International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Comparative Analysis of IoT-Based Blockchain Frameworks for Secure and Scalable Applications

[1]Mr. Jayant P. Mehare, [2]Dr. Amit K. Gaikwad

Submitted: 22/04/2023 **Revised:** 26/06/2023 **Accepted:** 06/07/2023

Abstract: The rapid emergence and evolution of blockchain technology have created new opportunities for implementing secure and scalable applications on the Internet of Things. Unfortunately, choosing the right blockchain framework for these applications can be challenging due to the vast number of available options. The paper explores the three main frameworks that are used in the development of IoT-based applications: IOTA, Hyperledger, and Ethereum. This paper aims to provide a comprehensive analysis of the various aspects of the three main blockchain frameworks used in the development of IoT applications. It will help decision-makers make informed decisions when it comes to implementing their applications. The paper's introduction highlights the importance of considering the various factors that affect the development and implementation of IoT-based applications. It also provides a comprehensive overview of the various blockchain frameworks that are used for this type of technology. In addition, it reviews the literature on the security challenges and scalability issues of these frameworks. This paper aims to provide a comprehensive analysis of the research that has been conducted on the secure and scalable implementation of these types of applications. This study presents the methodology for analyzing the various blockchain frameworks that are used for building IoT applications. The evaluation criteria are defined and the methods are described. The study also acknowledges the potential biases and limitations of these frameworks. The comparative analysis section of the paper takes a look at the different blockchain frameworks. It offers descriptions of IOTA, Ethereum, and Hyperledger Fabric and their features. It also delves into their security protocols and mechanisms, as well as their scalability solutions. The study explores the applications and use cases of these frameworks. The findings and discussion section compares and examines the security attributes of the different frameworks. It also explores their performance and scalability. In addition, it talks about the implications of such applications for their stable and scalable nature. The paper's comprehensive analysis of the three main blockchain frameworks used for developing IoT applications, namely IOTA, Ethereum and Hyperledger, provides valuable insight for decision-makers when it comes to choosing the ideal framework for their projects. The findings and recommendations that the paper presents contribute to the established body of knowledge about this type of technology and its applications.

Keywords*: IoT-based blockchain, Secure applications, Scalable applications, Hyperledger Fabric, Ethereum and IOTA.*

1. Introduction

The rapid emergence and evolution of blockchain technology and the Internet of Things have raised significant concerns about their potential to transform the way organizations operate. With the combination of these two technologies, organizations can now achieve new levels of trust and transparency in their systems. Due to the complexity of the IoT environment and the varying options available, it is still challenging to choose the right blockchain framework for applications that are based on this technology[1], [2].

The goal of this study is to provide an in-depth analysis of the various blockchain frameworks that are used for the Internet of Things (IoT). They are examined based on their scalability and security features. Some of these include IOTA, Hyperledger Fabric, and Ethereum. These have gained widespread attention due to their potential to provide stable and secure applications[3]–[5].

Developers of blockchain frameworks for the Internet of Things ecosystem aim to address specific challenges and requirements when it comes to integrating the technology into their applications. These frameworks offer the necessary resources and infrastructure to enable secure and distributed transactions, as well as data sharing and smart contract execution as shown in fig.1. Each framework's architecture and features are designed to accommodate different IoT applications' needs.

1PhD Scholar, Assistant Professor, Department of CSE G H Raisoni University, Amravati, Maharashtra, India, 444701
Jayant.mehare@ghru.edu.in
2Associate Professor, Department of CSE G H Raisoni University, Amravati, Maharashtra, India, 444701
Amit.gaikwad@ghru.edu.in

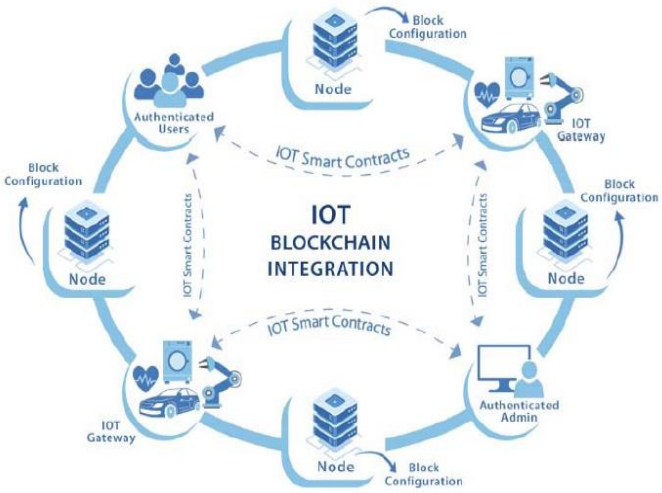

Fig. 1 Integration of IoT with Blockchain

The Hyperledger Fabric is a framework created by the Linux Foundation that is designed to provide a flexible and modular infrastructure for developing IoT applications. It features a variety of features such as smart contracts and secure access control, which are ideal for use cases that require high levels of privacy and governance.

