A Scalability Enhancement Scheme for Ethereum Blockchains: A Graph-based Decentralized Approach

Burhan Ul Islam Khan
Department of CST, Faculty of CS and IT, Universiti Malaya, Kuala Lumpur, Malaysia | Fakultas Teknik, Universitas Negeri Padang, Padang, Sumatera Barat, Indonesia
burhankhan@um.edu.my (corresponding author)

Khang Wen Goh
Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia
khangwen.goh@newinti.edu.my

Megat F. Zuhairi
Malaysian Institute of Information Technology, Universiti Kuala Lumpur, Malaysia
megatfarez@unikl.edu.my (corresponding author)

Rusnardi Rahmat Putra
Department of CE, Fakultas Teknik, Universitas Negeri Padang, Padang, Sumatera Barat, Indonesia
rusnardi.rahmat@ft.unp.ac.id

Abdul Raouf Khan
Department of Computer Sciences, King Faisal University, Al-Ahsa, Saudi Arabia
raoufkhan@kfu.edu.sa

Mesith Chaimanee
School of Engineering, Metharath University, Pathum Thani, Thailand
mesith.c@mru.ac.th

Received: 22 July 2024 | Revised: 17 August 2024 | Accepted: 22 August 2024

 DOI: https://doi.org/10.48084/etasr.8465

ABSTRACT

Amidst the rising demands for data security across expansive networks, blockchain technology is witnessing an upsurge in its adoption, particularly within Internet of Things (IoT) applications, services, and smart cities. Blockchains offer an immutable property that bolsters security and aids in the structured management of distributed ledgers. Nevertheless, ensuring scalability remains a formidable challenge, especially within decentralized Ethereum systems. Current methods often fall short of offering tangible solutions, and the scrutiny of Ethereum-based cases reveals persistent deficiencies in addressing scalability issues due to inherent system complexities, dependency on resource-intensive consensus algorithms, lack of optimized storage solutions, and challenges in ensuring synchronous transaction validation across a decentralized network. This paper proposes a foundational scheme underpinned by a unique graph-based topology and hash bindings for nodes that join the system. The proposed scheme establishes an innovative indexing mechanism for all transactions and blocks within the IoT framework, ensuring optimal node accessibility. Transaction and block replications occur over the joining nodes' graphical structure, ensuring efficient subsequent retrieval. A standout feature of the proposed scheme is its ability to enable participating nodes to forgo retaining a complete ledger, making it non-reliant on individual node capabilities. Consequently, this facilitates a broader spectrum of nodes to participate in the consensus system, irrespective of their operational prowess. This study also offers a novel empirical model for Proof-

of-Validation (PoV), which reduces computational intricacy and expedites the validation process in stark contrast to prevailing blockchain systems.

Keywords-blockchain; scalability; graph; Ethereum; immutable; consensus system; Proof-of-Validation (PoV)

I. INTRODUCTION

Blockchain technology is a distributed ledger or database system that has gained significant support, primarily due to its robust data security capabilities [1]. Beyond safeguarding sensitive transactions, blockchain can accelerate data transfers, reduce compliance costs, authenticate product origins, and streamline contract management processes [2, 3]. However, these advantages come with challenges, since traditional blockchain models face issues such as increased energy consumption, susceptibility to malicious activities, regulatory uncertainties, persistent scalability challenges, and broader adoption concerns [4-6]. Numerous studies have attempted to address these impediments, offering innovative solutions [7-10]. However, scalability, defined as a blockchain's capacity to handle increasing volumes of transactions and maximize network node efficiency, remains a critical yet often unsolvable issue, particularly in decentralized systems such as Ethereum [11]. Enhancing scalability requires a fundamental reevaluation of decentralization and security mechanisms within existing blockchain architectures [12-14]. The block size increases as the number of transactions increases, leading to a proportional increase in resource demand [15]. Continuous blockchain replication across all post-mining nodes consumes significant network resources. This becomes increasingly problematic in large-scale networks, particularly in Internet of Things (IoT) applications, where blockchain data can become unwieldy over time [16-18]. In addition to these challenges, there is the economic aspect. Transaction fees in blockchain networks can be prohibitively high, creating a disparity in transaction verification priorities [19, 20]. Users who can afford higher fees gain priority, leading to transaction backlogs for others and exacerbating the network imbalances that hinder scalability.

In response to these multifaceted issues, this paper introduces a different computational approach to enhance the scalability of decentralized blockchains with a focus on Ethereum. A graph-based mechanism is proposed that integrates a unique block and a transaction structure supported by a hash tree. This new technique incorporates a distinct graphical network layout and an efficient analytical model for Proof-of-Validation (PoV) at the consensus layer. Further innovations are also suggested, such as replication strategies at the storage layer and advanced retrieval mechanisms in the view layer, all underpinned by a refined reward/penalty system. The contribution of the current study is multifaceted, focusing on developing an innovative approach to Ethereum blockchain scalability. The proposed core is a novel graph-based method enhanced with hash bindings. This method establishes a unique network topology specific to decentralized Ethereum structures. Additionally, this approach includes security features and distinct analytical modeling. These elements work collaboratively to ensure scalable and secure operations within the IoT. Another crucial result is the introduction of an innovative proof of the validation mechanism. This mechanism utilizes an auditor node to authenticate blocks and transactions, significantly enhancing lookups' efficiency. In addition, the proposed scheme was comprehensively investigated using a simulation-based test environment. This environment was designed to rigorously benchmark the proposed design against existing Ethereum architectures.

A. Different Scalability Approaches

Most recent studies on addressing scalability performance in blockchain focuses on the following approaches:

1) Typical Scalability Enhancement Approach

According to existing practices in achieving scalable blockchain performance, two systems have evolved: one is revising the blockchain structure, and the other introducing methods outside the blockchain [21]. Blockchain scalability can be achieved by considering storage management [22], adopting a parallel multiprocessor to minimize mining latency and maximize the number of transactions per second [23], layer-2 solution [24], parallel mining architecture [25], a generic computational model for assessing blockchain [26], Byzantine tolerant methods [27], and evaluating the locality of content to minimize storage cost [28]. On the other hand, in [29], a directed acyclic graph was proposed to address the inherent scalability constraints of blockchain, supported by an accelerator based on parallel memory processing. These models demand robust computational resources to implement, which might be an obstacle in resource-constrained environments. The landscape was further enriched in [30], which proposed a cloud-centric model to decentralize Ethereum blockchain frameworks, and in [31], which focused on cross-sharding techniques for Ethereum 2.0.

2) Machine Learning-based Approaches

Machine learning algorithms can quickly study complex data patterns by implementing innovative caching strategies to improve overall system performance and adjust dynamic block size. In [32], machine learning techniques were used to study smart contract vulnerabilities via multidimensional feature assessment. In [33], Ethereum was aligned with a reinforcement learning model to optimize pricing strategies. Machine learning, with its potential to reshape conventional systems, presents a great interest but also inherent challenges. These issues include extensive resource consumption, protracted training durations, and a pronounced dependence on pre-trained datasets, which raises concerns about their adaptability in liquid decentralized ecosystems. Further schemes based on machine learning were proposed in [34-36]. In [37], deep learning with a genetic algorithm was proposed, where multiple machine-learning approaches were studied to identify malicious events on Ethereum. Such powerful models carry the risk of overfitting and may sometimes need to be revised when applied to diverse scenarios.

3) Encryption-based Approaches

Although encryption approaches cannot directly address scalability, they play a critical role in constructing a robust

foundation toward scalable blockchain performance by enhancing security, privacy, and efficiency in various ways. In addition, the emphasis on encryption methodologies, highlighted in [38-41], signals a priority to fortify security, but this often comes at the cost of increased latency.

