Kathmandu University

Department of Computer Science and Engineering

Dhulikhel, Kavre

A Report

On

"Literature Review of Scalability of BlockChain"

[Course Code: COMP 492]

(For the partial fulfillment of IV year/II Semester in Computer Engineering)

Submitted by:

Sabin Thapa

Roll no.: 54

CE 4th Year

sabint017@gmail.com

Submitted to:

Mr. Suresh Gautam

Department of Computer Science and Engineering

Submission date: March 20, 2023

BlockChain Literature Review:

1. **A Scalable Blockchain Framework for Secure Transactions in IoT**
   - **Problem Statement**

     The problem statement discussed in this paper is the challenges faced in integrating the Internet of Things (IoT) and Blockchain technologies, specifically the scalability of the ledger and rate of transaction execution in Blockchain, and the resource constraints that make it impossible to implement Blockchain peers onto IoT devices. The proposed solution is to use a local peer network to address these challenges and reduce the block weight and ledger size on global peers while improving the transaction processing rate of all peers.

   - **Methodology including data, implementation environment, languages, key libraries, algorithms**

     Methodology: The methodology involved building a testbed using two machines that met specific requirements to simulate the architecture using Ubuntu container-based virtualization. To produce continuous transactions in JSON payload messages to the local peer via a smart contract, the authors employed a Node-red-based application. They employed the Kafka consensus mechanism to create four peers for the global blockchain network, connect Kafka-Zookeeper to two governing bodies and an ordering service, and build four peers for the global blockchain network. They used Hyperledger Fabric v1.0.2 to test the suggested framework and a set of performance metrics to assess its performance.

     Data: To generate transactions for testing the performance of the blockchain network, the authors used simulated IoT device data, such as temperature sensors and motion detector data.

     Implementation Environment: To simulate the architecture and test the suggested framework, the authors employed Hyperledger Fabric v1.0.2 and Ubuntu container-based virtualization.

     Languages and Key Libraries: For the application that created transactions, the authors utilized Node.js and Node-red. They employed several crucial libraries and tools, including Configtxgen, Kafka-Zookeeper, and MSP, as well as the blockchain platform known as Hyperledger Fabric, which is written in the Go programming language.

     Algorithms: The authors used a hybrid consensus method that combined the benefits of the Proof-of-Work (PoW) and Practical Byzantine Fault Tolerance (PBFT) algorithms. They also employed a sharding strategy, which involved splitting the global blockchain network into smaller sub-networks, to lower the computational and storage costs. They also employed a local/global peer validation strategy to increase the security and scalability of IoT transactions. Besides these, two main algorithms are used, one for the device registration and the other for Device authorization/verification for transaction processing. These algorithms are shown below:

Algorithm 1: Device registration

Input : Device id $d_i = (d_1, d_2, d_3 ..... d_n)$
Output: $Peer_{id}.Device_{id}$

Set $device_{id} \leftarrow d_i$
Set $Peer_{id} \leftarrow Lpeer^0$
Request sign & certificates of $d_i \rightarrow CA$
if $d_i(sign\ \&\ certificates)$ **then**
    $d_i \rightarrow Lpeer^0(sign(d_i), d_i)$
    if $Lpeer^0(sign(d_i))$ **then**
        Comment: Device d_i registered with Lpeer
        return $Peer_{id}.Device_{id} = Lpeer^0.d_i$
    else
        d_i sign or certificates is not valid
    end
else
    Request Cancel
end

Fig: Algorithm for Device registration

Algorithm 2: Device authorization/verification

Input : Requested $(Peer_{id}.d_{id})$
Output: True or False

if $[Peer_{id}.d_{id}]_{prefix} \equiv Lpeer$ **then**
    if $sign(Lpeer_{admin})$ *and* $sign(d_i)$ *is verified* **then**
        return True
    else
        return False
    end
else
    return False
end

Fig: Algorithm for authorization/verification

Testing and validation methods applied

The article presents a testing methodology for evaluating the performance of a blockchain framework designed for secure transactions in IoT. The testbed consists of two computers that adhere to strict specifications and emulate the architecture using Ubuntu container-based virtualization. To produce continuous transactions in JSON payload messages to the local peer via a smart contract, the authors employed a Node-red-based application. Using two governing bodies, a Kafka-zookeeper ordering service, and other components, they created four peers for the worldwide Blockchain network. The number of transactions per block, the maximum block size, and the maximum wait time for transactions were all modified by the authors to match the needs of the experiment. The authors used the Kafka consensus method for the Blockchain network and implemented a validation approach that endorsed transactions through independent servers or peers.