With the ability to execute smart contracts, Ethereum is a leading platform for developing decentralized applications. Developers can use its platform to create and deploy DApps, which are internet of things-related services. Its open architecture and versatile tools make it an ideal choice for developing such applications.

IOTA utilizes a unique architecture, which is characterized by its use of the directed acyclic graph. Unlike other blockchain frameworks, it doesn't rely on a central chain of blocks to perform transactions. Instead, it uses a decentralized network to perform validation and confirm transactions. This makes it ideal for applications that deal with small and frequent transactions. IOTA's focus on low transaction fees, machine-to-machine communication, and scalability makes it an ideal choice for developing IoT applications.

When it comes to implementing blockchain technology into the Internet of Things ecosystem, there are various security issues that need to be resolved in order to ensure the confidentiality and integrity of the data and transactions as shown in fig.2. One of these is the protection of the identities of the devices. As the interactions between the network and the devices become more complex, it's important that the identities of the devices are secure.

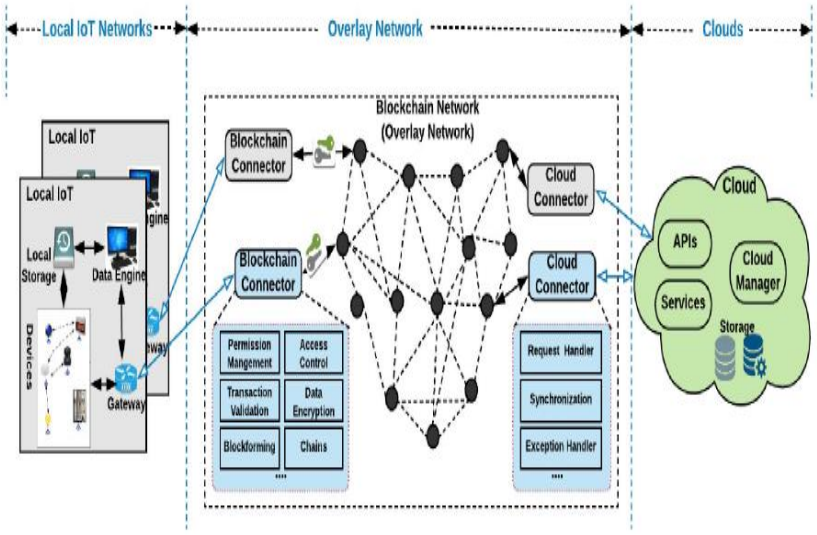

Fig. 2 IoT architecture with blockchain.[6]

Data privacy is another issue that needs to be resolved in order to ensure the confidentiality and integrity of the information and transactions. Since blockchain technology is transparent, it's important that the devices' sensitive information is protected. This can be achieved through the use of various cryptographic techniques such as homomorphic encryption and zero-knowledge proofs.[7], [8]

Due to the nature of blockchain technology, it's also important that the transactions are validated properly in order to prevent unauthorized access and manipulation. One of the most common attack vectors that can be used to take over a network is the Sybil attack. This type of attack can allow an adversary to take over multiple nodes in the network. Another issue that can affect the security of the blockchain is the vulnerability that's caused by smart contracts[9].

When it comes to developing blockchain applications for the Internet of Things ecosystem, scalability is another important factor that needs to be considered. Traditional networks can't handle the amount of data that's generated by the connected devices[10], [11]. This can prevent real-time applications from working properly. The issue of scalability can also be exacerbated by the limited resources of the connected devices. These gadgets typically have low memory, bandwidth, and computational power, making it hard to participate in the consensus mechanisms that are required by blockchain frameworks[12], [13].

Various methods to address this issue, such as sharing and off-chain solutions, have been proposed. The former involves splitting the blockchain into smaller parts, which can be used for parallel processing. Off-chain methods, such as sidechains and state channels, can also help improve the network's performance. Lightweight consensus methods, such as proof-of-stake (PoS) or directed acyclic graph (DAG) can be used to address this issue without compromising on security[14]–[16].

The paper aims to provide a comprehensive analysis of the various frameworks that are available for the Internet of Things ecosystem. It focuses on the features and architectures of IOTA, Hyperledger Fabric, and Ethereum. Through its overview, the paper can help developers identify which framework is ideal for their applications. The investigation of scalability and security issues along with blockchain applications for the IoT ecosystem provides valuable insights into the unique challenges and possible solutions. By evaluating the merits and drawbacks of these frameworks, testers can select the best option for their IoT deployments.