4) Miscellaneous Approaches

A software-defined network is another unique approach to improving blockchain scalability by providing a flexible and programmable network infrastructure. The involvement of smart contracts is inevitable in blockchain, where software-defined networks can be used to orchestrate network resources to support the demand. In [42], the integration of a software-defined network with an optimized blockchain mechanism reduced malicious traffic to reduce energy and CPU consumption while minimizing operational delays. Furthermore, game theory can be used to revise blockchain scalability through various means. The phenomenon of consensus mechanisms in blockchains can be designed using game theory, considering the rational behavior of the nodes. It can also reshape the blockchain incentive allocation process, improving overall efficiency. Game theory mechanisms promise reduced storage costs and enhanced network throughput but come with challenges, especially in computational intensity [43, 44].

B. Challenges in Scalability

Given the extensive exploration in the literature, several methods have been proposed to enhance the performance of the Ethereum blockchain. However, persistent challenges remain, especially in the realm of scalability.

1) Learning-based Algorithms

Their increasing adoption in blockchains aims to identify optimal solutions. However, it has challenges such as high resource consumption, prolonged training times, reliance on training data for accuracy, and unpredictability in transaction rates over iterations, rendering Ethereum less suitable for dynamic decentralized blockchain services.

2) Computational Complexity and Scalability

Current Ethereum systems are based on unstructured overlays and lack efficient mechanisms for identifying joining nodes or accessing block content. Transaction and block lookup mechanisms are non-deterministic, hampering Ethereum's scalability.

3) Decentralization and Consistency

Many existing schemes delegate block generation to a selected set of joining nodes, compromising decentralization and affecting scalability. Inconsistencies arise when distinct joining nodes append different longer chains, leading to a significant drop in transactions per second.

4) Storage Complexity

Most strategies have joining nodes that store the entire local ledger, replicate it, and escalate memory complexity. This not only burdens storage but also impacts the view layer.

5) Sharding

Sharding, often employed for scalability, splits the system into subsets of nodes that work on a ledger. Although it mitigates storage issues, it does not address the intricacies of communication when a block or transaction is present.

II. RESEARCH PROBLEM

The immutable nature of blockchain technology makes it a secure bulwark for data, ensuring the orderly management of distributed ledgers. However, as this field burgeons, achieving scalability in decentralized systems such as Ethereum presents a complex challenge. Despite their innovation, current Ethereum strategies have revealed recurrent scalability issues. Although learning-based algorithms are promising, they struggle with extensive resource demands, prolonged training phases, reliance on preprocessed data, and variable transaction rates. Such factors render Ethereum less than ideal for dynamic blockchain operations.

Ethereum's reliance on unstructured overlays poses another challenge, particularly in accurately identifying new joining nodes and accessing block content. This inefficiency leads to non-deterministic transactions and block lookups, exacerbating scalability problems. The pursuit of decentralization makes these complexities worse. Strategies that centralize block generation in specific nodes may improve efficiency but at the cost of the fundamental decentralized principle of blockchain. This approach also hinders scalability, mainly when nodes introduce divergent chains that affect transaction rates. Moreover, the prevalent storage practice, which requires nodes to maintain a complete local ledger, intensifies memory complexity, impacting storage capacity and viewing interface. While sharding techniques attempt to address storage concerns, Ethereum needs help managing the communication challenges associated with transactions or blocks.

In summary, although extensive research in the blockchain arena has led to significant insights and advances, scalability remains a formidable challenge, particularly within Ethereum. This study aims to address these issues by introducing a graph-based decentralized architecture approach to enhance the scalability of the Ethereum blockchain. The proposed system can improve transaction rates per second, throughput, latency, resource consumption, and computational processing time.

III. MATERIALS AND METHODS

In the proposed scheme, a novel framework to ensure enhanced scalability towards the usage of Ethereum-based blockchain operations is developed. Conventionally, there are various methods to incorporate scalability in Ethereum blockchain operations, such as sharding, Proof-of-Stake (PoS), Layer-2 solutions, etc. This study employs the PoS approach, which is more energy-efficient and permits validators to create and validate new blocks. Such a transition form minimizes network resource consumption and leverages scalability. The proposed scheme was implemented over a distributed scheme using a graph of nodes indexed with three entities:

- The name of the index.
- The numerical value of the index.
- The IP address of the node.

The complete formulated graph can search and explore the address of all nodes characterized by a particular numerical index (or name of the index) based on its respective numerical value. The initiator of the search for the node is returned with the IP address of the corresponding nodes if the formulated distributed graph consists of the target index. In a different case, only the IP addresses of the nodes of the highly correlated indices are returned to the target search.

The proposed scheme assumes that the participating nodes join the formulated graph in a highly decentralized approach (Figure 1). It considers a system to be partially synchronized, which indicates that message delivery and execution speed are bound within the operational times, achieving partial synchronization of the proposed scheme. Also, it deploys a timeout method and initiates the time for the processes to identify an event of failure in the case of an asynchronous process without any bounds. The scheme uses three methods to ensure that all nodes are synchronized in the trusted environment of Ethereum:

- The primary method uses a consensus approach to agree with the blockchain state across all nodes.
- The secondary method uses peer-to-peer networking, where blocks and transactions are broadcasted to the network, and verification with validation of the nodes is performed.
- The tertiary method uses the PoS system, where validators offer incentives or penalties to follow the rules.

According to this model, Ethereum considers a block as a dedicated block, when it successfully verifies the consensus, followed by appending it to the ledger terminal. In the proposed system, a dedicated block represents a block constructed using the consensus layer toward storage. This means that the block forwards the defined verified consensus, which is added at the end of the ledger. Hence, the difference between the standard and dedicated blocks is that the system generates the former, whereas the consensus layer generates the latter.

The proposed scheme considers all prior blocks as dedicated blocks from a time perspective. The proposed mechanism determines the strength and stability of each joining node in Ethereum. The term "joining nodes" represents the participating peer nodes in the proposed graph-based network. The scheme presents a specific field consisting of the attributes of joining nodes on the path of a query, with the final node on the search path assumed to be the outcome of the search process. Using transactions, each Ethereum is registered by the joining node with a data object called strength, which can also be used to perform the updating operation for a new set of transactions. The variable α signifies the level of financial assets of the owner, representing the remittance of financial information (cryptocurrency) between two nodes during payment transactions.

The cost of generating a transaction is covered using the stability set of the joining node. Hence, a tuple is constructed, which consists of a stability set, a strength set, a prior block, and the numerical value of the index representing information about all participating joining nodes. Based on the numerical value of the index, each joining node is visualized as a connection with other nodes cumulatively represented in this tuple. The prior block represents the hashed value of the prior dedicated block, which consists of all transactions currently undertaken in Ethereum. A hash-binding method is used, in which a matrix of hash values is formed with a representation of a data structure capable of reading and writing data. This mechanism permits one-way data binding, where it is challenging to derive source information from the hashed value to offer a degree of data security. It also contains updated information regarding the strength and stability sets. The scheme also assumes the use of an authentication technique to validate the legitimacy of the formulated graph in the presence of adversaries. Adversaries are further considered to gain control over a node to some extent while consistently developing various strategies to introduce lethal attacks on the system.