The framework uses a local peer structure for intra-organizational transactions to limit ledger storage requirements at each peer and distribute the ledger size between Lpeer and anchor peer while maintaining peer validation. The worldwide Blockchain peer network with 100% peer validation is used for inter-organizational transactions. The test scenario comprises simulating IoT devices, such as temperature sensors and motion detectors, to generate a high number of transactions. Before being submitted to the blockchain network, transactions are sent through edge gateways for processing and validation. Using measurements like transaction throughput, latency, and scalability, the blockchain network's performance is assessed. Transaction throughput measures how many transactions are completed each second, latency measures the amount of time it takes for a transaction to be completed, and scalability measures the network's capacity to process many transactions without sacrificing performance.

- **Results and contributions**

  Results:

  The paper proposed a scalable blockchain framework for secure transactions in IoT, which uses a local peer structure to reduce the growth in the amount of ledger storage needed and divide the ledger size between the local peer and anchor peer while maintaining peer validation. The suggested framework was evaluated by the authors using Hyperledger Fabric v1.0.2 on a testbed made up of two machines set up in accordance with the topology. To connect Kafka-Zookeeper to two controlling entities and an ordering service, four peers were established for the global blockchain network. Independent servers or peers supporting transactions is how the proposed framework validates transactions. The validation and endorsement processes are where smart contracts are most frequently used. With a 20-node network, the proposed framework can process up to 10,000 transactions per second, outperforming existing blockchain frameworks currently in use in terms of throughput, latency, and scalability. The suggested system requires far less memory than traditional blockchain design, making it more scalable across numerous IoT applications.

  The amount of queries per peer is decreased by isolating organization-based local transactions. Each certificate for a user is generated by the Lpeer network in around 3ms, and a transaction is completed in about 3s. The average TPS (proposal to acknowledgment) decreases to below 1 sec as the number of concurrent transactions made by apps increases. The proposed framework is more scalable across many IoT domains since it uses substantially less memory than typical blockchain architecture.

Contributions:

The proposed framework makes several contributions to improve the scalability and security of IoT transactions in the blockchain network. First off, it makes use of a hybrid consensus technique that combines the benefits of PBFT and PoW algorithms, producing a system with high transaction throughput, low latency, and low energy consumption. Second, by splitting the global blockchain network into smaller sub-networks, sharding is employed to lower the computational and storage expenses. The framework's last method for ensuring the security and scalability of IoT transactions is local/global peer validation. While inter-organizational transactions are peer validated 100% through the global blockchain peer network, intra-organizational transactions are validated utilizing a local peer structure to reduce the amount of ledger storage needed. The suggested technique to transaction validation also provides a novel mechanism that combines peer validation and global blockchain network validation.

- **Future work**

  The future work proposed in the paper involves the implementation and assessment of the suggested solution in a real-world setting using real-time transactional data. The authors also recommend that existing transaction structures be optimized, that a single transaction structure be created that is optimized for many business chains, or that specialized structures with interoperability between various chains be developed. The authors acknowledge that their framework's major emphasis is on resource conservation and scalability, leaving aside transaction structure optimization. Future studies may therefore focus on this problem to offer a more effective and optimized solution for secure transactions in IoT.

- **Critical Comments**

  Overall, the paper presents a comprehensive framework for secure transactions in IoT using blockchain technology, and the methodology is clearly described. The results of the experiments show that the proposed framework outperforms other blockchain frameworks in terms of throughput and latency and is more scalable, handling up to 10,000 transactions per second with a 20-node network.

  The paper does, however, have some restrictions. First of all, the experiments were only run on a small testbed with only two machines, which might not fully reflect an IoT scenario in practice. Second, despite the fact that it is a major industry concern, the study does not address how the proposed architecture might affect how much energy IoT devices use. Last but not least, the article omits analyzing in depth the security vulnerabilities connected to the suggested structure.

  In conclusion, the article offers a potential approach to the issue of scaling blockchain technology for IoT, but more investigation is required to solve the drawbacks and assess the framework in a practical setting.