2. Literature Review

The convergence of the Internet of Things (IoT) and blockchain technology has opened up new possibilities for secure and scalable applications. The combination of IoT and blockchain offers enhanced data integrity, privacy, and decentralized trust in various domains such as supply chain management, healthcare, and industrial systems. This literature review aims to provide an overview of the research conducted in the field of IoT-based blockchain frameworks, with a focus on challenges, solutions, and future directions. The selected research papers cover a wide range of topics, including security, scalability, privacy, adoption, and applications of blockchain in IoT.

A. Dorri et al.[17] presented a comprehensive review of blockchain in the IoT, highlighting the challenges and potential solutions for integrating the two technologies. They discussed the issues of scalability, interoperability, and resource-constrained IoT devices. J. Song et al.[18] proposed an anomaly detection and visualization tool for IoT blockchain, addressing the security aspects of IoT data. Their work focused on detecting abnormal patterns in IoT devices' behavior and visualizing the data for better analysis and decision-making. D. Minoli et al.[19] explored the mechanisms of using blockchain for IoT security. They discussed the different security challenges in IoT systems and presented blockchain-based solutions to address those challenges, such as data integrity, access control, and device authentication.

M. A. Khan et al.[20] conducted a review of IoT security, blockchain solutions, and open challenges. They discussed the vulnerabilities in IoT systems and the potential of blockchain technology to enhance security. The paper also highlighted the open research challenges and future directions in the field. H. T. T. Truong et al.[21] proposed a secure and decentralized data sharing framework for IoT. They presented a solution based on blockchain technology to enable secure and privacy-preserving data sharing among IoT devices and stakeholders. J. Hathaliya et al.[22] focused on the application of blockchain in remote patient monitoring. They proposed a blockchain-based solution to ensure secure and transparent sharing of patient health data, improving healthcare delivery and patient outcomes.

L. Tseng et al.[23] discussed the challenges, opportunities, and analysis of blockchain-based databases in IoT environments. They explored the potential benefits and limitations of integrating blockchain with IoT databases and highlighted future research directions. R. A. Memon et al.[24] conducted a comparative survey between cloud-based and blockchain-based IoT systems. They discussed the advantages and disadvantages of both approaches and presented insights for future research and development in the field. A. R. Mahlous et al.[6] provided

an insight view of the adoption of blockchain technology in the IoT domain. They discussed the potential benefits, challenges, and adoption factors for integrating blockchain into IoT systems, highlighting the impact on security, privacy, and efficiency. P. Patil et al.[25] conducted a review of blockchain for IoT access control, security, and privacy. They discussed the various blockchain-based access control mechanisms, security considerations, and privacy preservation techniques in IoT systems.

A. Attkan et al.[26] presented a comprehensive review of cyber-physical security for IoT networks, focusing on traditional, blockchain, and artificial intelligence-based key security mechanisms. They discussed the challenges and opportunities in securing IoT networks and highlighted the potential of blockchain and AI in addressing those challenges. S. S. Hameedi et al.[27] proposed a lightweight blockchain dynamic table for improving IoT data security and integrity. They presented a solution that combines blockchain technology with a dynamic table structure to enhance data security in IoT systems, addressing the challenges of scalability and storage efficiency. W. Liang et al.[28] conducted a systematic review of privacy challenges in IoT-based blockchain systems. They discussed the privacy concerns, threats, and countermeasures in the integration of IoT and blockchain and identified the future research directions for addressing privacy challenges.

E. Nehme et al.[29] proposed a conceptual ethics framework for the convergence of AI, IoT, and blockchain technologies. They discussed the ethical implications and considerations when combining these technologies, aiming to promote responsible and ethical practices in their development and deployment. D. Ravi et al.[30] presented a blockchain-based transparent supply chain management system using Hyperledger Fabric. They discussed the implementation of Hyperledger Fabric to ensure privacy-preserving and transparent supply chain operations, enhancing trust and efficiency in the supply chain ecosystem. T. Ye et al.[31] conducted a survey on redactable blockchain technology, discussing the challenges and opportunities in this emerging field. They explored the applications, benefits, and future directions of redactable blockchains, which allow for selective data removal or modification. M. M. Akhtar et al.[32] proposed a data communication framework using distributed ledger technology and IOTA-enabled IoT for future machine-to-machine economies. They presented a solution for efficient and secure data communication in IoT systems, leveraging the unique features of IOTA for machine-to-machine transactions.