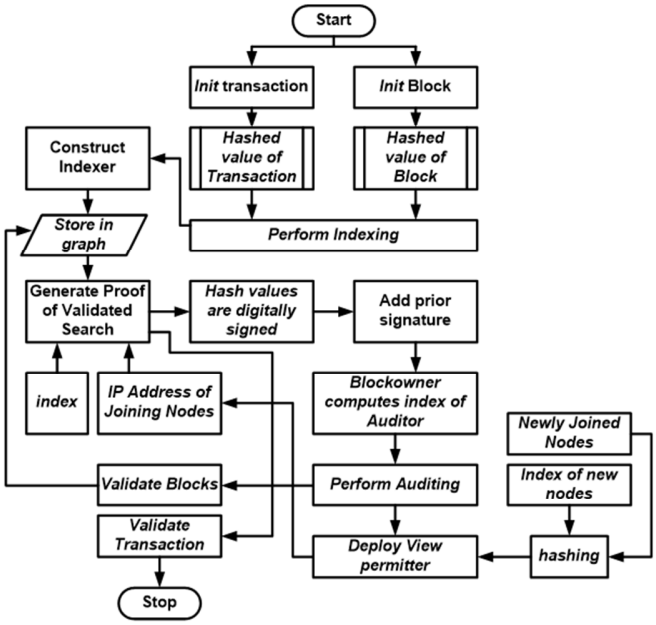

Fig. 1. The proposed method.

A. Block and Network Structure

This section discusses the novelty of the features associated with hash-binding in the proposed scheme concerning block and network structure generation. The scheme considers transaction γ in the Ethereum to be depicted by a tuple (hd, Φ, α, Pos, ht, sig). In this tuple, the first entity hd is a hash of a dedicated block in Ethereum to represent the prioritized order between all blocks and transaction γ without dependency on the synchronization clock. The priority of a block increases over transactions when indexed with hd. Variable Φ represents the identification of the owner node in the formulated graph that yields the transaction. Variable α represents the state transition of the "strength set" of the node (owner). The *Pos (*Prove-of-search) represents validated evidence of the search carried out over the joining node in the formulated graph to explore the auditor of the defined transaction. The auditor's role is to validate the block in the proposed blockchain network.

Variable *ht* represents the hashed value of transactions, which is calculated in (1) by applying the hash function over the concatenation of *hd*, Φ, *α*, *Pos*.

$$ht = hash\{hd \| \Phi \| a \| Pos\} \quad (1)$$

The final variable *sig* represents the digital signature of the auditor and the owner, considering its hash value.

In the equivalent process, block β of the proposed scheme is denoted as the tuple (*hd,* Φ, *cγ, Pos, ht, sig*). All variables are the same as previously except for *cγ* which represents cumulative transactions within a block in Ethereum. The hash value computation for block *ht* is empirically expressed by (2):

$$ht = hash\{hd \| \Phi \| c\gamma \| Pos\} \quad (2)$$

The distinction between (1) and (2) is that the former represents the hash value of the transaction, and the latter represents the block's hash value. It should be noted that the proposed scheme uses the formulated graph to define blocks, transactions, and joining nodes, leading to accountability and easy management in Ethereum. This also signifies that a formulated graph can be used to explore the presence of joining nodes and their associated transactions and blocks. The numerical value of the index and the name of the identifier of the joining nodes are considered in the hash value of a public key using a hashing function that can resist collision (Figure 2).

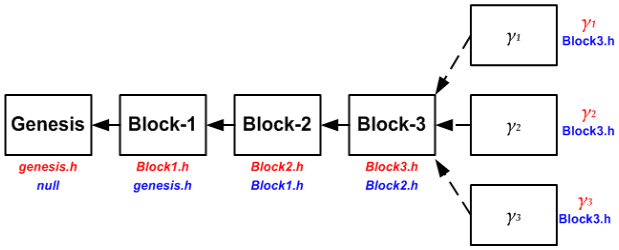

Fig. 2. Proposed architecture with hash-binding.

The malicious attempt of any intruder is resisted by enabling topology formulation using an index of nodes where a uniform localization of joining nodes is performed in the formulated graph. There are negligible chances of such index values of nodes being manipulated because indices are subjected to a hash function towards their public key with collision-resistant capabilities. This form of hash function is an arbitrary choice associated with the position of the participating nodes (or joining nodes), which restricts the decision to allocate the necessary power of an attacker to manipulate. The index's numerical value in the formulated graph is its corresponding hash value *ht,* whereas the index's name is a prior attribute *hd*. The proposed scheme generates a search for the numerical value of the index associated with the previous attribute *hd* in the formulated graph that yields a numerical value of the index, which is the hash value *ht* and the IP address of the joining node. In an equivalent process, the system can obtain the IP address of the joining node that bears the information of the consecutive block (or transaction) in Ethereum from the name of the index present in the formulated graph. This will also eventually mean that all consecutive intermediate blocks in Ethereum will possess their index name in the form of hash value *ht*. Such a characteristic ensures that the block updates the views towards the end of Ethereum by the joining nodes. This can be achieved by initiating a search towards the name of the index associated with the end block of the local Ethereum. The result of this search is a cumulative block of Ethereum added to the local network along with the currently verified transactions. An additional contribution of this scheme is that it does not require the complete Ethereum to be repositioned locally. The prior and consecutive blocks of the joining node can be retrieved using only a single-ledger block.

B. Proof of Validation

Unlike the conventional blockchain mechanism, the proposed scheme formulates a modified PoV mechanism for Ethereum, using a consensus layer to improve the scalability of the blockchain. Upon successful validation of the consensus in the PoV, the scheme verifies the block/transaction. For a transaction to be validated, it must be part of a verified block dedicated to Ethereum. PoV requires a fixed number of auditors to perform the analysis. The hash value *ht* must be digitally signed by several auditors to validate the blocks/transactions in the PoV. The operations towards PoV operations are performed in multiple steps.

1) Generation of Transactions

The task performed by the auditor is of prime importance in the PoV of the proposed system for each transaction *γ*. The empirical expression for the numerical value of the index for the i^{th} auditor in the formulated graph is given by (3).

$$\alpha ID_i = hash(\gamma.hd \| \gamma.\Phi \| \gamma.\alpha \| i) \quad (3)$$

αID_i is the auditor's index whose numerical information is searched for by the transaction owner considering the entire formulated graph. The IP address is only forwarded to the owner if the system finds the numerical value of the index for αID_i in the formulated graph. Otherwise, joining nodes with the index's most significant value of numerical information is forwarded to the owner. The formulated graph further generates proof of the validated search in either process. The proposed scheme depicts Pos_i as a variable representing validated evidence of exploration towards the numerical value of the index of a specific auditor *i* which further consists of indexers and cumulative IP addresses of the joining nodes residing over the exploration path in the formulated graph. The proposed scheme considers the i^{th} auditor the final joining node that lives in an exploration channel to the auditor node αID_i. The transactions are further appended with the evidence of a validated search by the owner of the transaction carried out for all auditors, followed by an evaluation of the hash value *ht*. The hash values *ht* are further digitally signed, and the generated value is added to the prior signature value *sig*.

Furthermore, the transaction owner seeks to verify transaction *γ* to auditors, who later assess its authenticity and correctness. The outcome of the validated transaction is confirmed by the signature received by the transaction owner on the hash file or denial from the auditor. The advantages of this transaction operation are the following.

- The proposed scheme ensures a better form of robust transaction with the condition that states that the prior value *hd* should consistently direct towards the dedicated and audited hashed block considering the ledger, where there is no presence of any form of consequent blocks with any owner's transaction.
- The proposed transaction γ is considered to offer higher precision with the condition that the verified transition state of the owner is represented by α attribute.
- The proposed transaction also ensures higher precision towards the value of hash *ht* where digital signatures are verified along with authentication *Pos* associated with all the auditors of a given transaction γ.
- The proposed transaction strategy allocates rewards to all nodes that participate in the auditing process.

