Comparative Analysis of Transaction Speed and Throughput in Blockchain and Hashgraph: A Performance Study for Distributed Ledger Technologies

[1]Dinesh Kumar K, [2]Duraimutharasan N, [3]Shanthi HJ, [4]Vennila G, [5]Prabu Shankar B and [6]Senthil P
[1]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, TamilNadu, India.
[2] Department of Computer Science and Engineering, AMET University, TamilNadu, India.
[3] Department of Computer Applications, Hindustan Institute of Technology and Science, TamilNadu, India.
[4]Department of Artificial Intelligence and Machine Learning, Mohan Babu University, Andhrapradesh, India.
[5] Department of Computer Science and Engineering, Alliance University, Karanataka, India.
[6]Department of Computer Science and Engineering, Gojan School of Business and Technology, TamilNadu, India.
[1]dineshkumar01@gmail.com, [2]duraibose@gmail.com, [3]shanthi_harold@yahoo.co.in, [4] vennila.g@mbu.asia
[5]prabu2000@gmail.com, [6]pv.senthil25@gmail.com

Correspondence should be addressed to Dinesh Kumar K : dineshkumar01@gmail.com.

Article Info
Journal of Machine and Comp uting (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202303041
Received 20 March 2023; Revised from 18 July 2023; Accepted 12 August 2023.
Available online 05 October 2023.

Abstract – Blockchain technology garners significant attention and recognition due to several key advantages it offers. Trust, reliability, speed, and transparency are among the prominent benefits that contribute to its growing prominence. The decentralized nature of blockchain allows for a high level of trust as transactions are recorded and verified by multiple participants across the network. This, in turn, enhances reliability as there is no single point of failure. Speed is also a notable advantage, particularly when compared to traditional systems that involve intermediaries and complex processes for verification. Blockchain enables faster and more efficient transaction processing, reducing delays and costs. This research paper aims to provide a comprehensive comparative analysis of two prominent distributed ledger technologies, namely blockchain and hashgraph. Both blockchain and hashgraph offer decentralized and secure systems for recording and validating transactions or information. It explores the underlying mechanisms, consensus algorithms, advantages, and limitations of these technologies. It also examines their potential applications and discusses the implications of their respective design choices. By understanding the nuances of blockchain and hashgraph, seeks to contribute to the ongoing discourse on distributed ledger technologies and aids in decision-making for their appropriate adoption in various domains and applications.

Keywords – Blockchain, Hash Graph, Distributed Ledger Technologies, Consensus Algorithm, And Decentralized Systems.

I. INTRODUCTION

Distributed ledger technologies have revolutionized the way transactions and information are recorded and verified in decentralized systems. Two prominent technologies in this field are blockchain and hashgraph. Both blockchain and hashgraph aim to provide secure, transparent, and decentralized systems for various applications. This introduction provides a detailed overview of blockchain and hashgraph, highlighting their key features, underlying mechanisms, and potential applications. Blockchain technology gained widespread recognition with the emergence of cryptocurrencies, particularly Bitcoin [1]. At its core, blockchain is a decentralized and distributed ledger that enables the recording and validation of transactions in a transparent and secure manner. The blockchain consists of a chain of blocks, with each block containing a set of transactions or data. These blocks are linked together using cryptographic hashes, creating an immutable and tamper-evident record which

is cryptographically secured. One of the fundamental aspects of blockchain is its consensus mechanism, which ensures agreement among network participants on the state of the ledger. Two commonly known consensus mechanisms used in blockchain are Proof of Work (PoW) and Proof of Stake (PoS) [2]. PoW involves miners competing to solve complex mathematical problems, while PoS allows validators to secure the network based on the number of tokens they hold or stake. Blockchain technology provides several benefits, including decentralization, transparency, security, and immutability. It eliminates the need for intermediaries or central authorities, as the consensus protocol ensures the validity and integrity of transactions [2]. Blockchain has expanded beyond cryptocurrencies and is being explored in various domains, such as supply chain management, healthcare, finance, Educational Certificate verification and voting systems [3].

