Underlying Consensus Algorithms, Architectures and Data Structures in Distributed Ledger Technologies Applications

DOROTHY G. BUNDI[1], STEPHEN M. MUTUA[2], SIMON M. KARUME[3]
[1] *School of Science Engineering and Technology, Kabarak University, Kenya*
[2]*School of Computing and Informatics, Meru University of Science and Technology, Kenya*
[3] *School of Science Engineering and Technology, Kabarak University, Kenya*

Abstract— Distribute Ledger Technologies (DLTs) provide a distributed and decentralized environment with no central trusted control authority. DLTs removes a single point of authorization hence increasing the levels of trust of distributed records however there are still challenges in the underlying consensus algorithms, architectures and data structures in DLTs applications that need to be addressed. This paper employs exploratory research design with an objective to review various literature on different consensus algorithms, architectures and data structures applied in DLTs applications. The study revealed proof-of-work and proof-of-stake as some of the common consensus algorithms used in DLTs. The review shows that DLTs use either linear or linked, complex and hybrid data structures. Blockchain, Directed Acyclic Graph, Hashgraph, Holochain and Tempo (Radix) as the common types of DLTs. The findings also indicated that DLTs architectural design is constructed of three layers Protocol, Network, and Data. This study contributes to body of knowledge in DLTs.

Indexed Terms: Distributed Ledger Technologies (DLT), Consensus Algorithm, Architectural Layers, Data Structures

I. INTRODUCTION

Distributed ledger technology (DLT) in the recent times has emerged as a disruptive technology with a wide range of applicability in different sectors [1]. DLT is a network platform with a distributed database in which data and transactions are recorded, stored in a shared ledger that is distributed across various computer nodes termed as the network nodes, institutions, countries and accessible simultaneously by multiple people spread out in the globe [2]. DLT offers an alternative to centralized storage techniques to databases, which rely on a single server or small network. DLTs have unique features that make them suitable for application in different sectors. The unique DLTs features are decentralization, immutability, distributed, shared ledgers, fault tolerance, transparency, efficiency and use smart contracts [3] . Additionally, DLTs also offer transactions that are secure, encrypted, time-stamped, anonymous, and verifiable records for every transaction without a central repository and usually without a central authority [4], [5].

The development of distributed ledger technology (DLT) has brought about significant changes in record-keeping by moving from a single, authoritative location to a decentralized system. However, there are still challenges in the underlying data structures, architectures, topologies, and consensus mechanisms in DLTs that need to be addressed. This paper aims to explore the algorithms, architectures, and data structures used in DLTs and identify the research issues that need to be addressed to improve the efficiency, scalability, and security of DLTs.

DLTs are made up of three common components the peer to peer network which is created when two or more computers in the network establishes a connection to aid in communication and sharing of information without going through a central server [3],[6]. This component helps in improving the security of the client-server network which store data only on the server side. The Nodes which are the independent computers that record, share and

synchronize transactions in the distributed ledger network. Nodes in the distributed network are connected to each other to act as communication links and points. Nodes and master nodes are expected to verify data for security purposes and to participate in the voting events and execution of important protocol operations in the distributed ledger network. Consensus mechanisms which are the set of rules that are used to determine how DLT network will reach agreement on either changing the transactions in the ledger or not, and if the changes are valid or not. Consensus protocols ensure that nodes on distributed ledgers have valid and consistent information at all times [1], [7].

DLTs can either be public which implies that they are open to everyone to view and verify data or private which means that they restricted to a select few participants [8]. DLTs can be categorized into three categories permission, permissionless and hybrid. Permissioned DLTs implies that the network nodes have to take permission from a central authority that deals with identity verification of nodes that needs to access or make any changes in the network. Permissionless DLTs have no central authority that is used to validate the transactions across the network but the existing nodes are collectively responsible for validating the transactions. This means that several consensus mechanisms have to be used in order to validate the transactions based on predefined algorithms. Hybrid DLTs are as a result of combining the permission and permissionless DLTs [9].

Blockchain, Directed Acyclic Graph (DAG), Hashgraph, Holochain and Tempo or Radix are some of the common types of DLTs based on their architectures [10]. DLTs also apply different consensus algorithms to ensure that the network nodes reach an agreement and maintain integrity and transparency. Some of the various consensus algorithms are; Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof-of-Authority (PoA), Ripple Protocol Consensus Algorithm (RPCA), Proof-of-Activity (PoA), Proof of Capacity (PoC), Proof of Identity (PoI), Proof-of-Elapsed Time (PoET), Proof of Importance (PoI), Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), delegated Byzantine Fault Tolerance (dBFT) and Stellar Consensus Protocol (SCP) or Federated Byzantine Agreement (FBA) [11].