The literature review highlights the challenges, solutions, and future directions in the integration of blockchain and IoT for secure and scalable applications. The analyzed research papers provide insights into various aspects of this field, including security, scalability, privacy, adoption, and applications. The findings emphasize the potential benefits of blockchain in enhancing the security and trustworthiness of IoT systems, while also highlighting the challenges such as scalability, interoperability, and privacy preservation. Future research directions include addressing vulnerabilities in smart contracts, improving scalability solutions, ensuring privacy in IoT-based blockchain systems, and exploring emerging technologies such as AI and redactable blockchains. By addressing these challenges and advancing research in these areas, the integration of IoT and blockchain can pave the way for secure, scalable, and privacy-preserving applications in various

3. Methodology

A. Selection of major IoT-based blockchain frameworks:

The study has selected IOTA, Hyperledger Fabric, and Ethereum as its primary frameworks for analysis. These are all popular in the field of Internet of Things-based applications, and they represent a variety of features and architectural designs.

B. Evaluation criteria for secure and scalable applications:

The study's evaluation criteria will help identify the various aspects of the chosen frameworks' capabilities for building secure and scalable applications.

- Security mechanisms: The study will look into the security mechanisms of the frameworks, such as authentication, encryption, and access control. These are designed to protect the data and devices of the Internet of Things.
- Privacy preservation: The study will also look into the various techniques that the frameworks employ to enhance the privacy of the data they collect. These include data anonymization and cryptographic protocols.
- Scalability solutions: The study will also look into the various scalability mechanisms that the frameworks employ to accommodate the growing number of transactions and devices connected to the Internet of Things.
- Performance evaluation: The study will also conduct performance tests to evaluate the various factors that affect the efficiency of the chosen frameworks for developing real-time applications.
- Development ecosystem: The development ecosystem of blockchain frameworks is examined. They are analyzed for their ease of use and

documentation, as well as their resources for developers creating applications that are built on the Internet of Things.

C. Data collection and analysis methods:

The data collected for this study is collected through a combination of quantitative and qualitative methods. Besides the usual sources, such as technical papers and white papers, the study also analyzed the various aspects of the frameworks' architecture and security features. It also conducted case studies on the implementation of these frameworks in real-world scenarios.

Through a systematic approach, the collected data is analyzed to determine the various features and performance metrics of the chosen frameworks. The evaluation criteria are then used to compare and contrast the various aspects of the frameworks. In addition, qualitative methods such as pattern recognition and content analysis are utilized to identify the common themes and weaknesses of the frameworks.

A quantitative analysis is carried out to generate an empirical evaluation of the performance metrics and scalability of the chosen frameworks.

D. Limitations and potential biases:

The study's potential biases and limitations are acknowledged. The research only focuses on three major blockchain frameworks: IOTA, Ethereum, and Hyperledger Fabric. This means that it doesn't consider other specialized or emerging frameworks that can offer distinct advantages. Furthermore, the evaluation parameters are predetermined and may not cover all aspects of the chosen technologies. The evaluation criteria might not be able to address every requirement for IoT-based applications.

The study is also conducted on the basis of publicly available information, which could be biased or incomplete representations of certain aspects of the chosen frameworks. In addition, the results of the evaluation may vary according to the network conditions, the test environment, and the configuration settings of the chosen frameworks.

Comparative Analysis of IoT-based Blockchain Frameworks

A. Hyperledger Fabric

- Description, features, and architecture:

The Hyperledger Fabric project is an open-sourced blockchain framework that's designed for business-grade applications[33], [34]. It features a flexible and modular design that can be used for various purposes. Its architecture is composed of various components, such as peers, an ordering service, and a membership provider. The members of the system maintain and execute chain contracts, while the ordering service checks the status of the distributed ledger. The management of access and identity within the network is handled by the MSP. Fig.3 shows the architecture.

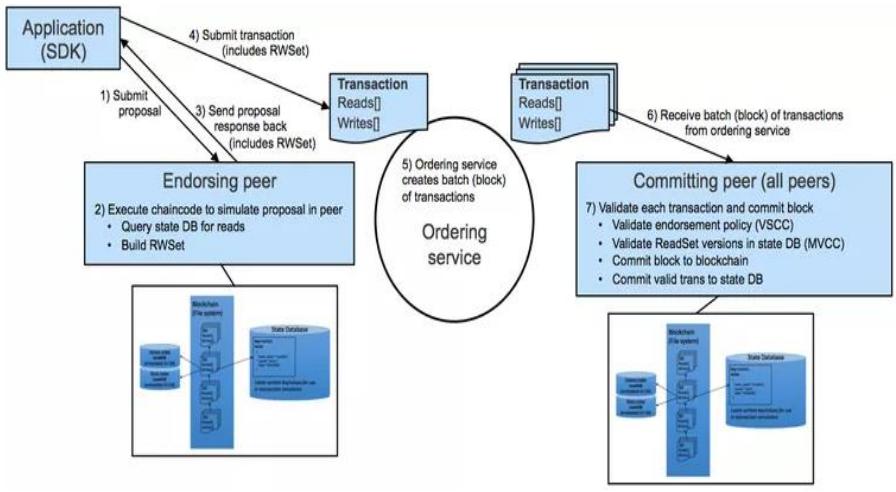

Fig. 3 Architecture of Hyperledger fabric (src-IBM)