Hashgraph: Hashgraph is a distributed ledger technology that offers an alternative approach to achieving consensus and maintaining a decentralized network. It employs a directed acyclic graph (DAG) data structure instead of a linear chain of blocks used in blockchain. Hashgraph aims to provide high throughput, low latency, and fairness in transaction processing. The underlying consensus algorithm used in hashgraph is known as the Hashgraph consensus algorithm [1]. This algorithm operates based on a combination of gossip about gossip and virtual voting. Network participants exchange information about events, representing transactions, through a gossip protocol. This information is then used for virtual voting to determine the order and validity of events in the hashgraph [4].

Hashgraph technology boasts scalability and performance advantages compared to traditional blockchain systems. It claims to achieve high transaction throughput and low latency, making it suitable for applications requiring fast and efficient processing. Hashgraph's design also offers fairness by providing a consensus order for events, eliminating the need for mining or staking competitions. Hashgraph has potential applications in various domains that require real-time transaction processing, such as financial services, supply chain management, Internet of Things (IoT), and gaming [4].

II. ARCHITECTURE AND COMPONENTS OF A DISTRIBUTED LEDGER TECHNOLOGIES

Architecture of blockchain

The architecture of a blockchain system is made up of the following components

Nodes: Nodes are the computers that participate in the blockchain network. They store the blockchain ledger and verify transactions. Transactions: Transactions are the smallest unit of data that can be stored on a blockchain. They typically represent the transfer of value between two parties.

Blocks: Blocks are groups of transactions that are bundled together and secured using cryptography. Chain: The chain is the chronological ordering of blocks that make up the blockchain ledger. Consensus mechanism: The consensus mechanism is the process by which nodes agree on the validity of transactions and blocks.

Ledger: The ledger is the database that stores blockchain data. It is distributed across all nodes in the network. Wallet: A wallet is a software application that allows users to store, send, and receive cryptocurrency [2].

The blockchain architecture is a complex system, but it is designed to be secure, decentralized, and transparent. These features make blockchain a promising technology for a variety of applications, such as financial services, supply chain management, voting Intellectual Property Management, Land Registry and Health care [3]. The blockchain version has smart contract feature which provides wide application in the area of Insurance, legal contract, Decentralized finance, Non-fungible tokens. The potential applications of blockchain are still being explored and vast. As technology continues to develop, we can expect to see even more innovative and groundbreaking applications emerge which provides decentralized infrastructure for secure transaction.

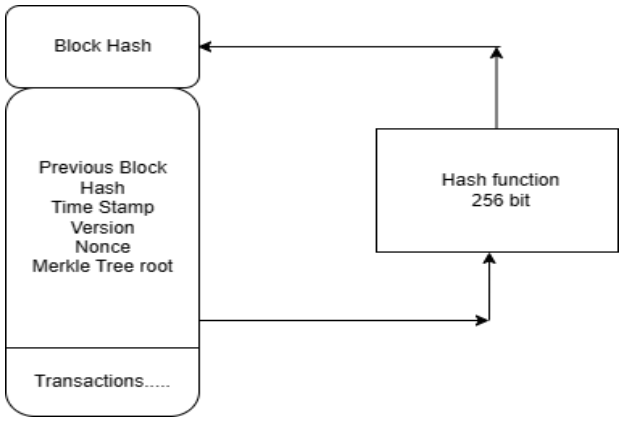

Fig 1. Blockchain Operation provides 256 bit Block Content and other Elements of Block