II. MATERIAL AND METHODS

This paper employs exploratory research design using integrative literature review with an objective to review and summarize various past and theoretical literature on different algorithms, architectures and data structures applied in DLTs. The study sort to address the following research question: RQ: Which are the common consensus algorithms, architectural layouts and data structure applied in DLT applications? The study employed an inclusion and exclusion criteria where only research on DLTs algorithms or architecture or data structures were included in the study and all the non-relevant publications were excluded. Data sources for the review included electronic databases and libraries.

III. RESULTS

Table i shows a summary of the key reviewed articles discussing the key findings and the limitations of the study.

Table i: Summary of the Findings

Author(s)	Year	Title	Discussion	Key Findings	Limitation(s)
Antal et al.	2021	Distributed Ledger Technology Review and Decentralized Applications	DLT Data structures. The three-tier conceptual architecture.	Blockchain, DAG, Hashgraph, Holochain & Tempo (Radix). Interoperability Tier, Protocol and Network Tier	High costs imposed by the mining nodes hence some tradeoffs may be made due to the core-architectural designs and properties of the existing DLTs

		Development Guidelines	Consensus Protocols	NonByzantine fault-tolerant algorithms and Byzantine fault-tolerant algorithms.	
Anthony Jnr., B.	2023	A developed distributed ledger technology architectural layer framework for decentralized governance implementation in virtual enterprise.	Architectural governance-by-design framework that	Defines the governance of DLT as a combination of architectural layers and governance of DLT dimensions. DLT enables a decentralized architecture that allows multiple actors that do not trust (or know) each other to interact securely under fixed conditions	The only IOTA tangle-based DAG was employed in this study as other DLT were not considered.
Chowdhury et al.	2019	A comparative analysis of distributed ledger technology platforms.	Blockchain DLT platforms: These platforms are usually categorized as public vs private, general purpose vs application specific	Some Blockchain DLT platforms: Bitcoin, Ethereum, Multichain, EOS, Cardano, Hyperledger Fabric, Hyperledger Sawtooth, Hyper Ledger Burrow, IOTA, Corda, Waltonchain	Other DLT platforms were not covered
Krishnamurthi, R., & Shree, T.	2021	Brief Analysis of Blockchain Algorithms and Its Challenges.	The consensus algorithms of blockchain	Proof of work (POW), proof of stake (POS), ripple protocol consensus algorithm (RPCA), delegated proof of stake (dPOS), stellar consensus protocol (SCP), and proof of importance (POI).	Other Consensus algorithms are not covered
Leonulous, R.	2020	Various types of Distributed Ledger Technology	Blockchain	Bitcoin use case	Discussed a specific use case
Natarajan et al.	2017	Distributed Ledger Technology (DLT) and Blockchain.	Comparison of DLT and Blockchain	Characteristics and features	Discussed a single DLT that is the Blockchain

Suciu et al.	2018	Comparative Analysis of Distributed Ledger Technologies	The main characteristic of distributed ledgers is that they do not have a central administration component, due to advanced algorithms and methods used for record-keeping.	Characteristics of Blockchain and Tangle technologies	Other DLTs have not been discussed
Rauchs et al.,	2018	Distributed Ledger Technology Systems: A Conceptual Framework.	DLTs architectural design is constructed into three interdependent core layers	Protocol Layer, Network Layer, and Data Layer	The conceptual framework and does not quantifying abstract aspects of DLT systems such as 'decentralization'

IV. DISCUSSION

The study revealed that DLTs utilize smart contracts which are computer programs that execute algorithms or predefined actions when certain conditions within the system are met to create a new transaction that is tracked in a distributed ledger. Computer machines or nodes on a distributed ledger network are then allowed to group those transactions and send them through the shared network in a peer-to-peer manner. Data is then in turn synchronized using the consensus algorithms or agreements among the distributed network peers so that eventually each machine has an exact copy of the data in the ledger throughout the network. Consensus is the system of ensuring that all the participating parties and nodes agree to a certain state of the system as the true system state using synchronized series of transactions without a central control or authority within the decentralized database. DLT process captures the current transaction state of the ledger and also provides a transaction language to change the state of the ledger and uses a network protocol to build consensus for the transactions to be accepted by the ledger.

The findings also indicate that the security of distributed ledger is driven by the consensus within the peer-to-peer design. This is achieved by ensuring that data is the same at all nodes on the distributed ledger network and preventing malicious actors from manipulating the data in the ledger. Security in DLTs is further enhanced by the concept that human trust is avoided by the fact that the distributed ledger network operates in an environment secured using cryptography and cryptographically secured digital signature that is verified, ordered and bundled to form a record or event in the distributed network, hence allowing secure communication between parties to ensure authenticity of the actors and immutability of the data being communicated.

