BLOCKCHAIN TECHNOLOGY

PRESENTED BY
SABIN THAPA
ROLL NO. 54
CE IV/II

Scalability of BlockChain

A PRESENTATION ON THE LITERATURE REVIEW OF THE PAPERS

A Scalable Blockchain Framework for Secure Transactions in IoT by Biswas et. al.

&

Solutions to Scalability of Blockchain: A survey by ZHOU et. al.

MARCH 17, 2023

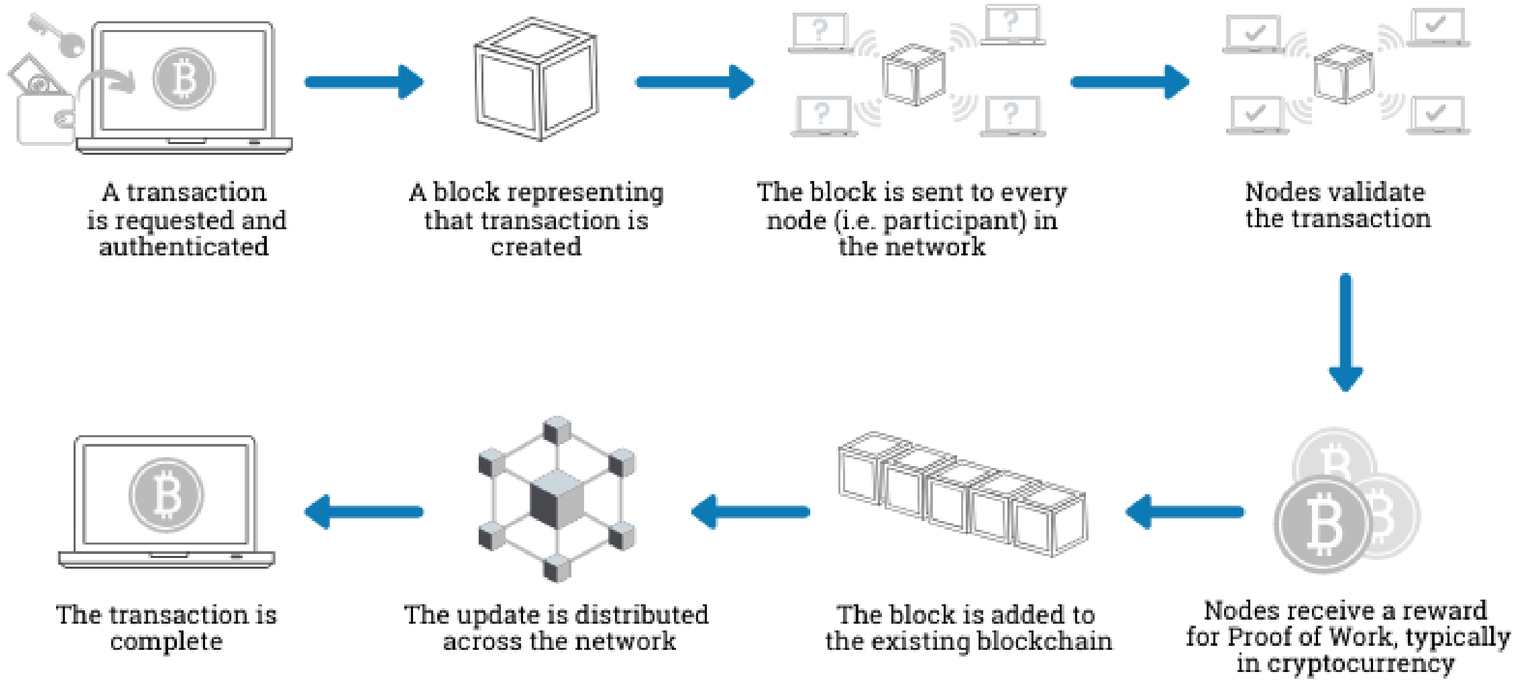
BLOCKCHAIN INTRODUCTION

- A decentralized, distributed and public digital **ledger**
- Used to record transactions across many computers
- Secure and tamper-resistant

Note: A ledger is a digital or physical log that records transactions associated with a financial system

So, how does a transaction take place in a BlockChain?