The diagram **Fig 1** shows the different components of a blockchain system and how they interact with each other [5]. The nodes are connected to each other in a peer-to-peer network. They communicate with each other to share the blockchain ledger and verify transactions. The transactions are bundled together into blocks. Each block is secured using cryptography and contains a hash of the previous block. This creates a chain of blocks that are linked together cryptographically. The consensus mechanism is used to ensure that all nodes agree on the validity of transactions and blocks. This is done by having the nodes compete to solve a mathematical puzzle. The node that solves the puzzle first is rewarded with cryptocurrency and is allowed to add the next block to the chain. The ledger is the database that stores the blockchain data. It is distributed across all nodes in the network, meaning that there is no single point of failure. This makes the blockchain very secure and resistant to attack. The wallet is a software application that allows users to store, send, and receive cryptocurrency. It stores the user's private keys, which are used to sign transactions.

Blockchain Permission-less Model

The Permission-less model operates effectively in a large participant environment, enabling users to engage without the need for identifying each other. This model is particularly well-suited for financial applications involving cryptocurrencies [2]. It ensures privacy and security through a tamper-proof system, making it challenging to alter the blockchain as it grows. For instance, in Bitcoin, transactions are pseudo-anonymous, utilizing cryptographically generated addresses associated with public keys. These addresses function similarly to bank accounts, with wallets monitoring incoming transactions encrypted with the recipient's public key. While the transaction amounts are visible for validation, the identities of the parties involved remain undisclosed. The versatility of the permission less model extends to various applications, including cryptocurrencies like Ethereum, Bitcoin, and zcash, enabling anonymous interactions between users.

Blockchain Permissioned Model

In the permissioned model, all users have access to read transaction data, but only predetermined users possess the authority to validate transactions. This permissioned approach is especially well-suited for various sectors, including the industrial domain and supply chain management for products like luxury goods, pharmaceuticals, cosmetics, and electronics, where tracking provenance is essential. Unlike public networks, private networks with limited and whitelisted users do not require resource-intensive consensus protocols like Proof of Work (PoW). Instead, more cost-effective consensus algorithms, such as Practical Byzantine Fault Tolerance (PBFT) and Tendermint, are utilized in permissioned models. For instance, Hyperledger Fabric employs PBFT as its consensus algorithm, capable of handling Byzantine attacks and managing up to one-third of the replicas [2].

The PBFT process can be divided into three phases: pre-prepared, prepared, and commit [4]. These phases contribute to the secure and efficient operation of permissioned blockchains, catering to the specific needs and characteristics of closed network environments.

Architecture of Hashgraph

The Hashgraph Consensus Mechanism represents a form of distributed ledger technology (DLT) that relies on a distinctive algorithm to achieve consensus within its network participants. By utilizing the gossip protocol and virtual voting, it ensures the swift and secure validation of transactions, all while upholding the principles of decentralization. In contrast to traditional blockchain technology, Hashgraph offers enhanced efficiency, scalability, and equitable time-stamping, primarily attributed to its Directed Acyclic Graph (DAG) structure. The Hashgraph architecture is structured as a three-tiered system:

Internet Layer: The foundation of the architecture comprises nodes that constitute the network. These nodes are interconnected via the internet and communication among themselves via the internet and communicate among themselves through a gossip protocol [4]. Hashgraph Consensus Layer: Positioned in the middle, this layer is tasked with achieving consensus on the sequence of transactions. It employs a distinctive consensus algorithm known as “gossip about gossip” to accomplish [5]. Services Layer: Positioned at the topmost level, this layer caters to network users by offering various services. These services encompass data storage, execution of smart contracts, and token issuance, among others. At a conceptual level, a hashgraph consists of columns and vertices, as illustrated in **Fig 2**. Each column represents a user within the network, while vertices represent events. Users can perform two primary actions in the hashgraph: Submit a transaction: Users can create an event containing a new transaction, represented as a red vertex in **Fig 2.**

Gossip about a transaction: Users randomly select other users to share information with them. For example, in Figure 2, user C submits an event and then gossips about it to user D. This process facilitates the widespread dissemination of information about newly submitted transactions.