The proposed system represents the transaction if the field of strength depicts an authenticated transition state associated with the owner's financial assets. Moreover, (1) is used to assess the authenticity of the hash function by cross-checking the presence of authenticated and legitimate digital signatures. However, adopting this feature requires the owner to have sufficient resources to obtain this validation service. The numerical representation of the index assigned to transaction γ is ($\gamma.ht$), and the name of the index for transaction γ is ($\gamma.hd$) which is further appended to the end of the ledger, offering more chances of being discovered.

2) Verification of Blocks

The proposed scheme considers the block's owner generated by the joining node in Ethereum. Consider γ_m as the minimum number of transactions; the block owner adds the newly generated blocks to the ledger as a new block β. Eventually, the cumulative transactions $c\gamma$ now include the new block β. The numerical value of the index associated with the specific auditor is computed by the block's owner considering the prior hash value, that is, *hd* which is now added at the end of the ledger. The system allows the PoV auditor to assess the consistency and authenticity of block β upon receiving the request to carry out validation. The auditing is expressed by

$$\alpha ID_i = hash\left(hd \parallel \Phi \parallel c\gamma \parallel i\right) \quad (4)$$

This equation highlights the auditing mechanism, which is nearly equivalent to a transaction. The prime contribution of the proposed verification scheme is that it offers a higher degree of consistency because its prior hash value *hd* is directed to the existing end of the Ethereum chain. There is also a higher possibility of inconsistency, as the current end of Ethereum could only be updated while verification was carried out for the newly generated blocks. This problem can be solved by continuously monitoring the end of the ledger's updates using an arbitrarily selected PoV auditor. Finally, the validated block β is included in the formulated graph by the owner, who is further rewarded for this act. The term reward represents a constant attribute of the proposed scheme that rewards nodes that participate in producing Ethereum blocks. The proposed scheme considers a higher reward generation value than internal validation processing to simplify the validation process.

3) Replication

To make the proposed scheme highly efficient, it must have greater availability and retrieval capabilities. To this end, the local storage unit enabled by the owner is where blocks or transactions are replicated. The system also replicates the PoV auditors, and all selected entities are forwarded to formulated graphs. By performing this selection and updating the graph, every participating joining node can carry out the process of efficient exploration of blocks and transactions. The scheme also ensures at least one trustworthy replicate for each block and transaction. Therefore, the replication process is such that the complete information of the ledger does not require access or storage. The entire access mechanism is on demand, based on each block and transaction.

4) Retrieval Technique

From an application perspective, the proposed Ethereum scheme offers an improved view of joining nodes by permitting them to join the network. The proposed scheme uses a "view permitter" for novel joining nodes arbitrarily selected for sharing Ethereum views. The numerical value of the index is computed using the novel joining nodes via the view permitter. Assuming *njn* and *nuID* are newly joined nodes and the numerical value of the index, respectively, this study considers *njn.nuID* as the numerical value of the index associated with the novel joining node. The view permitter vp_i is the index's numerical value for the i^{th} view permitter. In the graphical structure, the proposed scheme determines the numerical value of the index of vp_i by computing a validated exploration process in Ethereum. The new joining nodes are contacted based on the search outcome, and information about their view is acquired. An iterative process is permitted for the value of i to accomplish a stabilized view of the blocks. The mechanism for securing the view is defined by

$$vp_i = hash\left(njn.nuID \parallel i\right) \quad (5)$$

The i^{th} view permitter identity is generated by hashing *njn nuID* and i. Local views must be updated with new block entries to survey the updates of the cumulative joining nodes. This part of the implementation offers a direct extraction of the updated joining node state by other joining nodes without any dependency on monitoring newly joined ledger blocks. This saves sufficient computational time and contributes significantly to enhancing the scalability of its operation. This operation is performed by considering each new block represented by different numbers of graphical nodes based on unit transactions. These are termed indexers of transactions, where indexers represent the positions where the data are stored in blocks of Ethereum. In addition, the transaction block retained within the dedicated block of Ethereum is described as an indexer with $nID=\gamma.\Phi$. The block owner incorporates the transaction indexer nodes correlated with each block, followed by a replication over the auditor of the PoV block. The proposed scheme removes the indexer node from the graph, which the owner and all auditors compute using a decentralized approach. However, the proposed scheme identifies a malicious

event if a new update is received and the termination of the indexer does not follow it. It should be noted that the process of removal of the indexer is performed by the auditors of the PoV and block owners with a buffer period of certain blocks while witnessing new transactions. The proposed scheme also adopts a measure to address any possibility of network-based artifacts, such as asynchronicity. In this process, some of the addresses of blocks can be eliminated when the PoV's auditors and the block's owners record a new transaction. By undertaking this operation, PoV auditors and block owners are facilitated with buffer time to search for new updates without threat. The system assumes that the interval size of the block is constant and can be customized based on any Ethereum-based application.

5) Reward Allocation

The proposed scheme has an exclusive mechanism for allocating rewards and penalties to control the risk factors associated with the decentralized usage of Ethereum. It should be noted that the security assessment of the transaction block is performed by the PoV auditor, which is arbitrarily selected through the consensus layer. The possible actions of an attacker are authenticated through the PoV. For this purpose, the ledger gains possession of an invalid block to identify the possibility of a threat. When the proposed scheme works according to the operation stated until prior modules, it is deemed to follow a routine operation; however, a malicious operation can be noticed when the defined operations are violated. The severity of a malicious operation can be assessed by the PoV auditor, arbitrarily selected by determining the blocks or transactions that have been submitted. The scheme configures the functional attributes of Ethereum in a unique form that does not allow any malicious node to win the trust of the PoV auditor. The identification module immediately alerts to any malicious event that has not bypassed the PoV as an intruder. Each joining node can assess the legitimacy of the other joining nodes by acting as an auditor and achieving a reward if the report of a malicious event is valid. Apart from the auditor's specific task, every joining node can assess the legitimacy of the other. When an auditor identifies a positive malicious event, particular evidence of this transaction is generated by an auditor in the α field, subject to an equivalent PoV validation. The idea is to assess the validity of malicious events reported by joining the nodes. After verifying the transaction, it is positioned on a dedicated ledger block. Concurrently, the system assigns a penalty to the joining nodes if they generate malicious events. Finally, the joining nodes are blacklisted and separated from the normal joining nodes.

IV. RESULTS AND DISCUSSION

Using Python, the proposed scheme was evaluated with 2000 nodes with variable block sizes of 10-50 transactions, considering 1000 transactions for each node. Analysis was performed in a 64-bit i5 Windows environment with 16 GB of memory. The proposed scheme incorporates an amendment to conventional Ethereum by revising a unique form of block structure in a decentralized manner and hash-binding to address possible security vulnerabilities. In short, this amendment offers higher scalability and extensive decentralization without producing a novel architecture. The idea is to provide effective decision-making to facilitate all joining nodes with fair chances of participating in consensus without much dependency or affecting their stake.

A. Assessment Environment

As the proposed scheme introduces a novel Ethereum-based blockchain design, a benchmark analysis should be performed and compared with existing Ethereum-based blockchain approaches. Thus, this study considers three sets of discrete Ethereum-based blockchain operations as existing systems and selects the following approaches.