How does a transaction get into the blockchain?



BLOCKCHAIN SCALABILITY

- Ability to handle increasing amounts of data and transactions **without compromising its performance or security.**

- As #users and #transactions on a blockchain network ⬆ , the system should still be able to operate efficiently and securely.

- Typically measured by the number of transactions that can be processed by the network per second

So, why is Scalability a problem in BlockChain?

Introducing BlockChain Trilemma

BLOCKCHAIN TRILEMMA

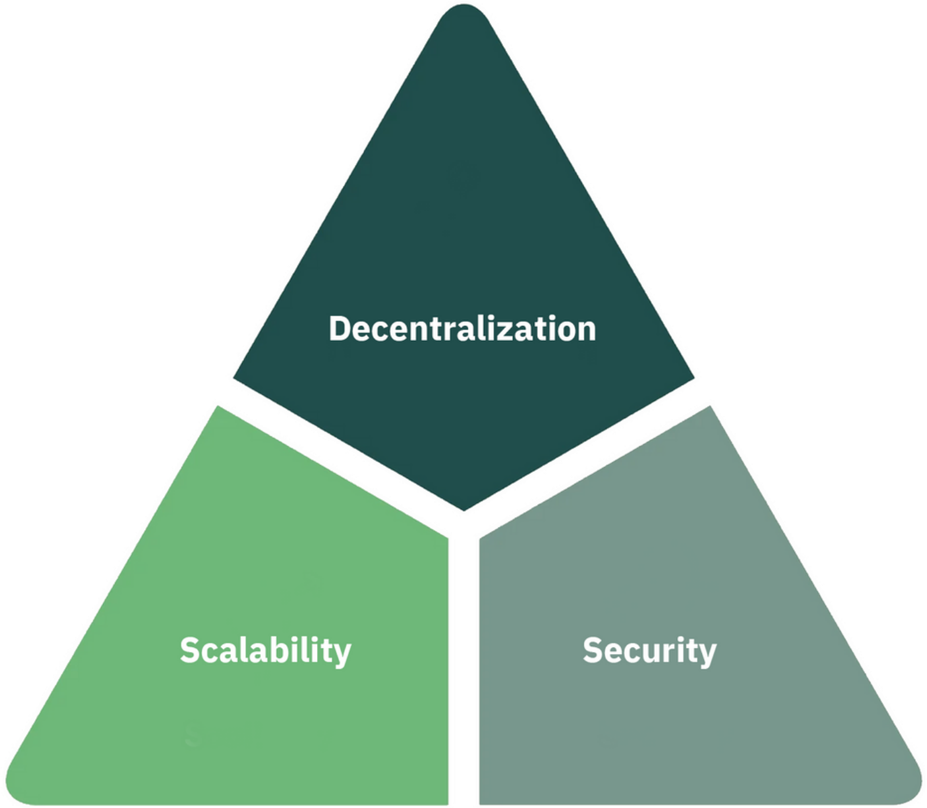
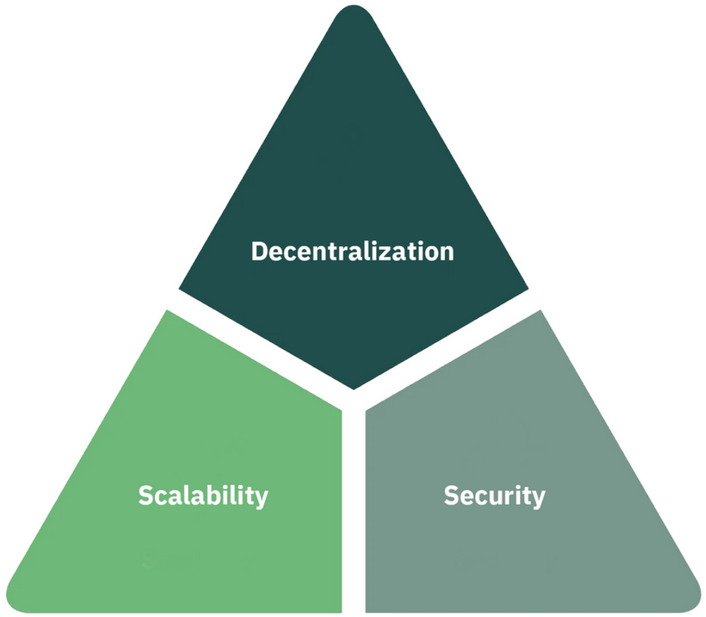