Every event in the hashgraph contains four key pieces of information:

Hash 1: The hash of the previous event generated by the user receiving the gossip.

Hash 2: The hash of the previous event of the user sending the gossip.

Transaction: This includes any transactions submitted by the user sending the gossip.
Timestamps: A field used to record when the event was submitted. Importantly, even if a user attempts to manipulate the timestamps, the voting algorithm employed for consensus will detect such attempts.

Hashgraph introduces a significant concept of ordering and fairness, which enables events to be properly sequenced and validated based on their order of occurrence. In this system, events are arranged chronologically, and their validity is determined accordingly. Consequently, if two users are vying for access to certain resources, the user who submitted the transaction first will be given priority. Unlike blockchain, where the order of transactions can be reversed depending on the selection made by miners, hashgraph ensures a more predictable and consistent ordering mechanism. This feature contributes to a fair and reliable consensus process in the hashgraph distributed ledger technology.

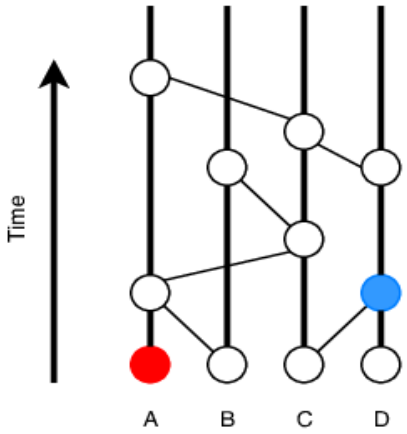

Fig 2. Hash Graph Data structure

The nodes in the hashgraph has its unique features
Hashgraph introduced the notion of fairness as a prominent new concept in the world of Distributed Ledger Technologies (DLTs). Here are the key aspects that demonstrate this fairness:
Fair Network: The timestamped consensus mechanism ensures that transactions are accurately ordered and recorded. This guarantees the correct sequence of handling transactions, leading to a fair and reliable system.
Virtual Voting: Every node in the network maintains a full copy of the hashgraph, eliminating the need for nodes to broadcast their votes across the network. Instead, they can calculate the votes of other nodes. The consensus algorithm takes into account scenarios where the network is not fully synchronized, meaning that nodes may have slightly different versions of the hashgraph.
Efficiency: Unlike blockchain, where some events may become stale or discarded, hashgraph ensures that no events suffer from such issues. This efficiency also extends to bandwidth usage, as only information about the transactions is transmitted, reducing unnecessary data transfer.
High Transaction Rate: Hashgraph is known for its fast network capabilities, mainly due to the use of the gossip protocol, which minimizes communication overhead. However, it's important to note that hashgraph has primarily been tested in private environments thus far. The introduction of these fairness principles in hashgraph has the potential to revolutionize the way consensus is achieved in distributed ledger technologies, providing a more efficient and equitable approach to transaction processing and validation.

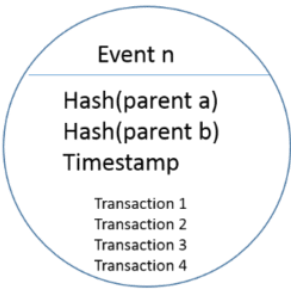

Fig 3. Nodes in Hash graph

DAG vs Blockchain

DAG, which stands for Directed Acyclic Graph, is a data structure comprising nodes connected by directed edges in a specific direction. It is characterized by a topological ordering where the sequence can only move from earlier to later points. DAG finds applications in various areas such as data processing, scheduling, navigation route optimization, and data compression.

