second, a similar technique is used to create numerous sub-chains as the answer for authorization in the alliance network. The same architecture is used by node with various permissions to establish many BC [8]. The design is inappropriate for the CDBC, which must be united.

The conventional digital currency design has many disadvantages in terms of resource usage and operational efficiency as compared to a centralised system. Although the modular architecture performs quite well, the CDBC reform does not meet the original design objectives.

C. PROPERTIES OF BLOCKCHAIN

A blockchain demonstrates a number of characteristics which makes it a viable option for a wide range of application fields. These characteristics are covered below.

- **Chain state distributed consensus***:* The capacity of any blockchain to reach a chain state distributed consensus independently about any third parties is one of its key characteristics. It now becomes possible to design and use a system in which any potential state or interaction may be independently verified by the designated parties.
- **Chain state's immutability and irreversibility:** After a specific amount of time, a decentralized consensus is achieved with the help of significant number of nodes, making the BC state effectively irreversible and unchangeable. This holds true for smart contracts as well, making it possible to deploy and run immutable computer programmes.
- **Permanence of data (transactions):** Data in a BC is distributed stored, ensures its persistence so long as there are active nodes inside the Peer-to-Peer network.
- **Data extraction:** Any blockchain that stores data uses a mechanism called a transaction to make this process easier. Public key cryptography must be used to digitally sign each transaction in order to verify the authenticity of the data resource. This creates a powerful quasi tool about any data in the BC when combined with the immutability and irreversibility of a blockchain.
- **Control over decentralized data***:* A BC makes sure that the data is kept in the network in a decentralized fashion with not any single potential site of failure.
- **Integrity and openness:** They are encouraged because every transaction between participating organisations as well as the chain's current status may be confirmed by any authorised entity.

D. Consensus Mechanism in the Blockchain

The consensus process, which explains how the miner synchronise the records, is foundation of the BC system. To guarantee that the system could continue to operate regularly even when faced with severe situation, the consensus process is centred on most of the blockchain architecture's components. Proof of Stake (POS), Proof of Work (POW), Ripple Consensus Protocol (RCP), Practical Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPOS), and others are typical consensus procedures [9,15].

- **The Proof of Work Consensus Technique:** The Proof of Work mechanism is created specifically for such Bitcoin network. To guarantee data consistency and consensus security, dispersed nodes compete for computer resources. The Proof of Work network's nodes competing for record creation through intricate but pointless calculations. With the exception of certain nodes having just half the computation power, the network can remain stable. The duration of manufacturing each block cannot be too brief in order to address the issue of block forks. However, this can slow down the pace at which transactions are processed.
- **The Proof of Stake Consensus Technique:** In Proof of Stake based cryptocurrency's, the next block's maker is picked using a variety of combinations of wealth or age and random selection (i.e., the stake). The node with the larger stake has a simpler time obtaining the ledger writing authority. Because sophisticated computations do not need to be performed by the accounting nodes, resource usage is efficiently avoided. However, the nodes with the largest mortgage interests are always the ones that can get bookkeeping power. As a result, there is a chance that the wealthiest node may take over the network. Similar to POW, the blockchain system's transaction processing performance has to improve in order to resolve the hard block fork.
- **The Practical Byzantine Fault Tolerance Consensus Technique:** The total number nodes must be atleast 3f+1 for PBFT solution to be stable, where f is the amount of node that don't reply to failures or faults. Ideally, the nodes must communicate 2n2 + n times (n being the number of nodes) in order to reach agreement, which is inefficient whenever n is large. However, the system is still quicker than Proof of Work& safer than Proof of Stake.
- **The Delegated Proof of Stake Consensus Technique:** In accordance with the Proof of Stake algorithm, the DPOS consensus algorithm has been enhanced. Block producers' nodes are now much more limited in their reach, and all these major nodes offered their money or computing power to win the support of the whole channels. To synchronise and broadcast blocks, these master nodes employ either a PBFT or a limited POS consensus. The processing speed is increased and broadcast numbers and resource requirements are decreased because there are often less than 50 producer nodes. However, there are a few things to think about: First off, since the likelihood of the Sybil Attack is low among regular users, this should be taken into account. Second, the DPOS utilised in EOS indicates that a high latency network makes the block fork easy to emerge, necessitating extra remedial action. Therefore, the performance of DPOS might be poorer in rare circumstances.[9]

When fraudulent nodes control half of the resources or votes in the Proof of Work& Proof of Stake consensus mechanisms, the majority of contributors may just confirm the content of the blocks that was created. The PBFT technique is reliable and effective, but as the number of nodes grows, performance may suffer significantly.