Figure: Three key aspects of a BC application

BLOCKCHAIN TRILEMMA



The trilemma arises from the fact that improving one aspect of the blockchain often comes at the expense of one or both of the other two aspects. For example:

- Increasing **scalability** may require sacrificing some level of security or decentralization.
- Increasing **security** may require sacrificing some level of scalability or decentralization.
- Increasing **decentralization** may require sacrificing some level of scalability or security.

Note: A careful balance of these three competing priorities is required in order to create a blockchain that is secure, decentralized and scalable.

BLOCKCHAIN TRILEMMA

BITCOIN suffers from BlockChain Trilemma!

- Bitcoin has been designed to prioritize security and decentralization over scalability
- Highly secure and decentralized.
- BUT can process a limited number of transactions per second.

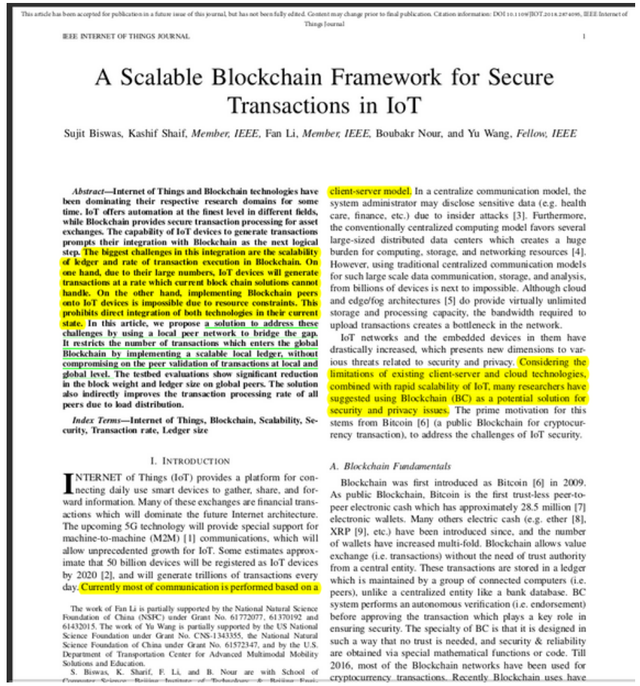
Note: BlockChain Trilemma remains an ongoing challenge for the development of blockchain technology.

BLOCKCHAIN TECHNOLOGY

THE ARTICLES

- **A Scalable Blockchain Framework for Secure Transactions in IoT**
  - *Biswas et. al. (2018)*

- **Solutions to Scalability of Blockchain: A survey**
  - ZHOU et. al. (2017)



This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2874099, IEEE Internet of Things Journal

IEEE INTERNET OF THINGS JOURNAL 1

A Scalable Blockchain Framework for Secure Transactions in IoT

Sujit Biswas, Kashif Shaif, *Member, IEEE*, Fan Li, *Member, IEEE*, Boubakr Nour, and Yu Wang, *Fellow, IEEE*

***Abstract*—Internet of Things and Blockchain technologies have been dominating their respective research domains for some time. IoT offers automation at the finest level in different fields, while Blockchain provides secure transaction processing for asset exchanges. The capability of IoT devices to generate transactions prompts their integration with Blockchain as the next logical step. The biggest challenges in this integration are the scalability of ledger and rate of transaction execution in Blockchain. On one hand, due to their large numbers, IoT devices will generate transactions at a rate which current block chain solutions cannot handle. On the other hand, implementing Blockchain peers onto IoT devices is impossible due to resource constraints. This prohibits direct integration of both technologies in their current state. In this article, we propose a solution to address these challenges by using a local peer network to bridge the gap. It restricts the number of transactions which enters the global Blockchain by implementing a scalable local ledger, without compromising on the peer validation of transactions at local and global level. The testbed evaluations show significant reduction in the block weight and ledger size on global peers. The solution also indirectly improves the transaction processing rate of all peers due to load distribution.**