The results shown that DLTs can be categorized into permissionless or open network which is similar to public network examples are Bitcoin and Ethereum framework. In permissionless networks the nodes and agents do not need to identify the participating nodes or parties. Secondly, permissioned network is a closed network where all parties involved are known and is deployed behind a firewall for local participants while using a virtual private network (VPN) to connect to outside, known participants and is a most suitable choice for companies looking to develop enterprise solutions. Lastly, Hyperledger which is an open-source projects that operate for the most part in permissioned or closed networks offering different frameworks such as Fabric, Sawtooth and Iroha, all which utilize a variety of consensus protocols. Parties involved in permissioned Hyperledger blockchains are authenticated and authorized to participate with the goal of creating enterprise grade, open source, distributed ledger frameworks and code bases that support business use cases [9].

The study revealed that there are several types of distributed ledger technologies types categorized based on their architectural data structures. Blockchain which stores transactions in form of a chain of blocks data structure in which each block is connected to the predecessor using a cryptographically secured reference. Directed acyclic graph (DAG) which stores transactions in a sequence data structure [12]. Hashgraph distributed ledger technology that uses a DAG data structure to store transactions. Holochain DLT uses a peer-to-peer network to store data and each node in the network stores only its data. Tempo (Radix) DLT uses a unique data structure known as Radix Tree to store transactions [3]

A. Types of DLTs Based on Architectural Data Structures

Blockchains is the widely used type of DLT that has it data structure configured in that it stores data and transactions in form of a chain of blocks. Each block produces a unique hash that can be used as a proof to validate transactions. Each node also has a copy of the ledger which make it more transparent [13]. Blockchain technology can either be grouped based on their architectures as public blockchains or private blockchains which is either permissioned or permissionless [14]. Both types of blockchains provide a peer-to-peer network which offers a decentralized and immutable ecosystem which are synchronized via different protocols which include use of smart contracts or consensus protocols like proof-of-work or proof-of-stake or both [15].

Directed acyclic graphs (DAG) has an architectural design that is composed of nodes and arrows between nodes. The DAG data structure organizes and orders data as a series of activities that is used to bring consensus. Each directed edge has a certain order that is in turn followed by the node. Every DAG starts with a node that has no parents and with one that has no kids. The validation of the transactions in the network requires the majority support from the most nodes. Every node in the network is expected to provide a proof of transactions on the ledger and then be in a position to initiate a transaction. This means that each node has to verify at least two of the previous transactions on the ledger in the network to form their transactions [16].

Hashgraphs is a DLT type that transactions are recorded and stored in a form of a directed acyclic graph, but it employs a different type of a consensus mechanisms that uses virtual voting with an aim of gaining network consensus. This means that the nodes in the network then do not need to validate each of the transactions in the network [17]. Holochain DLT is decentralized than blockchain. Its data structure proposed that each node to run on a chain of its own, with nodes or miners having the freedom of operating autonomously. It basically designed to use the agent-centric structure which means that agent are computers, nodes, and miners [18]. Lastly, the Tempo or Radix uses a method of making a partition of the ledger known as sharding which means that all the events that happen in the network are ordered. This implies that the transactions are added to the ledger on the basis of the order of the event than the timestamp [19]. A summary of the types of DLTs based on their architectures is shown in the Fig 1.

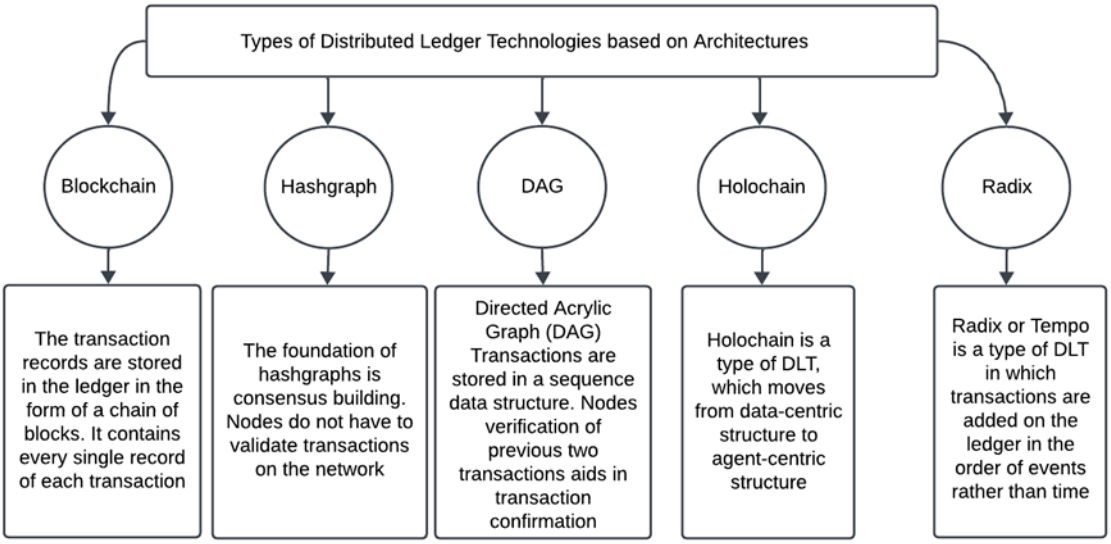

Fig 1: Types of DLTs [20]