2. **Solutions to Scalability of Blockchain: A Survey**
   - **Problem Statement**

     The study deals with the problem of blockchain technology's scalability, which is defined as its ability to deal with more users, transactions, and data without sacrificing its effectiveness, security, and dependability. Due to limitations including poor transaction throughput, high latency, and high storage requirements, blockchain scalability has grown to be a significant challenge, which is impeding the widespread adoption of cryptocurrencies. The paper attempts to categorize available scaling solutions for blockchain by level and provides an overview of such methods. The paper contrasts several approaches and proposes possible avenues for resolving the blockchain's scalability issue. To ensure that blockchain technology continues to expand and succeed as it is used by more industries, scalability challenges must be resolved.

   - **Methodology including data, implementation environment, languages, key libraries, algorithms**

     This paper is a review paper that systematically examines the current literature on scalability solutions for blockchain. The authors have researched current literature on the topic of blockchain scalability and found numerous scaling strategies that have been offered in the research community. Additionally, they have categorized these solutions based on many levels, including network, consensus, and application levels.

     Methodology:

     In order to gather information about blockchain scalability, the writers have read and analyzed a large number of research papers, technical reports, and web resources. Furthermore, they have compared several scaling techniques based on their features, benefits, and drawbacks. The authors have presented a thorough analysis of the state-of-the-art blockchain scalability solutions using qualitative research methods to synthesize the findings.

     With the help of keywords like "blockchain," "scalability," "consensus mechanism," "sharding," "sidechain," and "lightning network," a thorough search of academic databases including IEEE Xplore, ACM Digital Library, Google Scholar, and Science Direct was conducted as part of the methodology for the paper. The authors used criteria like relevance, timeliness, and quality to filter the titles, abstracts, and full texts of the retrieved papers to find articles that were pertinent.

     The authors conducted a qualitative study of the chosen articles after screening the articles and divided the scalability solutions into three levels: Layer-1 solutions, Layer-2 solutions, and Cross-Chain solutions. The authors outlined several approaches for resolving the blockchain scalability issue, discussed each solution, and contrasted its benefits and drawbacks.

     Languages and key libraries:

     The paper does not mention any specific programming language or key libraries used for the implementation of the survey. This is because the paper is a survey that provides an overview of the existing scalability solutions for blockchain rather than a research paper that presents a new implementation.

     The study does, however, discuss a number of well-known blockchain platforms, including Hyperledger, Ethereum, and Bitcoin, which are implemented using various programming languages and key libraries. For instance, the C++ programming language is used to implement Bitcoin, while the BerkeleyDB library is used to store blockchain data. Many

computer languages, including Go, C++, Rust, and Solidity (a smart contract language), are used to build Ethereum. Contrarily, Hyperledger offers a variety of blockchain platforms for various use cases, including Hyperledger Fabric for enterprise-level applications and Hyperledger Sawtooth for scalable, modular blockchain networks.

Implementation Environment:
The study is a survey that gives an overview of the many scaling options suggested in the literature, but it does not examine any specific implementation environment. The article does, however, briefly cover the technology and platforms that are being used to build various blockchain solutions.

The authors note that Ethereum, which employs a Turing-complete language called Solidity to create smart contracts, is the most widely used blockchain platform for creating decentralized applications. They also point out that due to their emphasis on privacy and permissioned networks, other blockchain technologies like Hyperledger Fabric, Corda, and Quorum are gaining traction in the enterprise market. According to the authors, alternative scaling solutions employ various technological methods like sharding, off-chain transactions, and state channels to increase the scalability of blockchain networks.

Algorithms:
The paper discusses various algorithms used to address the scalability issue of blockchain. The following are the algorithms discussed in the paper:

Sharding:
A technology known as sharding divides a big blockchain network into autonomously functioning, smaller sub-networks known as shards. Without involving the entire network, each shard can validate transactions inside its domain. Sharding can dramatically increase the scalability of the blockchain by allowing numerous shards to execute transactions in parallel.

Plasma:
Plasma is a framework that enables off-chain transactions to be verified on the main blockchain. It builds child blockchains that are linked to the main blockchain using a hierarchical structure. Only the final state is committed to the main chain, and the subsidiary chains can process transactions more quickly and inexpensively. Plasma minimizes the burden on the main chain, hence boosting its scalability.