***Index Terms*—Internet of Things, Blockchain, Scalability, Security, Transaction rate, Ledger size**

I. Introduction

INTERNET of Things (IoT) provides a platform for connecting daily use smart devices to gather, share, and forward information. Many of these exchanges are financial transactions which will dominate the future Internet architecture. The upcoming 5G technology will provide special support for machine-to-machine (M2M) [1] communications, which will allow unprecedented growth for IoT. Some estimates approximate that 50 billion devices will be registered as IoT devices by 2020 [2], and will generate trillions of transactions every day. Currently most of communication is performed based on a client-server model. In a centralize communication model, the system administrator may disclose sensitive data (e.g. health care, finance, etc.) due to insider attacks [3]. Furthermore, the conventionally centralized computing model favors several large-sized distributed data centers which creates a huge burden for computing, storage, and networking resources [4]. However, using traditional centralized communication models for such large scale data communication, storage, and analysis, from billions of devices is next to impossible. Although cloud and edge/fog architectures [5] do provide virtually unlimited storage and processing capacity, the bandwidth required to upload transactions creates a bottleneck in the network.

IoT networks and the embedded devices in them have drastically increased, which presents new dimensions to various threats related to security and privacy. Considering the limitations of existing client-server and cloud technologies, combined with rapid scalability of IoT, many researchers have suggested using Blockchain (BC) as a potential solution for security and privacy issues. The prime motivation for this stems from Bitcoin [6] (a public Blockchain for cryptocurrency transaction), to address the challenges of IoT security.

A. Blockchain Fundamentals

Blockchain was first introduced as Bitcoin [6] in 2009. As public Blockchain, Bitcoin is the first trust-less peer-to-peer electronic cash which has approximately 28.5 million [7] electronic wallets. Many others electric cash (e.g. ether [8], XRP [9], etc.) have been introduced since, and the number of wallets have increased multi-fold. Blockchain allows value exchange (i.e. transactions) without the need of trust authority from a central entity. These transactions are stored in a ledger which is maintained by a group of connected computers (i.e. peers), unlike a centralized entity like a bank database. BC system performs an autonomous verification (i.e. endorsement) before approving the transaction which plays a key role in ensuring security. The specialty of BC is that it is designed in such a way that no trust is needed, and security & reliability are obtained via special mathematical functions or code. Till 2016, most of the Blockchain networks have been used for cryptocurrency transactions. Recently Blockchain uses have

The work of Fan Li is partially supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61772077, 61370192 and 61432015. The work of Yu Wang is partially supported by the US National Science Foundation under Grant No. CNS-1343355, the National Natural Science Foundation of China under Grant No. 61572247, and by the U.S. Department of Transportation Center for Advanced Multimodal Mobility Solutions and Education.

S. Biswas, K. Shaif, F. Li, and B. Nour are with School of Computer Science, Beijing Institute of Technology, Beijing, P.

11

Solutions to Scalability of Blockchain: A Survey

QIHENG ZHOU, HUAWEI HUANG(MEMBER, IEEE), ZIBIN ZHENG(SENIOR MEMBER, IEEE), JING BIAN
School of Data and Computer Science, Sun Yat-Sen University, 510006, Guangzhou, China
National Engineering Research Center of Digital Life, Sun Yat-sen University, Guangzhou, China
Corresponding author: Huawei Huang, and Zibin Zheng. (e-mail: {huanghw28, zhzibin}@mail.sysu.edu.cn).

The work described in this paper was supported by the National Key Research and Development Program (2016YFB1000101), the National Natural Science Foundation of China (61902445, 61722214) and the Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2016).

ABSTRACT Blockchain-based decentralized cryptocurrencies have drawn much attention and been widely-deployed in recent years. Bitcoin, the first application of blockchain, achieves great success and promotes more development in this field. However, Bitcoin encounters performance problems of low throughput and high transaction latency. Other cryptocurrencies based on proof-of-work also inherit the flaws, leading to more concerns about the scalability of blockchain. This paper attempts to cover the existing scaling solutions for blockchain and classify them by level. In addition, we make comparisons between different methods and list some potential directions for solving the scalability problem of blockchain.