B. Common DLTs Data structures

DLT system is based on a shared data structure or ledger that has a set of crucial features the most important of which are usually persistence, transparency, standardization and censorship resistance. Within which they have a set of information states, property rights, functions and relations defined by a DLT system protocol [13]. The distributed ledger provides an authoritative version of records at a moment in time that is both shared amongst the users of the system and updated over time as users engage with one another via the distributed ledger system. DLTs use either linear or linked, complex and hybrid data structures [9]. The Fig 2 shows some examples of the data structures used by various types of distributed ledger technologies.

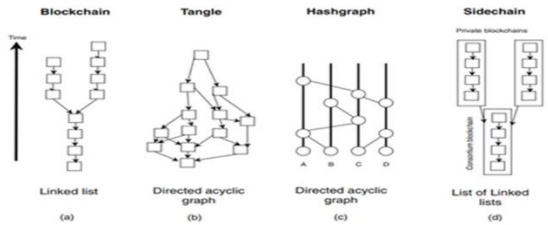

Fig 2: An Overview of the Existing DLTs Architectural Layout [13]

C. DLT Algorithms and Protocols

DLTs are implemented in various algorithms and protocols. According to Zheng and others [21] DLTs algorithms can either be consensus algorithms which implies that the DLT implements protocols that make sure all nodes (device on the distributed ledger that maintains the ledger and (sometimes) processes transactions) are synchronized with each other and agree on which transactions are legitimate and are added to the ledger. A protocol is a set of rules that govern how the distributed ledger system operates. These rules establish the basic functioning of the different parts of the system, how the nodes interact with each other, and what conditions are necessary for a robust implementation of the ledger [22].

In addition, blockchains can be implemented using smart contracts protocols. A smart contract [23] is a computer program stored on the decentralized blockchain network that executes the terms defined inside of it. The contract only runs when it is invoked to do so by an external event or if some predefined condition is met. According to [24] smart contract is also a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties.

The common consensus algorithms in DLT include Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Authority, Proof-of-Elapsed Time, Proof-of-

Importance, Proof-of-Capacity, Proof-of-Identity, Proof-of-Activity, byzantine fault tolerance, delegated proof-of-stake, delegated byzantine fault tolerance or practical byzantine fault tolerance or delegated byzantine fault tolerance (dBFT), stellar consensus protocol and ripple protocol consensus algorithm each explained in the section below.

i. Proof-of Work

According to [25] Proof-of Work (PoW) is the original consensus algorithm in a distributed ledger network. In Blockchain, this algorithm is used to confirm transactions and produce new blocks to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded.

ii. Proof-of-Stake (PoS)

The other one is Proof-of-Stake (PoS) is a consensus algorithm for blockchain networks that is based on a randomly selected state of validators who "stake" the native network tokens by locking them into the blockchain to produce and approve blocks. This concept is commonly applied in Bitcoin's transactions where its states that a person can mine or validate block transactions according to how many coins he or she holds. This means that the more Bitcoin or altcoin owned by a miner, the more mining power he or she has. (PoS) is a type of consensus algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus [26].

iii. Delegated Proof-of-Stake (dPoS)

Delegated Proof of Stake is different for Proof of Stake in its approach. dPOS is not entirely decentralized which implies that the network stakers do not have the ability to validate the blocks but they choose delegates who validate each transaction in the distributed network [27].

iv. Proof-of-Authority

Proof-of-Authority consensus algorithm is commonly used in private distributed networks since it is used entirely for the centralized systems based on reputation of trusted parties participating in the blockchain network. This implies that only the chosen and approved accounts by the system administrator are validated to be shared across the network. Validators stake their own identities and reputation instead of their resources [28].

v. Proof-of-Elapsed Time (PoET)

Proof-of-Elapsed Time (PoET) consensus algorithms is widely used for permissioned Blockchain network and it that chooses the next block using fair means. Every validator on the distributed ledger network gets a fair chance to create their own block. All nodes in the network wait for a random time and add the proof of their waiting time in the block. These created blocks are then in turn broadcasted in the network for all the other nodes to consider. The block from the winning validator node is then appended into the Blockchain. Other mechanisms are used to check, ensure, stop and regulate one node from always winning the election at all times [29].

vi. Proof-of-Importance

Proof of importance (POI) consensus algorithms uses a decision-making process for a group of nodes in a distributed ledger network where the individual participants of the group constructs and supports the decision that works best for all the members in the distributed ledger network. It models a win-win model for the network as the consensus only agrees to what will benefit the majority members by voting for what is beneficial for all participants in the network and not favoring one node [30].