1) Enterprise Blockchain (EBC)

This method was proposed in [45], achieving the immutability characteristic of the blockchain along with decentralization. This approach models zero dependency on any intermediaries, while edge devices trade the data in IoT with third parties. Encryption is computed using Advanced Encryption Data in a cloud environment. The results showed low latency and effective resource utilization. The primary motive for selecting this model is its simplified methodology, adopted most frequently by existing schemes.

2) Extended Secure Searchable Encryption (ESSE)

This model was introduced in [46], where machine learning was adopted to offer better performance in IoT-based healthcare use cases. The model applies homomorphic encryption to secure the search within its database, whereas a trust factor is integrated with the blockchain to improve security performance. This model uses convolution neural networks and Long Short-Term Memory (LSTM) to identify threats in the blockchain. The analysis considers 100 blocks over the hyperledger fabric using Ethereum to access different information such as the cost, the number of transactions, the resources, and others, over 5000 iterations. The main reason for adopting this model is that most existing security schemes adopt deep/machine learning approaches, with promising results in terms of security and efficiency. Hence, adopting this approach for comparative analysis ensures a high degree of effectiveness assessment for the proposed approach.

3) Ethereum-based Shared Manufacturing (ESM)

This model was discussed in [47], where the concept of shared manufacturing was shown to achieve better immutability properties on the blockchain. The model discusses cross-chain transactions and can be applied to a large-scale production unit with a faster mechanism to assess smart contracts. It offers a higher scalability score over the practical environment of the consumer side chain, where Ethereum relates to the conventional side chain to accomplish the outcome. The outcome was assessed in terms of service costs and service time. The primary reason for selecting this model for comparative analysis is that the model exhibits the most simplified Ethereum implementation towards a practical manufacturing environment with effective scalability scores in its performance.

Table I highlights the differences and similarities between all the critical elements involved in the proposed and existing schemes. Although all schemes have similar agendas to address identical security problems, their methods differ significantly.

The three models for comparative analysis must be assessed initially in a discrete test environment. Therefore, minor fine-tuning was conducted as follows:

- All existing schemes were converted into Ethereum functions in the same developed environment where the proposed system is implemented.
- The sizes of the blocks, data size, transactions, etc. were homogenously considered uniform for both the proposed and existing schemes to arrive at unbiased outcomes over multiple performance metrics.
- As the use cases of all existing studies differ, existing approaches extract only the core implementation approach and discard the different use cases to arrive at a uniform decentralized blockchain implementation. The operations conducted by the proposed scheme are mainly associated with the construction and joining of a formulated graph in a hash tree, performing an initial configuration for a new node to participate in the blockchain network, the validation of blocks and transactions, and storage.

TABLE I. SCHEME DIFFERENCES AND SIMILARITIES

	Differences	Similarities
EBC [45]	**Encryption**: AES **Signature**: Elliptical Curve Digital Signature **Attack**: Cyberattacks	**Design**: Decentralization **Problem**: Data security **Focus**: Access control
ESSE [46]	**Encryption**: Homomorphic **Signature**: Attribute-based signature **Attack**: Replay attack	
ESM [47]	**Encryption**: Nil **Signature**: Identity-based signature **Attack**: Side-channel attack	
Proposed	**Encryption**: Via hashing **Signature**: Novel & simplified signature **Attack**: AI-based cyber threats	

B. Discussion

The experiment was conducted with regard to standard performance metric parameters such as transactions per second, throughput, latency, resource utilization, and processing time. The results were analyzed to assess the impact of the proposed model on the scalable performance of the Ethereum-based blockchain design. The proposed model is expected to maintain higher security strength and sustainability toward consistent transactions in an extensive IoT network.

1) Analysis of Transactions per Second

Regarding transaction performance, the proposed scheme offers improved transactions per second. Each blockchain (both proposed and existing) was allowed to be iterated for 2000 simulation rounds, where the transactions were recorded for each approach (Figure 3).

According to Figure 3, the proposed scheme offers more transaction support than ESM, because the ESM mechanism involves exploring cross-chain technology, where a frequent assessment demands the prosumer's supply and demand structure. This operation is slightly iterative, and its reliable parameters are frequently altered, thereby degrading the number of transactions when exposed to a large IoT environment. Hence, ESM is suitable for small-scale decentralization with homogeneous data management. This problem is addressed using a neural network-based approach in ESSE, where a hybrid deep-learning-based approach can offer more transactions than ESM. However, issues regarding a large stream of incoming heterogeneous data still need to be addressed, where training operations must be re-performed for predictive analysis. Hence, the ESSE scheme is suitable for small-to-medium-scale decentralized blockchain applications with fewer chances of significant data fluctuations. Moreover, the mechanism discussed in EBC is one of the most simplified architectures of Ethereum and uses a conventional encryption method.

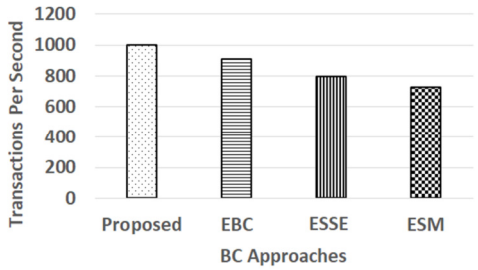

Fig. 3. Comparative analysis of transactions per second.

In addition, advanced encryption protocols offer more hardware acceleration, which is suitable for meeting large-scale security demands in IoT. This mechanism suits medium-scale decentralized blockchain operations, where the core system can govern the upper and lower time-window limits. However, the pitfall of this approach is that its vital management mechanism still needs to be executed on centralized logic by the manager node, which is finalized during data transfer.

On the other hand, the proposed scheme introduces an entirely novel scheme of decentralized Ethereum graph topology, unlike any of the above-mentioned existing schemes, offering more importance on indexing the name and numerical value of the blocks. A closer look at the empirical expression of the proposed scheme shows that a similar evaluation of the verification of blocks and transactions is used with a slight change in its input argument, which makes the process work relatively fast and reliable. This results in less dependency while verifying the hashed block and transaction data, supporting a more significant number of transactions in each unit of time. Most of the execution involved is based on assessing the conditional logic, which reduces the computational effort and ensures a faster validation period to process the maximum number of blocks. In addition, the hash data update mechanism is instantaneous and memory efficient, supporting the following stream of incoming data in the IoT. Hence, the proposed scheme offers highly scalable performance towards a large data stream without sophisticated operation.

2) Throughput Analysis

The proposed scheme considers the use case of an IoT, where the throughput is computed for participating IoT nodes that use the proposed Ethereum operation. The idea is to explore the impact of newly incorporated features in Ethereum on data transmission performance in IoT.

Figure 4 illustrates that the proposed scheme offers significantly better throughput than EBC, ESSE, and ESM. The reason for such throughput scores is as follows: ESM claimed to provide higher transaction throughput in its environment, where decentralization entirely depends upon cross-chain technology. However, when exposed to the proposed assessment environment, significant data are omitted from the record-off-chain, where the sharding principle is used for scalability. Unfortunately, the validation is highly time-consuming, and more computational effort is required, as it still needs to be feasible to support individual shards in interacting, resulting in potential declination toward throughput.

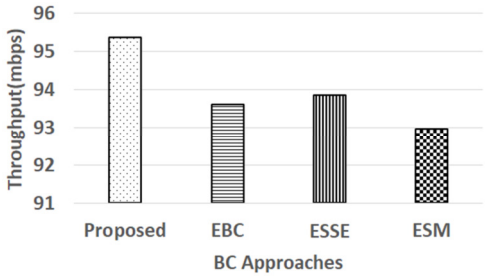

Fig. 4. Comparative analysis of throughput.