- Security mechanisms and protocols:

The Hyperledger Fabric uses various security protocols and mechanisms. Its permissioned model ensures that users are authorized and can access the network. Its identity management system, which is handled by the managed service provider, ensures that all interactions are secure. Private channels are enabled by Hyperledger Fabric. These allow for the transmission of confidential information to only authorized users. Moreover, it offers granular control measures to enforce the confidentiality of its data.

- Scalability solutions and performance evaluation:

Through its various scalability techniques, such as channel partitioning, Hyperledger Fabric can be used for various applications. It can allow for more privacy and increased transaction throughput for certain use cases. Its modular design allows organizations to expand their networks horizontally. The evaluation results of the Hyperledger Fabric demonstrated its low latency and high throughput. It's ideal for developing complex IoT applications.

- Use cases and applications:

Various industries consider Hyperledger Fabric suitable for its applications. One of its most common use cases is supply chain management, as it enables companies to ensure the integrity and traceability of their products. It's also been utilized in healthcare to secure the exchange of patient data. Its ability to facilitate secure access control and collaboration enables organizations to interact with multiple stakeholders in various IoT-related fields.

The scalability and robust nature of Hyperledger Fabric make it ideal for business-grade Internet of Things (IoT) applications. Its privacy features, security measures, and modular design make it suitable for various use cases. These factors help ensure that the data integrity, transparency, and access control of the system remain uncompromised.

B. Ethereum

- Description, features, and architecture:

Developers can create and deploy various decentralized applications with the help of Ethereum, a blockchain platform that allows smart contracts to be executed[35], [36]. It is constructed on a public ledger, and it has a global state, which is represented by the Ethereum virtual machine. Smart contracts are defined by rules and logic, and they can be written in various programming languages. Fig.4 shows the architecture.

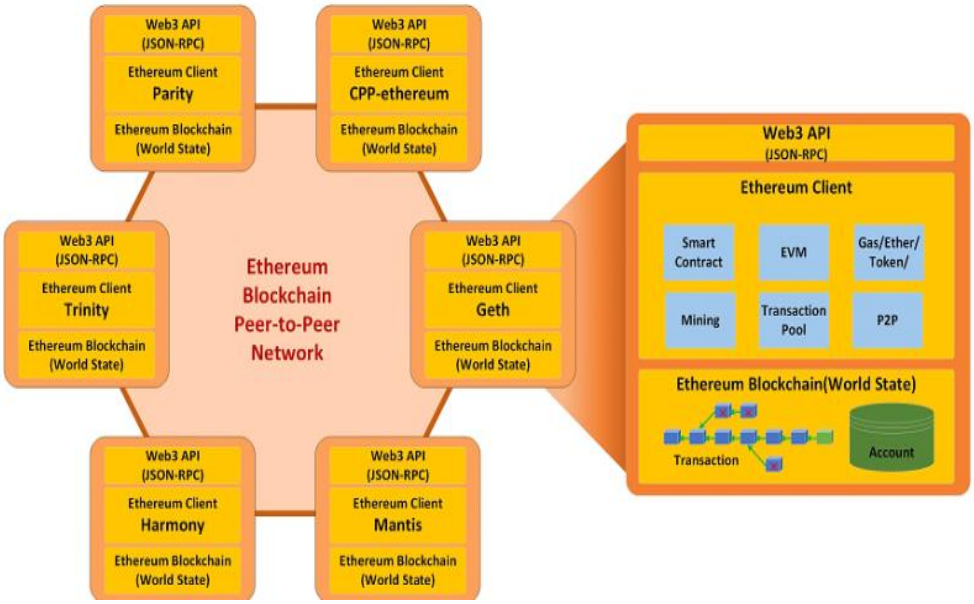

Fig. 4 Architecture of Ethereum (src-bootcamps)

- Security mechanisms and protocols:

The platform uses various security protocols and mechanisms to ensure the safety and integrity of its operations. One of these is the "Ethash consensus algorithm". This ensures that the blockchain can remain immutable by requiring its nodes to solve computational puzzles. In addition, it supports the integration of secure hash functions and cryptographic signatures to verify the authenticity of smart contracts and transactions.

- Scalability solutions and performance evaluation:

Due to its current architecture's limitations, Ethereum has been criticized for its lack of scalability. In an effort to address this issue, the company has been working on various scalability solutions. One of these involves the development of a new consensus mechanism known as PoS. This feature will allow users to perform parallel transactions on the Ethereum blockchain. Another scaling solution that is designed to increase throughput and reduce costs is the sidechains and state channels.