vii. Proof of identity (PoI)

Proof of identity (PoI) this consensus algorithm is attached to cryptographic confirmation of authorized identity using the user's private key. This means that a block of data can be created and managed by each identified user in a network and presented to others in the distributed ledger network [31].

viii. Proof of activity (PoA)

Proof of activity (PoA) in this consensus algorithm, the miners are expected to solve the cryptographic problem as soon as possible using electric energy and hardware. But, when one comes across a given set of blocks in the network the only information known to them is about the identity and reward transaction of the winner [32].

ix. Proof-of-Capacity (PoC)

In the Proof of Capacity consensus, validators are supposed to invest their hard drive space instead of investing in expensive hardware or burning coins. The more the hard drive space validators have, the better their chances of getting selected for mining the next block and earning the block reward [33].

x. Byzantine fault tolerance (BFT) or Practical Byzantine Fault Tolerance (PBFT) or delegated byzantine fault tolerance (dBFT)

Byzantine fault tolerance or practical byzantine fault tolerance or delegated byzantine fault tolerance is a

consensus algorithm that was designed to solve problems associated with Byzantine Fault Tolerance in the distributed and blockchain environments [34].

xi. Proof of Burn (PoB)

Proof of Burn is a consensus algorithm that validators "burn" coins by sending them to an address from where they are irretrievable. When the validators burn coins it implies that they commit the coins to unreachable address hence get a privilege to mine on the system based on a random selection process. This means that the validators have a long-term commitment in exchange to their short-term loss. This consensus algorithm is applied in Bitcoin mining process. The disadvantage with this type of consensus algorithm is that it wastes resources needlessly which implies that mining power goes to those who are willing to burn more money [12]

xii. Stellar Consensus Protocol (SCP)

Stellar consensus protocol (SCP) also known as federated Byzantine agreement (FBA) is a consensus algorithm that achieves robustness through quorum slices where individual trust decisions made by each node that together determine system-level quorums. These Slices bind the blockchain system together [35].

xiii. Ripple protocol consensus algorithm (RPCA)

Ripple protocol consensus algorithm (RPCA) takes advantage of the network topology when it holds several sub-networks with poor connections between them. It is applied every few seconds by all nodes, in order to maintain the correctness and agreement of the network [36].

D. Properties of Consensus Algorithm

According Yadav, Shikha, Gupta and Kushwaha [37] there are numerous consensus algorithms used in DLTs designed as per the requirements of various applications yet they share some common design properties like:

i. Termination which implies that the whole process of getting a consensus must be ended at some point and every node or agent should decide on a single value.
ii. Cooperative which means that every node involved in consensus process must work together with other nodes in the distributed network by forfaiting all their individual interests working as a team with the aim of achieving consensus.
iii. Agreement seeking where each consensus algorithm should be designed with the aim of bringing maximum agreement from all the nodes in the network as possible.
iv. Collaborative effort where individual nodes in the distributed network should collaborate for the sake of the entire group.
v. Egalitarian in nature that implies that consensus algorithm should have equal voting value. This means that no vote should have more value or less value than the other vote in the distributed ledger network.
vi. Inclusivity which implies that the consensus algorithms should be designed with an aim of bringing many entities together as possible. This means that every entity in the distributed ledger must feel that their vote holds value in the consensus and none is less valued.
vii. Integrity must be maintained as a priority. This means that if a certain value is denoted to correct the consensus process, then the same value should be used to correct the consensus process.
viii. Participatory of every node in the distributed ledger network.

E. DLTs Architecture

Distributed ledger technologies support a decentralized architecture that allows multiple nodes, agents or actors that do not know or trust each other in the network to securely interact under defined conditions [1]. DLTs architectural design is constructed into three interdependent core layers namely Protocol, Network, and Data [38]. The protocol layer defines the set of software-defined rules that determine how the distributed ledger system operates, the network layer is the interconnected actors and processes that implement the protocol and the data layer allows information flow through the distributed ledger system that has a specific meaning in relationship to the design and functions of the system. The DLT architecture layout is shown in the Fig 3 below:

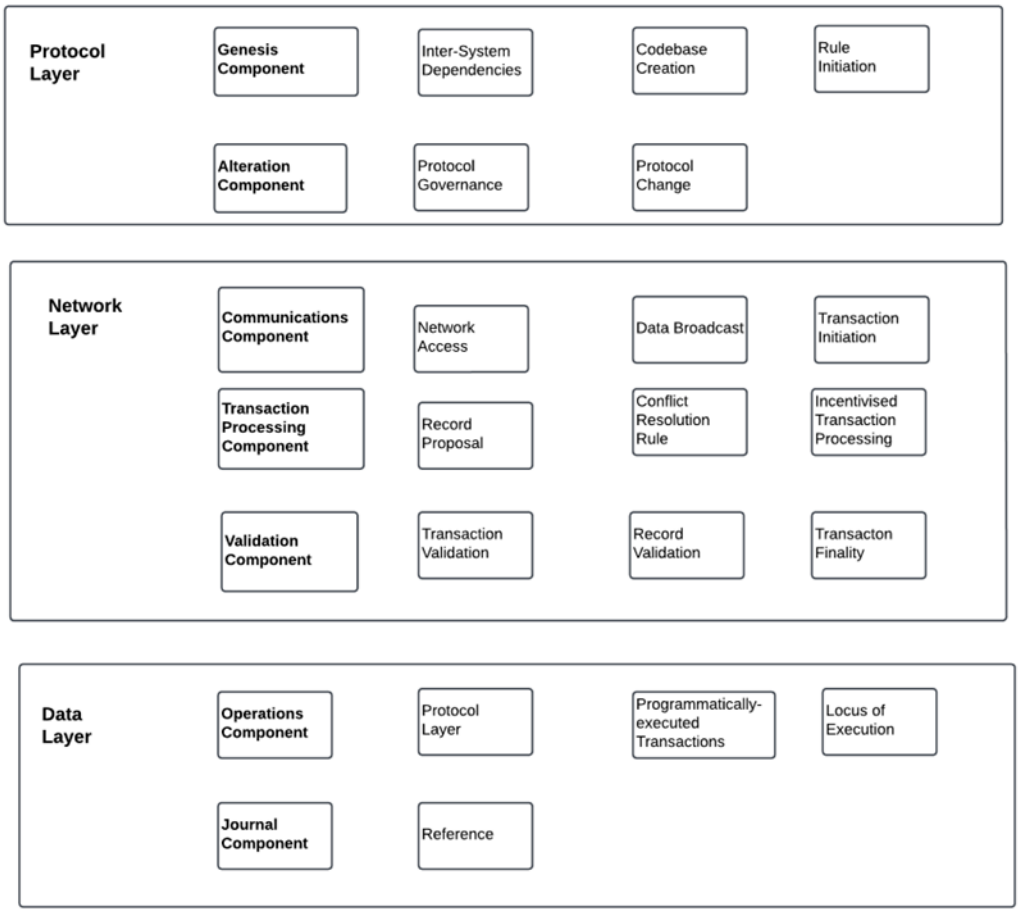

Fig 3: DLT System Architecture Anatomy [38]

F. Challenges with existing Distributed ledger Technologies architectures, algorithms and data structures

The study also revealed that there some challenges with the existing distributed ledgers architectures, algorithms and data structures. These challenges include:

i. *Scalability of distributed ledger technologies (DLTs*): As the number of transactions and participants' increases, the network can become slower and less efficient. This is particularly important for public DLTs using blockchains like Bitcoin, where the entire network needs to validate each transaction before storing and approving it [39]

ii. *Energy Consumption*: High energy consumption associated with some consensus algorithms, such as Proof of Work (PoW) . The computational power required for mining new blocks in PoW-based DLTs like blockchains can be energy-intensive and environmentally unsustainable [40].

iii. *Privacy and Confidentiality:* Maintaining privacy and confidentiality of data on a distributed ledger can be challenging. While the ledger itself may be transparent and immutable, ensuring that sensitive information is not visible to unauthorized parties can be a complex task that requires a multi-level security measures [41]

iv. *Interoperability:* Achieving interoperability between different distributed ledger technologies is a challenge [40]. As there are various types of DLTs with different architectural designs, data structures and consensus algorithms, integrating them and enabling seamless communication and data exchange can be difficult [3].

v. *Governance and Regulation:* Distributed ledger technologies often operate in a decentralized manner without a central authority or administrator. This poses challenges in terms of governance, regulation, and legal frameworks, as there may be a lack of clarity on responsibilities and accountability of the participating nodes [42].
vi. *Adoption and Integration:* The adoption and integration of distributed ledger technologies into existing systems and processes can be challenging for organizations. Implementing DLT requires changes in infrastructure, workflows, and business models, which can be disruptive and costly to these organizations [43].

CONCLUSION AND RECOMMENDATIONS

Distributed ledger technology is a technology that allows data storage in a decentralized ledger and a distributed database that allows communication between the nodes through a peer-to-peer network. DLT uses consensus mechanisms and algorithms to secure and maintain its database. Over the years DLT ecosystem has developed different consensus algorithms which most of the popular ones have been discussed in this paper. The paper summarizes the DLT architectures by showing the three architectural layers protocol, network and data and gives an overview of the common data structures used in the DLT applications. Thus, the choice of the right consensus algorithm is dependent on the DLT type and application that one intends to use. Some of the challenges with existing distributed ledger architectures, data structures, and algorithms include scalability, energy consumption, privacy and confidentiality, interoperability, governance and regulation, as well as adoption and integration. Overcoming these challenges is crucial for the widespread adoption and successful implementation of distributed ledger technologies in different sectors. For future studies the study proposes an in-depth study of specific architecture, algorithms and data structure for each on the DLTs.