INDEX TERMS Blockchain, Scalability

I. INTRODUCTION

Blockchain as an emerging technology to realizing the distributed ledgers has attracted extensive research attention recently. Such a ledger intends to achieve decentralized transaction management, which means that any node joining the ledger can initiate transactions equally according to rules, and the transaction does not need to be managed by any third party. All transactions in the system are stored in blocks, which are then linked as a chain and organized in chronological order. Moreover, transactions that have written in blocks are immutable and transparent to all peers. With all these attractive characteristics, blockchain is drastically different from the traditional centralized trust entities and becomes a significant enabler to future financial systems. In recent years, the blockchain has developed rapidly, from Bitcoin [1], the first decentralized cryptocurrency, to Ethereum [2] with smart contracts, followed by the emerging permissioned blockchain (e.g. Hyperledger fabric [3]). Because of the wide adoption of Blockchain, blockchain based applications have been getting involved in our daily lives.

When the number of users of blockchain systems increases extensively, the scalability issues of major public-chain [4] platforms (e.g. Bitcoin and Ethereum) have arisen and greatly affected the development of blockchain.

Transaction throughput and transaction confirmation latency are two most talked-about performance metrics of blockchain and both of them have not reached a satisfactory level in recent popular blockchain systems [5], which leads to the bad user's quality of experience. However, compared with the centralized payment system like banks, these two metrics cannot be improved easily in blockchain, a self-regulating system, that needs more considerations in order to maintain decentralization. After numerous studies on the particularities of blockchain, some researchers raise the view of Blockchain Trilemma [6]. Similar to the CAP theory [7] in the traditional field of the distributed system, the Blockchain Trilemma points out that three important properties of a blockchain system, involving decentralization, security, and scalability, cannot perfectly co-exist. For instance, considering a simplified circumstance, adding a centralized coordinator into the system can reduce the consumption (e.g. computational resources consumed by proof-of-work [8]) for all users in the system to reach consensus on a set of transactions. Another example, shortening the block interval of Bitcoin can increase the transaction throughput but also affects the security of the whole system because of the increasing probability of fork. Therefore, balancing or even achieve these three aspects of blockchain system well is essential for the future development of blockchain that is suitable for more complex and larger-scale scenes in our daily lives.

16

Both articles are accepted to be published in IEEE.

PROBLEM STATEMENT

- The problem statement of article 11 is the difficulties faced while integrating Internet of Things (IoT) and Blockchain technologies.
- The **scalability** of the ledger and **rate of transaction execution** in Blockchain as well as resource limitations that prevent the implementation of Blockchain peers onto IoT devices are discussed.
- The problem statement of article 16 is the limitations of BC like *poor transaction throughput, high latency, and high storage requirements*, due to which blockchain **scalability** has grown to be a significant challenge.
- **Article 11 is a research article whereas article 16 is a survey article.**

Scalability is the major concern in both of the papers.

BACKGROUND

A Scalable Blockchain Framework for Secure Transactions in IoT

- Traditional security measures are challenging to implement in IoT systems -> a large number of devices and data they generate.
- Potential Solution: Blockchain technology (by providing a decentralized and tamper-proof mechanism for storing and sharing data.)
- However, current blockchain solutions have limitations in terms of scalability and efficiency, which make them unsuitable for IoT systems.
- The proposed article aims to address these limitations by proposing a **scalable blockchain** framework specifically designed for **secure transactions in IoT systems**.

BACKGROUND

Solutions to Scalability of Blockchain: A survey

- Scalability of blockchain has been a major challenge, with limited transaction throughput and high latency.
- The article aims to provide a **comprehensive survey of the different solutions** proposed to address the scalability issues of blockchain technology.
- It covers different categories of solutions, including ***consensus mechanisms, sharding, off-chain transactions, and network optimization techniques*.**
- It discusses the advantages and disadvantages of each solution and provides a critical evaluation of their effectiveness.