ESSE uses LSTM along with CNN to better diagnose faults in predefined attack models. However, when subjected to the proposed environment, learning models perform well in intrusion identification if they are well-defined during training. When analyzed with arbitrary attack values, the training time shows a slight improvement. More resources and operational blocks are involved in validation, resulting in a slightly increased throughput compared to ESM. EBC is a simplified architecture that is operationally found to sustain medium classes of a network but not higher classes. This is the main reason why EBC performed suboptimally compared to ESSE. However, the proposed scheme delivers improved throughput. This is due to the decentralized block management and the transmission of blocks for validation. The proposed scheme considers the transaction minimum to be incorporated within a block during the initial rounds, which enables scalability based on the formulated graph.

Further allocation of rewards/penalties ensures proper operation of block management in a decentralized manner, which significantly ensures the contribution of all parameters to accomplish a common objective of scalability by improving the graphical structure for maximum coverage. Hence, the throughput continues to increase, even under peak traffic conditions. Additionally, the involvement of PoV auditors assists in effectively replicating blocks that render better search operations with faster retrieval techniques. Another justification for the better throughput in the proposed scheme is its independence from monitoring the trace of novel ledger blocks, enabling each joining node to retrieve the updated information of another joining node of equivalent interest. Hence, better data transmission performance is ensured.

3) Analysis of Latency

Latency is another performance metric that indicates better scalability performance in the proposed scheme. It is computed by assessing the duration between the transaction submission and the conformance of the IoT network considered. The scalability of the blockchain is significantly affected by latency. The optimal latency performance is a direct indication of superior scalability in a decentralized blockchain implementation environment. Figure 5 shows that the proposed scheme offers significantly reduced latency compared to conventional blockchain techniques. The proposed scheme comprises a more significant number of conditional checks and a smaller number of computations using hashing and validation. This significantly reduces its latency.

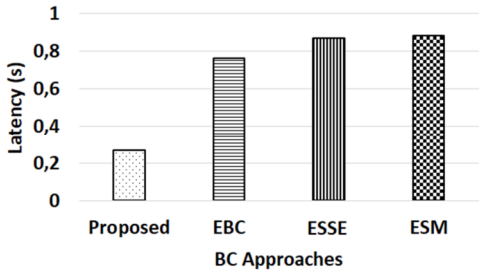

Fig. 5. Comparative analysis of latency.

4) Analysis of Resource Consumption

Resources such as energy and bandwidth consumption were considered. As the scheme was evaluated in a large IoT environment, it is evident that resource consumption gradually increases with increasing transactions. However, optimal scalable performance will always maintain a higher consumption score within a tentative limit. Figure 6 shows that the proposed scheme offers a reduced consumption of resources compared to existing schemes. ESM manages global and local blockchain information split under four different layer-based operations. The local operation is performed for the physical, cyber, and decision layers, whereas the global operation is performed for the service layer. Therefore, it increases the dependency of computational resources to interact with each layer, whereas negotiation operations between operators and consumers have more validations under a unique discovery contract. Although this offers significant security, it is associated with substantial computational costs. ESSE encounters a similar problem, where most of the iterative training operations consume more resources.

Further adoption of homomorphic encryption in EBC requires a dedicated backup of the client-server application, which linearly increases dependency on resources. In contrast, the proposed scheme introduces a formulated graph that generates indexers without dependence on calling the data into any intermediate validation task. This significantly reduces the dependency on energy, memory, and bandwidth consumption.

The proposed scheme ensures reduced energy consumption due to the adoption of fewer iterations. The proposed scheme ensures lower bandwidth consumption using transaction indexers and distributed hashing. Reduced memory consumption is achieved by splitting blocks based on the number of nodes, whereas existing shardless schemes only consider blocks. Eventually, the proposed scheme ensures the accessibility of transactions and blocks with a higher probability at any specific time.

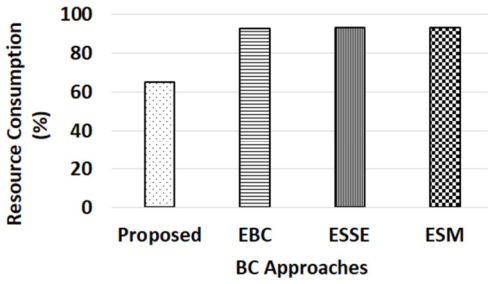

Fig. 6. Comparative analysis of resource consumption.

5) Analysis of Processing Time

Processing time refers to the overall time required for the proposed blockchain operation to be completed. Observations were performed for 500 iterations and averaged. The lower the processing time is, the higher the supportability towards scalable performance.

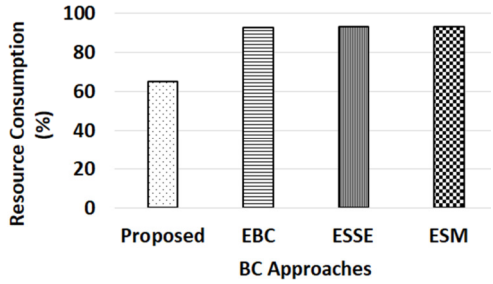

Fig. 7. Comparative analysis of resource consumption.

Figure 7 shows that the proposed scheme offers significantly reduced processing time compared to existing blockchain operations. Due to the adoption of a unique topology in the graph, faster update, faster validation process, and reduced iterative operation, the proposed scheme offers a shorter processing time, potentially assisting in achieving better scalability performance. It should be noted that the designed environment for assessment was run in a simulation-based model, where the churn trace of Ethereum was considered for each node with an anticipated duration of 3 hours to generate the first round of transactional details. Furthermore, it was simulated over a variable size of nodes and joining nodes, where an extensive simulation was carried out to understand the outcomes. The proposed scheme was evaluated from the security perspective of service, data availability, integrity, and privacy. The data integrity and privacy of the proposed model represent a visualization of the joining node from the perspective of the ledger nodes that are not altered. It is dedicated only to new blocks associated with the authenticated number of transactions to the existing end of the ledger node, based on authentication by the auditor of the PoV module. Hence, no node other than the validator or authorized joining node is allowed to perform validation checks. The availability of the dedicated block was ensured to be always accessible. The proposed system assesses the availability of services in the form of consensus availability. Service availability represents all the regular nodes that execute their operation according to the protocols defined in the proposed Ethereum design in the presence of an honest auditor node of the PoV. This is done to authenticate the genuity of the blocks and transactions.

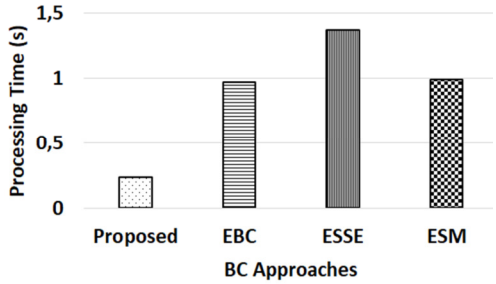

Fig. 8. Comparative analysis of processing time.

Based on the previously stated results, the proposed model offers higher data privacy and integrity preservation, even when an adversary's power to disrupt the system is exponentially increased. It should be noted that if a similar adversarial power is implicated in conventional Ethereum or Bitcoin models, the blocks and transactions are entirely compromised in terms of data integrity. This is evidence that the modified PoV model controlled by an auditor is a significant novel contribution toward enhanced data security, which is absent in the conventional blockchain architecture. The proposed PoV model is more capable than the validation operation performed by traditional hashing in the hyper ledger.