ACKNOWLEDGMENT

Sincere appreciation and gratitude to the faculty members of Kabarak University and Meru University of Science and Technology for their invaluable contributions, feedback and support during the preparation of this research review paper. Their comments, expertise, guidance, and unwavering commitment have significantly enriched the quality of this research work.

REFERENCES

[1] B. Anthony Jnr., A developed distributed ledger technology architectural layer framework for decentralized governance implementation in virtual enterprise, no. 1. Springer Berlin Heidelberg, 2023. doi: 10.1007/s10257-023-00634-2.

[2] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System By Satoshi Nakamoto - Fact / Myth,” Oct. 2008, [Online]. Available: http://factmyth.com/books/bitcoin-a-peer-to-peer-electronic-cash-system-by-satoshi-nakamoto/

[3] C. Antal, T. Cioara, I. Anghel, M. Antal, and I. Salomie, “Distributed ledger technology review and decentralized applications development guidelines,” Futur. Internet, vol. 13, no. 3, p. 62, Mar. 2021, doi: 10.3390/fi13030062.

[4] G. Suciu, C. Nadrag, C. Istrate, A. Vulpe, M. C. Ditu, and O. Subea, “Comparative Analysis of Distributed Ledger Technologies,” 6th Glob. Wirel. Summit, GWS 2018, pp. 370–373, 2018, doi: 10.1109/GWS.2018.8686563.

[5] M. Hölbl et al., “A Systematic Review of the Use of Blockchain in Healthcare,” Symmetry (Basel)., vol. 10, no. 10, p. 470, 2018, doi: 10.3390/sym10100470.

[6] N. Kannengießer, S. Lins, T. Dehling, and A. Sunyaev, “Trade-offs between Distributed Ledger Technology Characteristics,” ACM Comput. Surv., vol. 53, no. 2, Jun. 2020, doi: 10.1145/3379463.

[7] M. Olsson, “A study and review of distributed ledger technologies,” no. C, 2020, [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1447100

[8] M. J. M. Chowdhury et al., “A comparative analysis of distributed ledger technology platforms,” IEEE Access, vol. 7, pp. 167930–

167943, 2019, doi: 10.1109/ACCESS.2019.2953729.

[9] H. Natarajan, S. K. Krause, and H. L. Gradstein, "Distributed Ledger Technology (DLT) and Blockchain," FinTech Note, no. 1, pp. 1–60, 2017, [Online]. Available: http://hdl.handle.net/10986/29053%0Ahttp://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf

[10] S. Manski, "Distributed Ledger Technologies, Value Accounting, and the Self Sovereign Identity," Front. Blockchain, vol. 3, no. June, pp. 1–12, 2020, doi: 10.3389/fbloc.2020.00029.

[11] C. Arslan, S. Sipahioğlu, E. Şafak, M. Gözütok, and T. Köprülü, "Comparative Analysis and Modern Applications of PoW, PoS, PPoS Blockchain Consensus Mechanisms and New Distributed Ledger Technologies," Adv. Sci. Technol. Eng. Syst. J., vol. 6, no. 5, pp. 279–290, 2021, doi: 10.25046/aj060531.

[12] G. A. F. Rebello, G. F. Camilo, L. C. B. Guimarães, L. A. C. de Souza, G. A. Thomaz, and O. C. M. B. Duarte, "A security and performance analysis of proof-based consensus protocols," Ann. des Telecommun. Telecommun., vol. 77, no. 7–8, pp. 517–537, 2022, doi: 10.1007/s12243-021-00896-2.

[13] N. El Ioini and C. Pahl, A review of distributed ledger technologies, vol. 11230 LNCS. Springer International Publishing, 2018. doi: 10.1007/978-3-030-02671-4_16.

[14] J. M. Roman-Belmonte, H. De la Corte-Rodriguez, and E. C. Rodriguez-Merchan, "How blockchain technology can change medicine," Postgraduate Medicine, vol. 130, no. 4. 2018. doi: 10.1080/00325481.2018.1472996.

[15] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.

[16] N. Zivic, E. Kadusic, and K. Kadusic, "Directed Acyclic Graph as Hashgraph: An Alternative DLT to Blockchains and Tangles," 2020 19th Int. Symp. INFOTEH-JAHORINA, INFOTEH 2020 - Proc., no. March, pp. 18–20, 2020, doi: 10.1109/INFOTEH48170.2020.9066312.

[17] J. James, D. Hawthorne, K. Duncan, A. S. Leger, J. Sagisi, and M. Collins, "An experimental framework for investigating hashgraph algorithm transaction speed," BlockSys 2019 - Proc. 2019 Work. Blockchain-Enabled Networked Sens. Syst., pp. 15–21, 2019, doi: 10.1145/3362744.3363342.