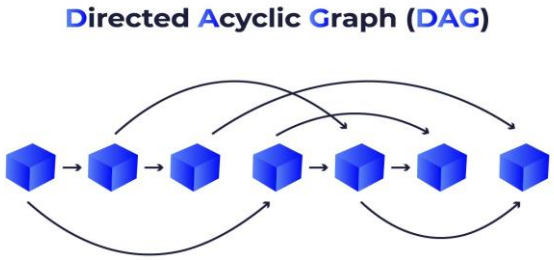

Fig 4. Directed Acyclic Graph structure

In this structure, nodes are interconnected with edges forming a web-like configuration. The edges have specific directions, allowing movement only in one direction, making the graph non-circular or acyclic. The absence of cycles ensures that the same node cannot be encountered more than once when following the edges from node to node. The key difference between DAG and traditional blockchain lies in their data structures [4]. While blockchains add blocks sequentially to a chain, DAG uses a web-like Directed Acyclic Graph. This parallelization of validation results in higher throughput. A new competitor called Byteball is offering a solution that addresses the shortcomings of Bitcoin and its blockchain, introducing new features using the Directed Acyclic Graph organizational model.

In DAG, transactions are linked from one to another, and each transaction confirms the next, eliminating the need for miners' Proof of Work required in traditional blockchains. As the term suggests, DAG's links replace the hashed blocks found in the blockchain. The sequential nature of blockchains poses challenges in their transaction throughput and scalability, leading to higher storage and bandwidth requirements as the blockchain grows. On the other hand, DAGs resemble flow charts, with all points heading in one direction, offering a more scalable and efficient structure. DAG operates on multiple layers of transactions in nodes, and every transaction must verify two other transactions, preventing unnecessary verification. This approach reduces the reliance on miners, as nodes themselves become "miners" and verify transactions for their closest neighbors. This eliminates mining fees and minimizes centralization concerns seen in traditional blockchain.

DAGs hold promise for high-functioning and low-fee chains, enabling users to send micro-payments without the heavy fees associated with Bitcoin or Ethereum. Companies like IOTA and ByteBall are at the forefront of developing DAG technology and are expected to drive its adoption in applications that require scalability in handling thousands of transactions per second, offering a potential solution to the challenges faced by traditional blockchain networks.