E. Features of Blockchain

Various features of the blockchain are listed in the table 1: -

Table 1: Feature of Blockchain with its description

Features	**Description**
Decentralised	No central authority or middleman to supervise and approve transactions
Responsibility and openness	It encourages accountability and transparency because every contact between participating entities as well as the chain's current state can be confirmed by any authorised entity.[4]
Immutability	Once a transaction is uploaded to the BC & verified by the participation of active nodes, it can't be altered or manipulated.
Availability	The ledger itself is accessible to node security because to its distributed and decentralised nature.
Security	Utilizing a strong public/private key pair, a hashing method, digital signatures, and encryption
Non repudiation	Once a transaction has been uploaded to and approved on a BC, the blockchain node can't find it.
Auditability	Make it possible for users to track any transaction inside a ledger

Identification of data tampering	Since the current block contains the hash value of the preceding blocks, any modification with the contents in any block would result in changed hash value, which is a sign that tampering has occurred.
Data durability	As soon as there are active nodes in the Peer-to-Peer network, the distributed repository of data on a blockchain ensures its persistence. [4]

F. Limitation of Blockchain

- **Energy consumption**: Adding transactions to a blockchain requires a high and constantly changing charge. The complexity of the puzzle (which needs a lot of energy consumption) and the block mechanism along with the difficulty of the puzzle lead to the miner nodes behaving correctly.
- **Scalability**: Blockchains struggle to handle enormous volumes of transactions. There are issues with the rising transaction volume because of the fixed block size.
- **Size:** They slow down as they grow larger because they require more storage space. It takes a lot longer to copy blockchains to new nodes on the network when they are larger. Depending on the network capacity, it may take a few hours to several days. More bandwidth is required to transport data to another node due to the increased blockchain size. This has an impact on newly installed nodes as well as outdated nodes that come back up.

IV. BLOCKCHAIN AND DATABASE TECHNOLOGY COMPARISON

The blockchain and database technology comparison iterations are reported in Table 2. We will outline the specifics of this comparison using the various criteria outlined in [10] in the section that follows. We have presented a more thorough study (in comparison to [10]) by taking into account various consensus techniques and attack vectors.

A. Establishing Trust

Immutability is among the key characteristics of BC technology. The decentralised consensus process creates immutability. A consensus process is used by each participating node to determine if a given transaction is legitimate or not. Each node in the network has the equivalent capabilities and amount of accessing (for example, to the public blockchain). Because it democratises the entire system, this offers a strong foundation for fostering trust. Inside a conventional DB, we are compelled to trust a particular central administration that manages network accessibility rights. When the person in charge of the system is trustworthy and acts honourably, the system is beneficial.

B. Confidentiality and Privacy

A common misunderstanding regarding blockchain is that it only stores encrypted data. This is untrue, though. The participants to the transaction have digitally signed the data, but it isn't automatically encrypted. In actuality, it is a public record model in which anyone out there may part & verify every network transaction. Although, public key cryptography is used to protect the participants' confidentiality and privacy. The transactions make the parties to the transaction and their data visible. Strong anonymization has newly been proposed by investigators utilising cryptographic techniques as the Zero Knowledge protocol [14].

C. Reliability

A distributed computing technique is used by blockchain, a decentralised system, to offer resilience and fault tolerance. Distributed storage is used for data on the blockchain. Every node that is taking part keeps a replica of the BC. As a result, it could be any kind of online assailant that poses a threat to a singular point of vulnerability. The BC network is impervious to attacks like DoS &DDoS. Other nodes can still complete the task even if one node fails or is hacked.