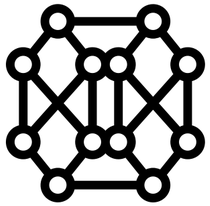
BLOCKCHAIN TECHNOLOGY

METHODOLOGY

A Scalable Blockchain Framework for Secure Transactions in IoT

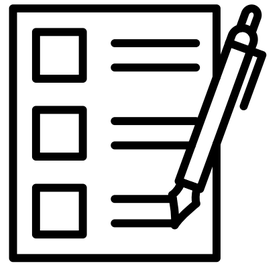
Systematic literature review

Develop a framework to improve scalability



Employ hybrid consensus algo(POW+PBFT) to facilitate high throughput, low latency, and energy efficiency

Used a local/global peer validation approach to make IoT transactions more secure and scalable.



Tested and validated the proposed framework using Hyperledger Fabric and simulated IoT transactions.

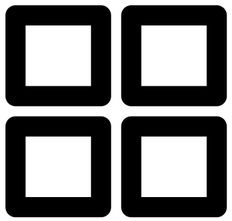
PBFT: Practical Byzantine Fault Tolerance

METHODOLOGY

Solutions to Scalability of Blockchain: A survey

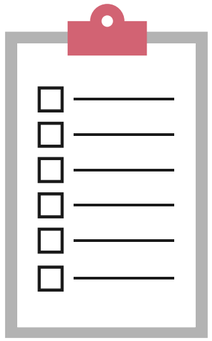
Search for articles

Systematic literature review



Categorization based on the proposed solutions

Comparision & analysis of advantages and disadvantages of solutions.



Summary of the surveyed solutions

Future directions for research

IMPLEMENTATION

A Scalable Blockchain Framework for Secure Transactions in IoT

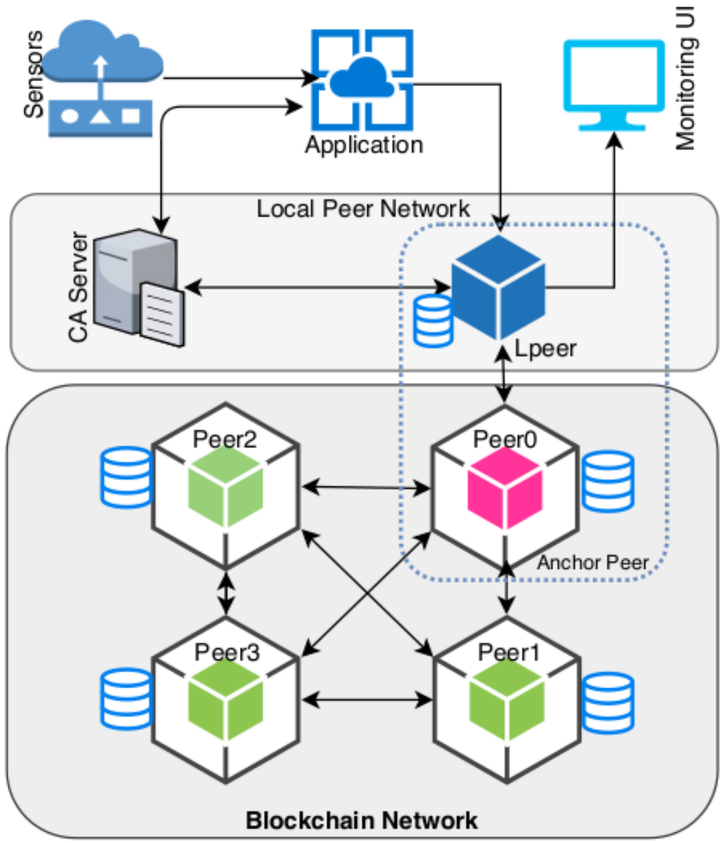


Fig. 2: Local peer based network model.