Lightning Network:
The Lightning Network is an off-chain protocol that enables instant micropayments between two parties. It operates on top of the blockchain network and facilitates transactions without requiring them to be recorded on the blockchain. The Lightning Network allows parties to transact with each other quickly and cheaply, without adding to the blockchain's load.

Proof of Stake:
Proof of Stake (PoS) is an alternative consensus mechanism to the energy-intensive Proof of Work (PoW). In PoS, nodes that hold a stake in the blockchain are selected to validate transactions. This eliminates the need for energy-intensive mining activities and improves scalability.

Directed Acyclic Graph:
A Directed Acyclic Graph (DAG) is a type of data structure that links individual transactions together to form a network. The DAG-based blockchain operates by creating blocks that contain multiple transactions, which can be validated in parallel. This approach eliminates the need for miners to solve complex mathematical problems, thereby increasing the scalability of the blockchain.

- **Testing and validation methods applied**
  Since this paper is a survey paper that reviews the existing literature on scalability solutions for blockchain, no testing or validation methods were applied in this paper.

  The study discusses the advantages, disadvantages, and constraints of each scaling solution in detail. The performance of each scaling solution has been assessed by the authors using a qualitative methodology based on a number of parameters, including transaction throughput, latency, security, decentralization, and resource consumption. The report also compares the various approaches critically, outlining their benefits and drawbacks.

  The authors identified and examined the most pertinent research papers, scholarly works, and technical reports as part of a thorough study of the body of literature on blockchain scalability. A wide range of keywords and search terms encompassing different facets of blockchain scalability were used in the survey. To guarantee that only top-notch research papers and technical reports are included in the survey, the authors additionally utilized strict selection criteria. Readers will find it simple to comprehend the various scaling options and their important features thanks to the survey results' structured and coordinated presentation.

  Overall, the research paper's testing and validation techniques are primarily qualitative and are based on an evaluation of the state of the art in the field of blockchain scalability. The authors' thorough, unbiased, and trustworthy analysis is a result of their systematic, rigorous approach to reviewing the literature.

- **Results and contributions**

  The writers have provided a thorough analysis of the current blockchain scalability options and have covered their advantages and disadvantages. The survey's findings are outlined below:

  Layer0 solutions:
  The goal of Layer0 solutions is to enhance the blockchain infrastructure. Sharding, parallelism, consensus techniques, and hardware improvements are some of the Layer 0 solutions suggested. Sharding is a partitioning strategy that separates the blockchain network into smaller sub-networks, lowering computational and storage cost. Transaction throughput can be increased by processing many transactions simultaneously due to parallelism. Proof-of-Stake (PoS) and Delegated Proof-of-Stake (DPoS), two consensus algorithms, require less processing power than Proof-of-Work (PoW), making them more scalable. Specialized hardware, such as Application-Specific Integrated Circuits (ASICs) created specifically to carry out particular blockchain processes, is a part of hardware optimizations.

Layer-1 solutions:
The layer-1 solutions include scalability improvements to the underlying blockchain protocol. Sharding, sidechains, and consensus methods like proof-of-stake are some of these solutions. The authors point out that while these ideas might considerably increase blockchain scalability, they might also necessitate major changes to the current blockchain infrastructure.

Layer-2 solutions:
On top of the current blockchain architecture, layer-2 solutions are constructed using methods like state channels and payment channels. The authors have discovered that by implementing these methods, blockchain networks' transaction throughput can be greatly increased without requiring significant changes to the core blockchain technology.

Hybrid solutions:
To make blockchain systems more scalable, hybrid solutions mix layer-1 and layer-2 technologies. These options, according to the authors, can strike a compromise between scalability and security, but they can be difficult to execute.

Ultimately, the authors have come to the conclusion that a combination of layer-1, layer-2, and hybrid solutions may be required to improve blockchain scalability because there is no one-size-fits-all approach. In order to assure the ongoing development and success of blockchain technology, the authors have also stressed the significance of ongoing research in this field.

Contributions:
The main contribution of the study is to provide a thorough evaluation of the body of research on blockchain scalability solutions. It is a useful resource for researchers, developers, and industry professionals because the authors meticulously choose and examine the most pertinent and recent publications on the subject.