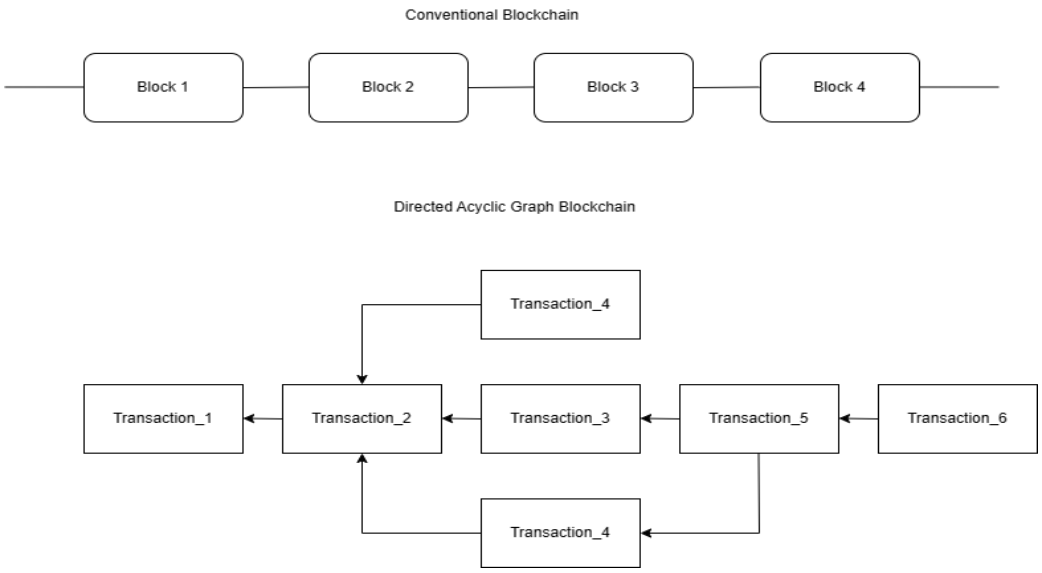

Fig 5. Blockchain vs Hashgraph

Hash Graph – Gossip Protocol

The term gossip protocol refers to a specific type of P2P (peer-to-peer) communication that takes place between computers and other digital devices. The coinage of the term was inspired by the conventional form of gossip that is common within social groups [7]. In the context of computer science, gossip protocol is related to a kind of communication that takes place when data is transmitted through different computer nodes, which are part of a distributed network. As the name suggests, a gossip protocol communication takes place when information is broadcasted from one computer to another until it is eventually spread all across the network [5]. Currently, there are numerous variants of the Gossip protocol that can be applied to different scenarios depending on the needs of the user or organization. There are two main types of Gossip manifestation: information dissemination and information aggregation [7]. These two types are key elements of large scale distributed systems. On the one hand, gossip dissemination, also known as multicast, relates to the traditional way of data distribution (one network node at a time). On the other hand, the aggregating gossip protocols are the ones that process data, i.e., that first summarize information and then distribute it (this type of gossip communication may also be referred to as distributed data mining).

An interesting example of a distributed system that uses a gossip protocol is the Hashgraph created by Leemon Baird in 2016. It is a distributed ledger technology that employs an asynchronous Byzantine Fault Tolerance (aBFT) consensus algorithm. The nodes of a Hashgraph network gather and summarize information about transactions and other events and spread this data to other neighbor nodes that are chosen randomly [6]. So instead of building a chain of blocks, the Hashgraph network builds a tree of events where all information is recorded (no data is ever discarded).

High level algorithm for gossip-based DAG

Initialization:

- Each node in the network is assigned a unique identifier.
- Each node maintains its own local view of the DAG, containing the information it possesses.
- Initially, a node starts with its own information as the source of the gossip.

Gossiping Process:

- At regular intervals (or whenever triggered), each node selects a limited number (e.g., k) of random neighbors from its local view of the DAG.
- The node then sends its local information to the selected neighbors.
- Upon receiving information from another node, a recipient node updates its local view with the new information and marks the sender as a parent node in the DAG.

DAG Formation:

- As nodes receive information and update their views, a directed acyclic graph (DAG) will gradually form.
- Each node maintains a set of parent nodes, representing nodes from which it received information.
- Duplicate Handling:
- Nodes may receive duplicate or conflicting information from different parents.
- To ensure consistency, each node can maintain a version number or timestamp for the information it holds.
- When a node receives information with a lower timestamp than what it already possesses, it discards the incoming information as it's outdated.

Termination Condition:

- The gossiping process continues until a certain termination condition is met. For example, it may continue until every node has received the information from a specific number of sources, or until the information is propagated to all nodes in the network.

Fault-Tolerance:

- The gossip-based DAG algorithm is inherently fault-tolerant since information can spread through multiple paths and nodes can recover from partial failures.

Performance Considerations:

- The choice of gossip interval, number of neighbors to gossip with (k), and the frequency of gossiping events can impact the performance and convergence speed of the algorithm.
- Adjusting these parameters might be necessary to achieve desired results depending on the network size, communication delay, and desired consistency guarantees.

III. COMPARISON

Table 1 comprises several DLTs, each presenting its own advantages and disadvantages. Both Blockchain and Sidechain share the same data structure, resulting in comparable analyses with only slight variations in scalability [9]. While Blockchain accommodates various platforms, including those discussed in section 3.1 besides Bitcoin, it is crucial to note that Hyperledger Fabric may not be a viable solution due to its restriction to private networks, thereby disallowing the incorporation of new machines into the network. This limitation poses a significant drawback within the context of the machine economy.