IMPLEMENTATION

A Scalable Blockchain Framework for Secure Transactions in IoT

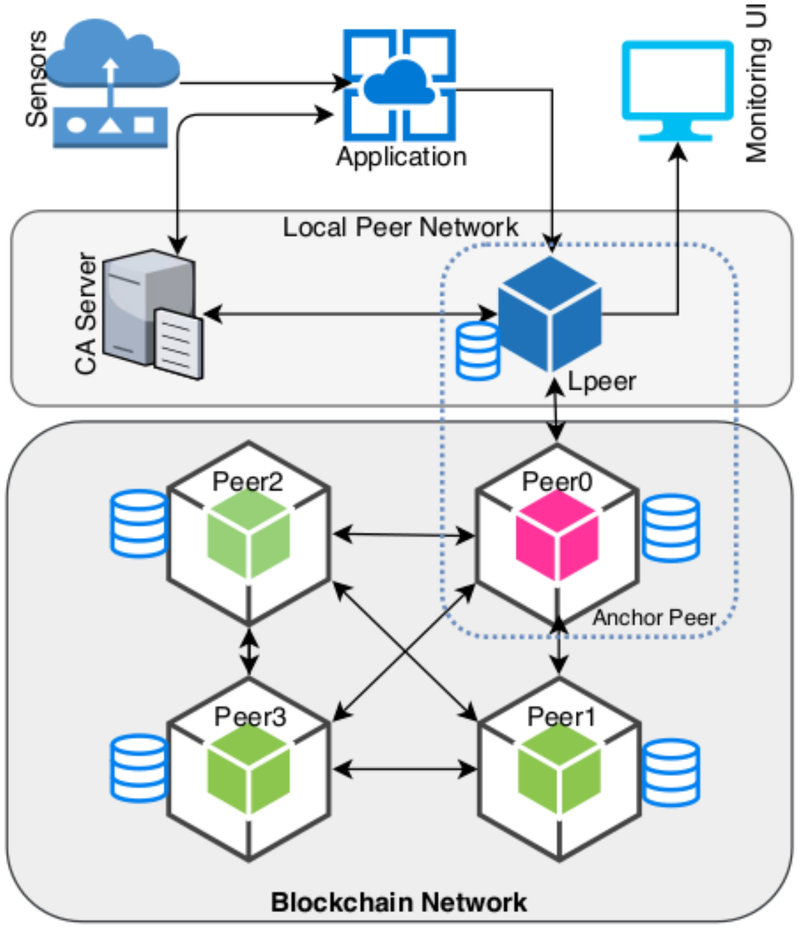


Fig. 2: Local peer based network model.

- Blockchain network -> smaller, localized networks, each with its own set of nodes and consensus mechanism.
- **Lpeer** is a local peer network that processes transactions within a small group of nodes, improving throughput and reducing latency.
- **Anchor Peer** - a node that connects multiple Lpeer networks, enabling secure and transparent data sharing between the networks.
- Result: Increased scalability, reduced latency, and improved security for IOT systems.

- Note: All IoT devices have an association to an organization.

IMPLEMENTATION

Solutions to Scalability of Blockchain: A survey

- Survey paper -> no implementation.
- Detailed analysis of different proposed solutions including consensus mechanisms, sharding, off-chain transactions, and n/w optimization techniques.
- Divided the scalability solutions into three layers: Layer0, Layer1, and Layer2.

Layer	Categories
Layer0:	Data propagataion
Layer1:	Block data, consensus, sharding, DAG
Layer2:	Side chain, cross-chain, off-chain computation

IMPLEMENTATION

Solutions to Scalability of Blockchain: A survey

Layer0 solutions

Improves the underlying blockchain infrastructure, including improving consensus mechanisms and network protocols.

IMPLEMENTATION

Solutions to Scalability of Blockchain: A survey

Layer1 solutions

Involves modifying the blockchain architecture to increase transaction throughput and reduce latency, such as sharding, parallelization, and pruning.

IMPLEMENTATION

Solutions to Scalability of Blockchain: A survey

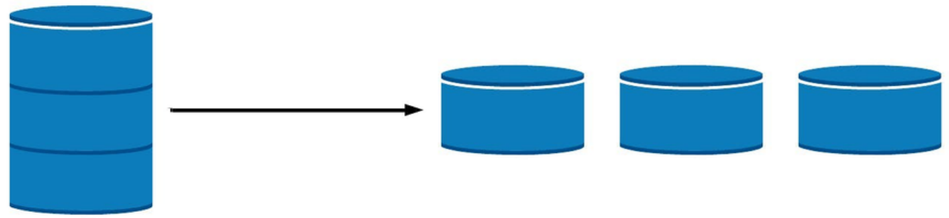
Layer2 solutions

Off-chain solutions that leverage the underlying blockchain infrastructure to enable faster and cheaper transactions, such as state channels, payment channels, and sidechains.