- Performance evaluations:

Although its performance has been commended, the high transaction volumes that the Ethereum network encounters can result in slower confirmation times and increased fees. In order to address these issues, the company is developing a new version of its software known as Ethereum 2.0, which will introduce more robust and efficient scaling solutions.

- Use cases and applications:

Developers can utilize the Ethereum platform for a wide range of applications and use cases, especially within the finance industry. Its smart contracts allow them to create decentralized platforms that are designed to provide various services, such as loan applications and exchanges. Ethereum's smart contracts also enable tokenization and crowdfunding through initial coin offerings (ICOs) and security token offerings (STOs). Developers can also use the Ethereum platform for various IoT-based applications, like supply chain management. Its smart contracts can help ensure the traceability, transparency, and automation of various processes.

Developers can also use the platform to create decentralized marketplaces, digital identity management systems, and other decentralized applications. Its ecosystem, which includes a robust developer community, interoperability, and a wide range of smart contracts, makes it an ideal choice for developing Internet of Things (IoT) applications. Ethereum is a blockchain-based platform that enables developers to create and deploy decentralized applications. It can be used for various purposes, such as the development of smart contracts. Its interoperability, security measures, and ongoing optimizations make it a suitable choice for developing IoT applications in diverse sectors.

C. IOTA

- Description, features, and architecture:

IOTA is an open-source distributed ledger system that is designed for the Internet of things. It utilizes a distributed ledger known as the Tangle, which is a type of distributed ledger that's built on a direct acyclic graph[37], [38]. It allows for efficient and fee-free transactions between users. IOTA is ideal for the IoT as it eliminates the need for central authority in order to perform transactions. Fig.5 shows the architecture of IOTA.

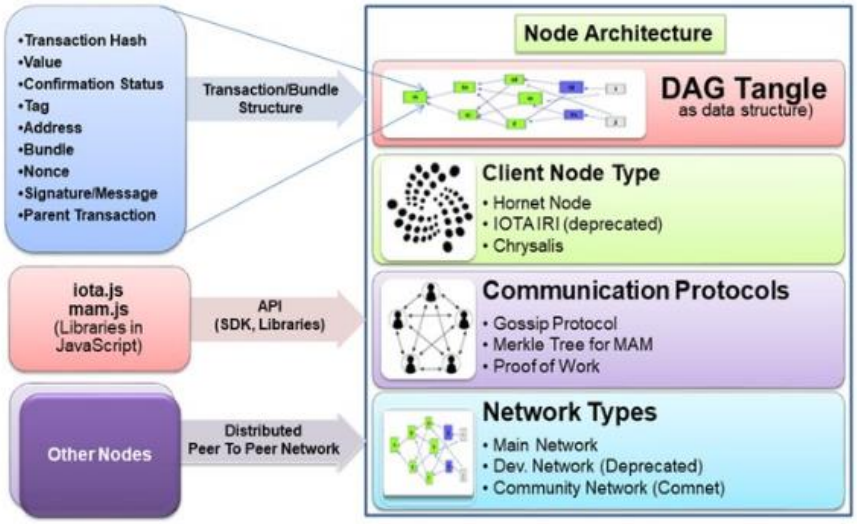

fig. 5 Architecture of IOTA

- Security mechanisms and protocols:

IOTA uses various security protocols and mechanisms to protect its network from attacks. One of these is the Coordinator, which is a consensus mechanism that's designed to prevent attacks during the initial stages of the network. Its milestones serve as references that help validate transactions. It also utilizes digital signatures and hash functions to prevent tampering.

- Scalability solutions and performance evaluation:

One of the main factors that IOTA uses when it comes to developing its network is its ability to maintain high scalability. Its structure allows for multiple transactions to be performed simultaneously, which creates a network effect. One of its solutions is called Flash Channels, which enables off-chain micro-transactions. It's also exploring other methods such as swarm intelligence and sharding to improve its performance.

IOTA has demonstrated its ability to perform numerous transactions with low resource requirements and minimal latency. Its fee-free nature makes it ideal for the IoT, especially in applications that require frequent micro-transactions, which is why it's widely used.

- Use cases and applications:

IOTA is widely used in various applications and sectors within the Internet of Things (IoT). One example of its use is in smart cities, where it enables secure and efficient payments through its micro-transactions. These services include the provision of electric vehicle charging and energy management. In logistics and supply chain management, IOTA provides a way to ensure that transactions are conducted in a transparent and traceable manner.

IOTA is also widely used in data marketplaces, where it enables organizations and individuals to easily share and monetize the information collected by their IoT devices.