Table 1. Comparative study of Hashgraph and blockchain

Technical Paramater	Blockchain	Hashgraph
Consensus Algorithm	PoS, PoW and more	Virtual Voting
Scalability	Low (3-27)	High (150,000 to 250,00)
Interoperability	Medium	Low
Energy Consumption	Very High (890 kwh)	Low (7 kwh)
Efficiency	Low	High
Fees	Yes	No
Validation Time	Minutes	Seconds
Security	High	High
Platforms	Bitcoin, Etheurem, Hyperledger fabric	Hedra

Scalability: Concerning scalability and addressing the issue of the "blockchain bottleneck," several solutions stand out. DAG, Hashgraph, and Holochain offer promising approaches. DAG employs multiple attachment sites for new transactions, while Hashgraph utilizes the "gossip" protocol, leading to faster transaction validation. The Transactions per Second (TPS) rate for Hashgraph varies based on current literature, but it surpasses the rates of Blockchain, Sidechain, and DAG [10]. On the other hand, Holochain boasts the highest theoretical scalability potential, yet no practical experiments have been conducted to verify this theory.

Interoperability: In terms of interoperability, it is crucial to highlight that Blockchain, as the most mature form of DLT presently, lacks a universal standard, leading to underdeveloped interoperability for business applications. Consequently, other DLT alternatives are still in their nascent stages of defining standards for industrial usage.

Security: Security is a paramount aspect shared among all the DLTs analyzed in Table 1. Both Blockchain and SideChain boast robust security features that demand an attacker to acquire 51% or more of the total mining power to impede new data transactions, an arduous task. On the other hand, Hashgraph provides additional security measures as all participants are known beforehand, and the network restricts access to only registered participants [10], reducing the likelihood of potential attacks.

Fees: Blockchain and SideChain are likely to have high fees since they share the same data structure. On the other hand, Hashgraph and DAG do not impose fees as they do not require "mining" for validating data transactions within the network. As for Holochain, there is limited information available in the literature regarding whether it incurs fees during validation [11]. Secure medical storage data through blockchian incorporates cryptography algorithms such as two fish encryption with multiple precision technique applied in both blockchain and hashgraph shows significant difference in transaction speed. This approach also reduces the encryption time and decryption time in the blockchain network [13].

Validation Time: Validation time is indirectly related to scalability and TPS (Transactions Per Second), meaning that higher TPS rates lead to faster transaction validation. According to a study by [20], Blockchain's validation time varies from 10 minutes for Bitcoin to 0.25 minutes for Ethereum. However, DAG provides instant validation since it does not involve mining. As mentioned in section 3.3.1, Hashgraph utilizes a virtual voting protocol, where all nodes validate transactions independently, resulting in exceptionally rapid validation times [10] [11].

The **Table 2** shows the throughput of some popular blockchain and hashgraph networks:

Table 2. Throughput Blockchain Vs Hashgraph

Network	Throughput
Bitcoin	7 TPS
Ethereum	15 TPS
Hedera Hashgraph	10,000 TPS
Chia Network	1,700 TPS

IV. DISCUSSION AND CONCLUSION

When comparing Blockchain and Hashgraph in terms of throughput, Hashgraph has a clear advantage in handling a higher volume of transactions per second. Its consensus mechanism and asynchronous nature allow for faster and more efficient validation, making it well-suited for applications with demanding performance requirements. However, it is important to note that each technology has its own strengths and use cases. Blockchain still excels in decentralization, security, and immutability,

while Hashgraph's focus on scalability and throughput makes it a compelling option for certain applications. The choice between the two will depend on the specific needs and objectives of the project at hand. In conclusion, both blockchain and Hashgraph are distributed ledger technologies that offer valuable advantages for various applications. Blockchain has been at the forefront of the decentralized movement, gaining widespread recognition and adoption due to its role in powering cryptocurrencies and its potential for secure and transparent transactions in various industries. On the other hand, Hashgraph brings a unique approach to distributed consensus with its directed acyclic graph (DAG) structure, which allows for high throughput, low latency, and fast transaction processing. It addresses some of the scalability issues faced by blockchain, making it suitable for applications that require real-time transaction processing and high-performance decentralized systems. Blockchain remains a robust and widely adopted solution for many decentralized applications, while Hashgraph offers a promising alternative, particularly for scenarios where speed, scalability, and real-time performance are critical factors. As the technology landscape continues to evolve, further research and practical implementations will help to better understand and leverage the strengths of both blockchain and Hashgraph to cater to diverse and complex distributed ledger needs.