D. Performance

Bitcoin and blockchain in general are notoriously sluggish. A network confirmation of a transaction takes ten minutes. If the network experiences a soft fork [11], this duration might increase to 60 minutes. Thousands of transactions per second may be handled by conventional database systems. The network manager can change the network to support significant number of transactions if he discovers a performance bottleneck. Research is being done to increase the consensus mechanism's effectiveness, nevertheless, in terms of performance. Within 10 to 20 seconds, consensus algorithms like Ethash [12] and X13 [13] can reach an agreement.

E. Security

Blockchain's elasticity plays a role in its security. More users may be needed to reach consensus as the system's user base grows. A block in the Blockchain protocol is approved if 51% of the mining nodes concur. Therefore, an "invalid transaction" might be regarded as a "legal transaction" if fraudulent individuals control 51% of the mining nodes. It might appear difficult, yet it is doable if there are enough participants in the network.

In such a conventional DB, the state of a database is maintained by a centralised system. Access to the data is regulated by the accessibility management technique the system has developed. This system is vulnerable if the network manager is exploited.

Table 2: Database and Blockchain Comparison

Properties	BC	Conventional DB	Benefit
Establishing trust	could function without the involvement of a reliable third party	managed by a single, trustworthy party	Blockchain
Reliability	Data distribution between nodes	Information is kept in a central database.	Blockchain
Confidentiality of data	All of the nodes can see the data.	Only authorised people are allowed access.	Database
Performance	Consensus is reached slowly.	execution or updating of nodes instantly	Database
Redundancy	Every contributing server has the most updated incarnation.	Replication exists in the centralised System.	Blockchain
Security	Utilize cryptographic constraints	uses conventional access control	Blockchain

V. CONCLUSIONS

The blockchain is appreciated and approved for its peer-to-peer architecture and decentralised design. Bitcoin could, however, cover a majority of blockchain research. Blockchain, however, has several uses that go far beyond Bitcoin. We've undertaken a comparative analysis between blockchain and conventional database systems on the basis of the several characteristics utilised to rate an information technology. We have discovered that blockchain is a superior option if the system's priorities include building trust, scalability, fault tolerance, and data redundancy. Traditional databases are still the preferable option if performance and integrity are your major priorities.

REFERENCES

[1] Tabora, V. (2018). Databases and blockchains, the difference is in their purpose and design. *Hentet*, *13*, 2019.

[2] Greenspan, G. (2016). Blockchains vs centralized databases. *MultiChain: London, UK*.

[3] Rehmani, M. H. (2021). *Blockchain Systems and Communication Networks: From Concepts to Implementation*. Springer.

[4] Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018, August). Blockchain versus database: A critical analysis. In *2018 17th IEEE International conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)* (pp. 1348-1353). IEEE.

[5] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375.

[6] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE transactions on knowledge and data engineering*, *30*(7), 1366-1385.

[7] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference* (pp. 1-15).

[8] Mukhopadhyay, S. (2019). Identification of normal modes responsible for ferroelectric properties in organic ferroelectric CBDC. *Journal of Physics Communications*, *3*(11), 113001.

[9] Zhang, J., Tian, R., Cao, Y., Yuan, X., Yu, Z., Yan, X., & Zhang, X. (2021). A hybrid model for central bank digital currency based on blockchain. *IEEE Access*, *9*, 53589-53601.

[10] Greenspan, G. (2016). Blockchains vs centralized databases. *MultiChain: London, UK*.

[11] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, *19*(5), 653-659.

[12] Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016, December). A brief survey of cryptocurrency systems. In *2016 14th annual conference on privacy, security and trust (PST)* (pp. 745-752). IEEE.

[13] Rabah, K. (2017). Overview of blockchain as the engine of the 4th industrial revolution. *Mara Research Journal of Business & Management*, *1*(1), 125-135.

[14] Fortnow, L. (1987, January). The complexity of perfect zero-knowledge. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing* (pp. 204-209).

[15] Kant, K., Pandey, S., & Shanker, U. (2022, May). A journey from commit processing in distributed databases to consensus in blockchain. In *2022 IEEE 38th International Conference on Data Engineering (ICDE)* (pp. 3236-3240). IEEE.