Its lightweight architecture and feeless nature make it ideal for devices that have limited resources. It has also been showcased in various sectors, such as healthcare and industrial IoT.

IOTA is a distributed ledger technology that's designed for the efficient and secure transactions that are required in IoT applications. Its feeless nature, scalability, and architecture make it ideal for various industries. Its security protocols and mechanisms ensure that the data and transactions are protected.

Comparative analysis of Hyperledger fabric, Ethereum and IOTA

Criteria	**Hyperledger Fabric**	**Ethereum**	**IOTA**
Security Strengths	- Permissioned model provides controlled access and privacy. - Granular access control policies ensure data confidentiality and authorized network participation. - Identity management system (MSP) ensures secure access and authentication of network participants.	- Strong cryptographic mechanisms and secure hash functions ensure transaction integrity and data security.	- Cryptographic algorithms and digital signatures protect transactions and prevent tampering.
Security Weaknesses	- Potential vulnerabilities in smart contract code. - Dependence on the security practices of network participants.	- Vulnerabilities in smart contract code and potential security risks in decentralization trade-offs. - Risk of security vulnerabilities in decentralized applications (DApps) developed on Ethereum.	- Coordinator dependency during early stages and potential security vulnerabilities in Coordinator implementation.
Scalability Performance	- Supports parallel transactions through private channels, enhancing scalability. - Horizontal and vertical scaling capabilities by adding more peers and increasing the capacity of existing peers. - High throughput and low latency demonstrated in performance evaluations.	- Ongoing scalability efforts through Ethereum 2.0 upgrade and layer 2 scaling solutions like state channels and sidechains. - Sharding and rollups aim to increase Ethereum's capacity and reduce transaction costs. - Improved transaction processing speed with Ethereum 2.0's transition to proof-of-stake (PoS).	- Inherent scalability through the Tangle structure and ongoing exploration of sharding and swarm intelligence for further scalability.

Scalability Limitations	- Resource requirements increase with network growth, potentially affecting scalability. - Performance degradation with increasing number of peers in the network.	- Network congestion affects performance during high transaction volumes.	- Limited scalability in terms of transaction volume and confirmation times during Coordinator dependency.
Use Cases and Applications	- Supply chain management, healthcare data sharing, smart cities.	- Decentralized finance (DeFi), tokenization and crowdfunding, digital identity management, decentralized marketplaces.	- Secure payment systems in smart cities, supply chain and logistics, data marketplace applications, IoT sensor networks.

Various security features are implemented by IOTA, Hyperledger Fabric, and Ethereum to ensure that sensitive information is protected. With its permissioned model, Hyperledger Fabric can provide users with complete privacy and control over their access. It also offers a secure identity management solution through its membership service provider. Strong cryptographic capabilities are used in Ethereum to ensure the integrity of transactions and data. However, there are some concerns about its smart contract code and decentralization trade-offs. IOTA utilizes various security features, such as digital signatures and algorithms, to protect its network.

Comparative analysis of the frameworks in various domains

Criteria	**Hyperledger Fabric**	**Ethereum**	**IOTA**
Supply Chain	Offers privacy and confidentiality for sensitive supply chain data through private channels.	Enables transparent and traceable supply chain transactions through smart contracts.	Facilitates secure and efficient payment systems for supply chain transactions.
	Granular access control policies ensure data privacy and access restrictions.	Smart contracts allow for automated execution of supply chain processes.	
	Provenance and traceability of goods can be recorded on the blockchain, ensuring authenticity and preventing counterfeit products.	Integration with Internet of Things (IoT) devices enables real-time tracking of goods and inventory management.	
	Enables secure sharing of supply chain data across multiple stakeholders with permissioned access.		
Multi-Layer IoT Industrial System	Provides a platform for secure and authorized access control across multiple layers of an industrial IoT system.	Allows for the development of IoT-based industrial applications with its extensive developer ecosystem.	- Facilitates secure machine-to-machine (M2M) transactions and data transfers within the industrial system.
	Granular access control and permissioned network ensure data confidentiality and integrity across different layers.	Smart contracts enable automation and self-execution of IoT processes.	

	Enables interoperability and seamless communication between IoT devices and systems.	Extensive developer community and toolsets for building IoT-based industrial solutions.	
	Integration with existing industrial protocols and systems for data exchange and interoperability.		
Healthcare	Ensures secure and interoperable sharing of patient data, improving healthcare data management and privacy.	Facilitates decentralized health records management, giving patients ownership and control over their medical data.	Enables secure sharing of healthcare data among authorized parties, ensuring data integrity and privacy.
	Granular access control and permissioned network safeguard patient data and ensure privacy compliance.	Secure storage and sharing of medical records using blockchain-based encryption and access control.	
	Enables seamless integration and sharing of healthcare data across multiple healthcare providers and systems.	Increased patient autonomy and control over their health data through self-sovereign identity solutions.	
	Transparent and auditable healthcare transactions, improving trust and reducing fraud.		