The deployment environment was also assessed on a large IoT environment with a distributed cloud system over millions of transactions for thousands of nodes and 50,000 blocks. It should be noted that the proposed scheme offers only 15 MB of storage overhead for each participating node to manage the blocks and transactions and retain the security strength of the proposed Ethereum design. Hence, greater storage space optimization is obtained by adopting the proposed scheme, in contrast to the conventional architecture of a centralized or decentralized blockchain. The storage overhead recorded for the traditional scheme is approximately 8 GB for each node evaluated in a similar test environment. The proposed scheme was evaluated for various functional operations during the configuration and validation stages. The duration of the data retrieval was approximately 370 ms in the proposed assessment environment. It was confirmed to be approximately 320 times faster when configuring a new participating node than conventional blockchain operation, which consumes approximately 4-5 hours of run time.

V. CONCLUSION

With its transformative potential to ensure data security and structured ledger management, blockchain technology faces a quintessential challenge to scalability, especially within Ethereum-based decentralized systems. This study mitigates this problem by proposing a graph-based decentralized mechanism specific to the Ethereum blockchain, which integrates the concepts of graph topology, a modified Proof-of-Validation (PoV) model, and memory utilization techniques. Such a combination creates a unique scheme that can overcome the limitations of existing models. This was evidenced by the benchmarked results achieved in terms of throughput, latency, resource consumption, and processing time. Furthermore, the strategic liberation of nodes from maintaining a complete ledger not only streamlines storage but also bolsters the system's adaptability to the dynamic demands of the IoT. The balanced approach ensures that no node, regardless of its hashing capacity, faces undue burdens and preserves the decentralized essence of blockchain while enhancing scalability. Although the proposed model exhibits significant strides in scalability enhancement, future research directions should involve deeper investigation into refining the authentication techniques, exploring adaptive algorithms to further optimize the graph topology in real time, and devising advanced security protocols to counter evolving adversarial strategies. The ternary scope of future work will include trust-based policies as an additional supplement to significantly strengthen hashing. Further studies can be conducted to optimize blockchain operations for streaming services.

ACKNOWLEDGMENT

This research was supported by the INTI IU Research Seeding Grant Phase 1/2023 initiative under Project Number INTI-FDSIT-02-01-2023.

REFERENCES

[1] A. K. Al Hwaitat *et al.*, "A New Blockchain-Based Authentication Framework for Secure IoT Networks," *Electronics*, vol. 12, no. 17, Jan. 2023, Art. no. 3618, https://doi.org/10.3390/electronics12173618.

[2] D. Xu, Y. Gao, and X. Xiao, "Precision Poverty Alleviation Methods in the Agricultural Field Based upon Wireless Communication Networks and Blockchain," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, 2022, Art. no. 2687445, https://doi.org/10.1155/2022/2687445.

[3] R. F. Olanrewaju, B. U. I. Khan, M. L. M. Kiah, N. A. Abdullah, and K. W. Goh, "Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT," *Electronics*, vol. 11, no. 23, Jan. 2022, Art. no. 3982, https://doi.org/10.3390/electronics11233982.

[4] F. Anwar, B. Khan, M. Kiah, N. Abdullah, and K. W. Goh, "A Comprehensive Insight into Blockchain Technology: Past Development, Present Impact and Future Considerations," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 11, pp. 878–907, Nov. 2022, https://doi.org/10.14569/IJACSA.2022.01311101.

[5] S. S. Taher, S. Y. Ameen, and J. A. Ahmed, "Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12822–12830, Feb. 2024, https://doi.org/10.48084/etasr.6641.

[6] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[7] B. U. I. Khan, K. W. Goh, M. S. Mir, N. F. L. Mohd Rosely, A. A. Mir, and M. Chaimanee, "Blockchain-Enhanced Sensor-as-a-Service (SEaaS) in IoT: Leveraging Blockchain for Efficient and Secure Sensing Data Transactions," *Information*, vol. 15, no. 4, Apr. 2024, Art. no. 212, https://doi.org/10.3390/info15040212.

[8] T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, Jan. 2018, https://doi.org/10.1109/ACCESS.2018.2842685.

[9] S. Rouhani and R. Deters, "Security, Performance, and Applications of Smart Contracts: A Systematic Survey," *IEEE Access*, vol. 7, pp. 50759–50779, Jan. 2019, https://doi.org/10.1109/ACCESS.2019.2911031.

[10] K. Godewatte Arachchige, P. Branch, and J. But, "Evaluation of Blockchain Networks' Scalability Limitations in Low-Powered Internet of Things (IoT) Sensor Networks," *Future Internet*, vol. 15, no. 9, Sep. 2023, Art. no. 317, https://doi.org/10.3390/fi15090317.

[11] N. Hossein Motlagh, T. Taleb, and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 899–922, Sep. 2016, https://doi.org/10.1109/JIOT.2016.2612119.

[12] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "BlockChain Technology: Beyond Bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–19, Jun. 2016.

[13] M. Y. Khan, M. F. Zuhairi, T. Ali, T. Alghamdi, and J. A. Marmolejo-Saucedo, "An extended access control model for permissioned blockchain frameworks," *Wireless Networks*, vol. 26, no. 7, pp. 4943–4954, Oct. 2020, https://doi.org/10.1007/s11276-019-01968-x.

[14] Md. R. Amin, M. F. Zuhairi, and M. N. Saadat, "Transparent Data Dealing: Hyperledger Fabric Based Biomedical Engineering Supply Chain," in *15th International Conference on Ubiquitous Information Management and Communication*, Seoul, Korea (South), Jan. 2021, pp. 1–5, https://doi.org/10.1109/IMCOM51814.2021.9377418.

[15] S. Tanwar, "Decentralization and Architecture of Blockchain Technology," in *Blockchain Technology: From Theory to Practice*, S. Tanwar, Ed. New York, NY, USA: Springer, 2022, pp. 63–81.

[16] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "The Energy Consumption of Blockchain Technology: Beyond Myth," *Business & Information Systems Engineering*, vol. 62, no. 6, pp. 599–608, Dec. 2020, https://doi.org/10.1007/s12599-020-00656-x.

[17] K. Tsantikidou and N. Sklavos, "Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare," *Cryptography*, vol. 6, no. 3, Sep. 2022, Art. no. 45, https://doi.org/10.3390/cryptography6030045.

[18] R. Longo, C. Mascia, A. Meneghetti, G. Santilli, and G. Tognolini, "Adaptable Cryptographic Primitives in Blockchains via Smart Contracts," *Cryptography*, vol. 6, no. 3, Sep. 2022, Art. no. 32, https://doi.org/10.3390/cryptography6030032.

[19] O. L. Mokalusi, R. B. Kuriakose, and H. J. Vermaak, "A Comparison of Transaction Fees for Various Data Types and Data Sizes of Blockchain Smart Contracts on a Selection of Blockchain Platforms," in *ICT Systems and Sustainability*, M. Tuba, S. Akashe, and A. Joshi, Eds. New York, NY, USA: Springer, 2023, pp. 709–718.

[20] A. Laurent, L. Brotcorne, and B. Fortz, "Transaction fees optimization in the Ethereum blockchain," *Blockchain: Research and Applications*, vol. 3, no. 3, Sep. 2022, Art. no. 100074, https://doi.org/10.1016/j.bcra.2022.100074.

[21] A. Hafid, A. S. Hafid, and M. Samih, "Scaling Blockchains: A Comprehensive Survey," *IEEE Access*, vol. 8, pp. 125244–125262, Jan. 2020, https://doi.org/10.1109/ACCESS.2020.3007251.