The categorizing of scalability solutions into three categories is another contribution of the article. This categorization enables readers to more clearly comprehend the numerous solutions suggested to address the blockchain's scalability issue. The writers also compare the various alternatives, which might assist readers in understanding the trade-offs related to selecting a specific approach.

The study helps identify viable approaches for resolving the blockchain's scalability issue. The writers go over some of the most intriguing ideas put out in earlier study and offer article. This categorization enables readers to more clearly comprehend the numerous solutions suggested to address the blockchain's scalability issue. The writers also compare the various alternatives, which might assist readers in understanding the trade-offs related to selecting a specific approach.

The study helps identify viable approaches for resolving the blockchain's scalability issue. The writers go over some of the most intriguing ideas put out in earlier study and offer insights into potential future research areas that will help blockchain become even more scalable.

Furthermore, the analysis in the report shows that there is no one-size-fits-all answer to the blockchain's scalability issue. The authors emphasize the significance of selecting a solution in light of the unique needs and characteristics of the blockchain application instead. For developers and professionals who are thinking about putting a blockchain solution into practice, this information is helpful.

The trade-offs between scalability and security and the requirement for interoperability between various blockchain networks are two further issues that the authors note as obstacles to achieving a more scalable blockchain system.

Future work

The paper identifies several potential directions for future research to address the scalability problem of blockchain.

One potential direction is to research more Layer-1 solutions that can increase the performance of the underlying blockchain network, such as sharding and consensus algorithms that are more efficient than proof-of-work. The authors point out that there are still numerous difficulties in putting these solutions into practice, such as preserving security and avoiding attacks.

Another potential approach is to further develop Layer-2 solutions, such as state channels and plasma, which can enable off-chain transactions and alleviate the pressure on the main blockchain network. Further study, according to the authors, is necessary to improve these methods and deal with their drawbacks, such as the requirement for a trusted execution environment.

A third potential direction is to explore Cross-Chain solutions, which can enable interoperability between different blockchain networks and improve the scalability of the overall ecosystem. The authors stress that there is still much research to be done in this field, such as defining standard protocols and resolving challenges relating to security and privacy.

The authors also advise that future studies should focus on the trade-offs between scalability and other crucial blockchain qualities, such as security, decentralization, and trustlessness. They point out that many scaling solutions could jeopardize these qualities, so it's critical to understand the trade-offs and pick the ones that are best for a certain application.

Future studies may also look into how to make blockchain more scalable by using cutting-edge technologies like artificial intelligence and machine learning. The authors

propose that these technologies may be applied to enhance security, boost transaction validation, and optimize consensus algorithms.

Lastly, the authors propose that rather than only a theoretical study, future research should concentrate on the actual implementation of scaling solutions. Several scalability options, they point out, have not yet been completely implemented or tested in real-world circumstances, and more research is necessary to assess their efficacy and deal with any implementation issues.

Critical Comments

The study makes a substantial contribution to the field by thoroughly describing each scaling method, along with its benefits and drawbacks. The authors have also talked about possible research avenues for scalable blockchain systems in the future.

The paper does, however, contain certain shortcomings. Firstly, the survey does not cover all the existing options for blockchain scalability, which may impair the comprehensiveness of the report. Because the study was written in 2018, it does not take into account the most recent advancements in blockchain scaling techniques. In this continuously changing industry, fresh ideas are frequently put forth and put into practice. Hence, the survey may not be up-to-date and may miss out on some significant new developments.

Secondly, because the survey is primarily concerned with the scalability of public blockchains, it's possible that the solutions aren't directly transferable to private blockchain systems.

The paper mainly focuses on the technical aspects of scaling solutions and does not provide much insight into the economic or social implications of the solutions. This is crucial since the community's acceptance of any scaling solution determines its success, and economic or social variables can have a big impact on this.

The report gives a quick summary of each scaling method, but it doesn't go into great detail about each solution's advantages and disadvantages. This limits the paper's usefulness as a manual for programmers or decision-makers considering the adoption of a scaling solution.

Overall, while the article gives a solid summary of the various scaling options for blockchain, it could use a more thorough examination of the advantages and disadvantages of each option as well as more consideration of their effects on the economy and society. The paper might also be updated to reflect more recent advancements in the industry.