[18] S. Zaman, M. R. A. Khandaker, R. T. Khan, F. Tariq, and K.-K. Wong, "Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare," vol. XX, no. X, pp. 1–16, 2021, [Online]. Available: http://arxiv.org/abs/2103.01322

[19] F. Masood and A. R. Faridi, "An Overview of Distributed Ledger Technology and its Applications," Int. J. Comput. Sci. Eng., vol. 6, no. 10, pp. 422–427, 2018, doi: 10.26438/ijcse/v6i10.422427.

[20] R. Leonulous, "Various types of Distributed Ledger Technology | DataDrivenInvestor," 2020. https://www.datadriveninvestor.com/2020/12/04/various-types-of-distributed-ledger-technology/ (accessed May 03, 2021).

[21] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017. doi: 10.1109/BigDataCongress.2017.85.

[22] N. Z. Tomić, "A Review of Consensus Protocols in Permissioned Blockchains," J. Comput. Sci. Res., vol. 3, no. 2, pp. 19–26, 2021, doi: 10.30564/jcsr.v3i2.2921.

[23] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustain. Cities Soc., vol. 39, 2018, doi: 10.1016/j.scs.2018.02.014.

[24] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood, "EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain," IEEE Access, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2917976.

[25] A. Gervais, K. Wüst, and H. Ritzdorf, “On the Security and Performance of Proof of Work Blockchains,” 2016.

[26] W. Li, “Securing Proof-of-Stake Blockchain Protocols,” pp. 297–315, 2017, doi: 10.1007/978-3-319-67816-0.

[27] R. Krishnamurthi and T. Shree, “A Brief Analysis of Blockchain Algorithms and Its Challenges,” https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-7998-5351-0.ch002, pp. 23–39, Jan. 2021, doi: 10.4018/978-1-7998-5351-0.CH002.

[28] M. A. Manolache, S. Manolache, and N. Tapus, “Decision Making using the Blockchain Proof of Authority Consensus,” Procedia Comput. Sci., vol. 199, pp. 580–588, 2021, doi: 10.1016/j.procs.2022.01.071.

[29] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview,” Natl. Inst. Stand. Technol., no. October, pp. 1–68, 2018, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

[30] H. Siham and I. F. T. Alyaseen, “Consensus Algorithms Blockchain: A comparitive study.” International Journal on Perceptive and cognitive Computing (IJPCC), 2019.

[31] T. Krishnamohan, “Proof of identity - a blockchain consensus algorithm to create a dynamically permissioned blockchain,” Int. J. Blockchains Cryptocurrencies, vol. 3, no. 4, p. 289, 2022, doi: 10.1504/IJBC.2022.128888.

[32] R. Belfer, A. Kashtalian, A. Nicheporuk, G. Markowsky, and A. Sachenko, “Proof-of-activity consensus protocol based on a network’s active nodes,” CEUR Workshop Proc., vol. 2623, pp. 239–251, 2020.

[33] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, “Reputation based pcroof of cooperation: an efficient and scalable consensus algorithm for supply chain applications,” J. Ambient Intell. Humaniz. Comput., vol. 14, no. 6, pp. 7795–7811, 2023, doi: 10.1007/s12652-023-04592-y.

[34] K. Christodoulou, E. Iosif, A. Inglezakis, and M. Themistocleous, “Consensus crash testing: Exploring ripple’s decentralization degree in adversarial environments,” Futur. Internet, vol. 12, no. 3, Mar. 2020, doi: 10.3390/FI12030053.

[35] D. Mazi`eres and M. Mazi`eres, “The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus,” 2016.

[36] S. Facundo, D. ’ Agostino, and J. P. Timpanaro, “Ripple Protocol performance improvement: Small world theory applied to cross border payments,” pp. 143–154, 2017, [Online]. Available: http://47jaiio.sadio.org.ar/sites/default/files/ASSE-13.pdf

[37] A. S. Yadav, S. Shikha, S. Gupta, and D. S. Kushwaha, “The efficient consensus algorithm for land record management system,” IOP Conf. Ser. Mater. Sci. Eng., vol. 1022, no. 1, 2021, doi: 10.1088/1757-899X/1022/1/012090.

[38] M. Rauchs et al., “Distributed Ledger Technology Systems: A Conceptual Framework,” SSRN Electron. J., no. August, 2018, doi: 10.2139/ssrn.3230013.

[39] https://www.analysysmason.com/research/content/articles/five-dlt-challenges-rdmy0/

[40] https://www.rand.org/pubs/research_reports/RR2223.html

[41] https://en.wikipedia.org/wiki/Distributed_ledger

[42] https://ccecosystems.news/en/need-for-change-challenges-for-companies-in-using-distributed-ledger-technologies/