Data Availability
The Data used to support the findings of this study will be shared upon request.

Conflicts of Interests
The author(s) declare(s) that they have no conflicts of interest.

Funding
No funding was received to assist with the preparation of this manuscript.

Ethics Approval and Consent to Participate
The research has consent for Ethical Approval and Consent to participate.

Competing Interests
There are no competing interests.

References
[1] D. Dasgupta, J. M. Shrein, and K. D. Gupta, “A survey of blockchain from security perspective,” Journal of Banking and Financial Technology, vol. 3, no. 1, pp. 1–17, Jan. 2019, doi: 10.1007/s42786-018-00002-6.
[2] Dinesh Kumar, K., Komathy, K., Manoj Kumar, D.S,”Block chain technologies in financial sectors and industries,” *International Journal of Scientific and Technology Research*, 8 (11), pp. 942-946, 2019.
[3] A. Haldorai, A. Ramu, and S. Murugan, “Computing and Communication Systems in Urban Development,” Urban Computing, 2019, doi: 10.1007/978-3-030-26013-2.
[4] Alshehab, T. Alfozan, H. F. Gaderrab, M. A. Alahmad, and A. Alkandari, “Identifying significant elements of the digital transformation of organizatios in Kuwait,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 26, no. 1, p. 318, Apr. 2022, doi: 10.11591/ijeecs.v26.i1.pp318-325.
[5] K. Apt, D. Grossi, and W. Van-Der-Hoek, “When Are Two Gossips the Same?,” EPiC Series in Computing, doi: 10.29007/ww65.
[6] J. Fu, L. Zhang, L. Wang, and F. Li, “BCT: An Efficient and Fault Tolerance Blockchain Consensus Transform Mechanism for IoT,” IEEE Internet of Things Journal, vol. 10, no. 14, pp. 12055–12065, Jul. 2023, doi: 10.1109/jiot.2021.3123626.
[7] P. Schueffel, “Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph - A High-Level Overview and Comparison -,” SSRN Electronic Journal, 2017, doi: 10.2139/ssrn.3144241.
[8] V. Badhe, P. Nhavale, S. Todkar, P. Shinde, and K. Kolhar, “Digital Certificate System for Verification of Educational Certificates using Blockchain,” International Journal of Scientific Research in Science and Technology, pp. 45–50, Sep. 2020, doi: 10.32628/ijsrst20758.
[9] K. Kumutha and S. Jayalakshmi, “A Comparative Analysis of Blockchain Platform: Issues and Recommendations-Certificate Verification System,” Computational Intelligence in Data Science, pp. 210–219, 2021, doi: 10.1007/978-3-030-92600-7_20.
[10] N. Zivic, C. Ruland, and J. Sassmannshausen, “Distributed Ledger Technologies for M2M Communications,” 2019 International Conference on Information Networking (ICOIN), Jan. 2019, doi: 10.1109/icoin.2019.8718115.
[11] Z. Akhtar, “From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild,” 2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON), Nov. 2019, doi: 10.1109/upcon47278.2019.8980029.
[12] H. Pervez, M. Muneeb, M. U. Irfan, and I. U. Haq, “A Comparative Analysis of DAG-Based Blockchain Architectures,” 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), Dec. 2018, doi: 10.1109/icosst.2018.8632193.
[13] D. K. K and D. N, “Two Fish Encryption Based Blockchain Technology for Secured Data Storage,” Journal of Machine and Computing, pp. 216–226, Jul. 2023, doi: 10.53759/7669/jmc202303020.