ALGORITHMS USED IN SOLUTIONS

Solutions to Scalability of Blockchain: A survey

- Sharding
- Plasma
- Lightning Network
- Proof of Stake
- DAG



Sharding algorithm in blockchain involves dividing the network into smaller subnetworks (shards) that can process transactions independently to increase scalability.

Note:The details of the algorithms are beyond the scope of the presentation

ALGORITHMS USED IN SOLUTIONS

Solutions to Scalability of Blockchain: A survey

- Sharding
- Plasma
- Lightning Network
- Proof of Stake
- DAG

It is a hierarchical structure that enables the creation of child chains or side chains that operate independently of the main chain but are still secured by it.

Note:The details of the algorithms are beyond the scope of the presentation

ALGORITHMS USED IN SOLUTIONS

Solutions to Scalability of Blockchain: A survey

- Sharding
- Plasma
- Lightning Network
- Proof of Stake
- DAG

The Lightning Network is a second-layer protocol that aims to address the scalability challenges of the Bitcoin blockchain by enabling off-chain transactions between two parties.

Note:The details of the algorithms are beyond the scope of the presentation

ALGORITHMS USED IN SOLUTIONS

Solutions to Scalability of Blockchain: A survey

- Sharding
- Plasma
- Lightning Network
- Proof of Stake
- DAG

is a consensus mechanism that selects block validators based on their stake in the network, and it has the potential to address the scalability and energy consumption challenges of the proof of work algorithm used in Bitcoin.

Note:The details of the algorithms are beyond the scope of the presentation

ALGORITHMS USED IN SOLUTIONS

Solutions to Scalability of Blockchain: A survey

- Sharding
- Plasma
- Lightning Network
- Proof of Stake
- DAG

The DAG (Directed Acyclic Graph) algorithm is a data structure used in some blockchain systems, which allows for parallel transaction processing and eliminates the need for miners, potentially addressing the scalability and energy consumption challenges of traditional blockchain systems.

Note:The details of the algorithms are beyond the scope of the presentation

RESULTS

A Scalable Blockchain Framework for Secure Transactions in IoT

- The proposed framework for IoT -> scalable and can handle a large number of IoT devices and transactions without compromising security or efficiency.
- Framework is more secure for IoT applications*(prevents unauthorized access and double spending attacks).*
- Increase in TPS for the global BlockChain.
- Limit the geometrical increase of ledger storage.
- 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.

RESULTS

Solutions to Scalability of Blockchain: A survey

- **A comprehensive survey** of proposed solutions to address scalability issues in blockchain technology
- **Identifies key challenges in scaling:** Transaction processing, data storage, and consensus mechanisms.
- **Analyzes** how the proposed solutions address these challenges.
- **Evaluates the effectiveness** of the proposed solutions in terms of their scalability, security, and decentralization.
- Concludes only one solution might not be enough.

FUTURE WORK

- Real world implementation using real-time transactional data
- Optimizing the consensus mechanism and reducing the communication overhead between local networks and the main blockchain network.
- The proposed framework can be **evaluated in more complex and realistic IoT environments** to validate its effectiveness and scalability.
- **Need for more research** on how to integrate different solutions at different layers to achieve scalable and secure blockchain systems.

CRITICAL COMMENTS

- Experiments were only run on a small testbed with only two machines, which might not fully reflect an IoT scenario in practice.
- The article omits analyzing in depth the security vulnerabilities connected to the suggested structure
- The paper could have discussed the limitations of the proposed framework and potential areas for improvement, which would have added more value to the paper.
- No detailed evaluation or comparison of the proposed solutions in terms of their effectiveness, efficiency, and security, which limits the usefulness of the paper.

THANK YOU!

SABIN THAPA
SABINT017@GMAIL.COM
DHULIKHEL-4, KAVRE
KU CE IV/II