[22] F. Gong, L. Kong, Y. Lu, J. Qian, and X. Min, "An Overview of Blockchain Scalability for Storage," in *26th International Conference on Computer Supported Cooperative Work in Design*, Rio de Janeiro, Brazil, Dec. 2023, pp. 516–521, https://doi.org/10.1109/CSCWD57460.2023.10152720.

[23] K. K. C. Martinez, "Blockchain Scalability Solved via Quintessential Parallel Multiprocessor," in *International Wireless Communications and Mobile Computing*, Marrakesh, Morocco, Jun. 2023, pp. 1626–1631, https://doi.org/10.1109/IWCMC58020.2023.10183268.

[24] S. Shirodkar, K. Kulkarni, R. Khanjode, S. Kohle, P. Deshmukh, and P. Patil, "Layer 2 Solutions to Improve the Scalability of Blockchain," in *5th International Conference on Advances in Science and Technology*, Mumbai, India, Dec. 2022, pp. 54–57, https://doi.org/10.1109/ICAST55766.2022.10039486.

[25] J. A. DeNio and S. A. Ludwig, "Improving Transaction Speed and Scalability in Blockchain Systems," in *IEEE International Conference on Big Data*, Orlando, FL, USA, Dec. 2021, pp. 3619–3628, https://doi.org/10.1109/BigData52589.2021.9671648.

[26] B. Nasrulin, M. De Vos, G. Ishmaev, and J. Pouwelse, "Gromit: Benchmarking the Performance and Scalability of Blockchain Systems," in *International Conference on Decentralized Applications and Infrastructures*, Newark, CA, USA, Aug. 2022, pp. 56–63, https://doi.org/10.1109/DAPPS55202.2022.00015.

[27] M. Capretto, M. Ceresa, A. F. Anta, A. Russo, and C. Sanchez, "Setchain: Improving Blockchain Scalability with Byzantine Distributed Sets and Barriers," in *International Conference on Blockchain*, Espoo, Finland, Aug. 2022, pp. 87–96, https://doi.org/10.1109/Blockchain55522.2022.00022.

[28] J. Liu, S. Wan, and X. He, "Alias-Chain: Improving Blockchain Scalability via Exploring Content Locality among Transactions," in *International Parallel and Distributed Processing Symposium*, Lyon, France, Jun. 2022, pp. 1228–1238, https://doi.org/10.1109/IPDPS53621.2022.00122.

[29] Q. Wang *et al.*, "A Highly Parallelized PIM-Based Accelerator for Transaction-Based Blockchain in IoT Environment," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4072–4083, Feb. 2020, https://doi.org/10.1109/JIOT.2019.2963245.

[30] B. Kaynak, S. Kaynak, and O. Uygun, "Cloud Manufacturing Architecture Based on Public Blockchain Technology," *IEEE Access*, vol. 8, pp. 2163–2177, Jan. 2020, https://doi.org/10.1109/ACCESS.2019.2962232.

[31] A. Kudzin, K. Toyoda, S. Takayama, and A. Ishigame, "Scaling Ethereum 2.0s Cross-Shard Transactions with Refined Data Structures," *Cryptography*, vol. 6, no. 4, Dec. 2022, Art. no. 57, https://doi.org/10.3390/cryptography6040057.

[32] Q. Zhou, K. Zheng, K. Zhang, L. Hou, and X. Wang, "Vulnerability Analysis of Smart Contract for Blockchain-Based IoT Applications: A Machine Learning Approach," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 24695–24707, Dec. 2022, https://doi.org/10.1109/JIOT.2022.3196269.

[33] A. Kumari and S. Tanwar, "A Reinforcement-Learning-Based Secure Demand Response Scheme for Smart Grid System," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2180–2191, Feb. 2022, https://doi.org/10.1109/JIOT.2021.3090305.

[34] T. Ashfaq *et al.*, "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism," *Sensors*, vol. 22, no. 19, Jan. 2022, Art. no. 7162, https://doi.org/10.3390/s22197162.

[35] M. A. Ammer and T. H. H. Aldhyani, "Deep Learning Algorithm to Predict Cryptocurrency Fluctuation Prices: Increasing Investment Awareness," *Electronics*, vol. 11, no. 15, Jan. 2022, Art. no. 2349, https://doi.org/10.3390/electronics11152349.

[36] S. Aladhadh, H. Alwabli, T. Moulahi, and M. Al Asqah, "BChainGuard: A New Framework for Cyberthreats Detection in Blockchain Using Machine Learning," *Applied Sciences*, vol. 12, no. 23, Jan. 2022, Art. no. 12026, https://doi.org/10.3390/app122312026.

[37] R. M. Aziz, R. Mahto, K. Goel, A. Das, P. Kumar, and A. Saxena, "Modified Genetic Algorithm with Deep Learning for Fraud Transactions of Ethereum Smart Contract," *Applied Sciences*, vol. 13, no. 2, Jan. 2023, Art. no. 697, https://doi.org/10.3390/app13020697.

[38] A. S. Rajawat, S. B. Goyal, P. Bedi, S. Simoff, T. Jan, and M. Prasad, "Smart Scalable ML-Blockchain Framework for Large-Scale Clinical Information Sharing," *Applied Sciences*, vol. 12, no. 21, Jan. 2022, Art. no. 10795, https://doi.org/10.3390/app122110795.

[39] A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, and A. Takacs, "Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network," *Sensors*, vol. 20, no. 10, Jan. 2020, Art. no. 2798, https://doi.org/10.3390/s20102798.

[40] N. Khan, H. Aljoaey, M. Tabassum, A. Farzamnia, T. Sharma, and Y. H. Tung, "Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum," *Electronics*, vol. 11, no. 22, Jan. 2022, Art. no. 3686, https://doi.org/10.3390/electronics11223686.

[41] S. Aslam, A. Tosic, and M. Mrissa, "Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions," *Journal of Cybersecurity and Privacy*, vol. 1, no. 1, pp. 164–194, Mar. 2021, https://doi.org/10.3390/jcp1010009.

[42] M. A. A. Ghamdi, "An Optimized and Secure Energy-Efficient Blockchain-Based Framework in IoT," *IEEE Access*, vol. 10, pp. 133682–133697, Jan. 2022, https://doi.org/10.1109/ACCESS.2022.3230985.

[43] X. Li, Q. Liu, S. Wu, Z. Cao, and Q. Bai, "Game theory based compatible incentive mechanism design for non-cryptocurrency blockchain systems," *Journal of Industrial Information Integration*, vol. 31, Feb. 2023, Art. no. 100426, https://doi.org/10.1016/j.jii.2022.100426.

[44] S. Surekha and Md. Z. U. Rahman, "Blockchain Framework for Cognitive Sensor Network Using Non-Cooperative Game Theory," *IEEE Access*, vol. 10, pp. 60114–60127, Jan. 2022, https://doi.org/10.1109/ACCESS.2022.3180336.

[45] A. Nawaz *et al.*, "Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain," *Sensors*, vol. 20, no. 14, Jan. 2020, Art. no. 3965, https://doi.org/10.3390/s20143965.

[46] A. Ali *et al.*, "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network," *Sensors*, vol. 22, no. 2, Jan. 2022, Art. no. 572, https://doi.org/10.3390/s22020572.

[47] N. Rozman, J. Diaci, and M. Corn, "Scalable framework for blockchain-based shared manufacturing," *Robotics and Computer-Integrated Manufacturing*, vol. 71, Oct. 2021, Art. no. 102139, https://doi.org/10.1016/j.rcim.2021.102139.