4. Discussion and Findings

- **Analysis of scalability solutions and performance results**

  One of the most critical factors that a blockchain application must consider when it comes to scalability is its ability to support multiple transactions. With the Hyperledger Fabric, it can be used to address this issue by allowing users to add more peers or vertically expand its capacity. Its low latency and high throughput make it ideal for mission-critical applications. In Ethereum 2.0, the company is working on various scalability solutions, such as sharding, PoS, and layer 2. Although these solutions are expected to improve the performance of its applications, network congestion and other factors can still affect it. One of the most important factors that IOTA can offer when it comes to addressing this issue is its ability to provide stable and fast transactions.

- **Implications for secure and scalable IoT-based blockchain applications**

  The results indicate that the two frameworks have weaknesses and strengths when it comes to scalability and security. The Hyperledger Fabric is ideal for applications that require privacy and control, while Ethereum is versatile enough for industrial IoT systems. Although IOTA's scalability and feeless transactions make it an ideal choice for supply chain management applications, its vulnerability to smart contracts and the role of the Coordinator in its security raise concerns.

  Before implementing and scaling an IoT-based blockchain solution, it's important that organizations thoroughly research the various requirements of the system. In addition to network access control and transaction throughput, other factors such as data privacy and interoperability should also be taken into account. Developers should also consider the ecosystem's development support, as well as the existing use cases of the platform.

The comparative analysis highlights the scalability and security attributes of IOTA, Hyperledger Fabric, and Ethereum. This resource serves as a valuable reference that enables organizations to make secure and manageable decisions with regard to implementing and managing IoT-centric blockchain applications.

5. Conclusion and Future Scope

This paper evaluated the capabilities of Ethereum, IOTA, and Hyperledger Fabric in the context of distributed ledgers that are secure and interconnected with the Internet of Things (IoT). The different frameworks exhibited distinct weaknesses and strengths in different areas, such as healthcare, supply chain, and industrial systems. The Hyperledger Fabric provides a secure and resilient supply chain management platform that can be used for various applications, such as supply chain management. Its scalability and developer ecosystem make it ideal for industrial IoT applications. IOTA, on the other hand, exhibited the potential of providing secure transactions and payments. Although the different frameworks exhibited strong capabilities, we identified several issues that could affect the operations of their distributed ledgers. These include network congestion, vulnerability in smart contracts, and coordination dependency. The different frameworks exhibited various limitations and challenges. For instance, the performance degradation of Hyperledger Fabric due to its increasing network size and resource requirements can affect its scalability. On the other hand, vulnerabilities in its smart contract code can lead to security risks. IOTA's vulnerability in its coordinator system could affect its operations.

In order to overcome these issues, further studies and development are needed. Some of the possible solutions include improving smart contract security and formal verification, as well as reducing network congestion and improving consensus mechanisms. One of the most important factors that could affect the operations of IOTA's network is the coordination dependency. This issue could be addressed by exploring other consensus mechanisms. Besides the examined frameworks, other factors such as technological innovations and emerging trends can also contribute to the development of secure and resilient blockchain applications for IoT. Some of the techniques that can be used to protect the confidentiality of data include multi-party computation and zero-knowledge proofs. One of the most effective ways to improve the efficiency of an IoT network is by implementing off-chain scaling techniques, such as state channels and payment channels. This can help reduce the number of blocks sent and received by an organization. Hardware wallets and secure execution environments can also help protect the devices connected to the blockchain.

References

[1] Industry, "Blockchain — Internet of Things Applications : Opportunities," 2023.

[2] G. Dittmann and J. Jelitto, "A blockchain proxy for lightweight iot devices," Proc. - 2019 Crypto Val. Conf. Blockchain Technol. CVCBT 2019, pp. 82–85, 2019, doi: 10.1109/CVCBT.2019.00015.

[3] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "Orchestrating product provenance story: When IOTA ecosystem meets electronics supply chain space," Comput. Ind., vol. 123, p. 103334, 2020, doi: https://doi.org/10.1016/j.compind.2020.103334.

[4] M. J. Peregrina-Pérez, J. Lagares-Galán, and J. Boubeta-Puig, "Chapter 16 - Hyperledger Fabric blockchain platform," R. Pandey, S. Goundar, and S. B. T.-D. C. to B. Fatima, Eds. Academic Press, 2023, pp. 283–295.

[5] J. Andrews, M. Ciampi, and V. Zikas, "Etherless Ethereum tokens: Simulating native tokens in Ethereum," J. Comput. Syst. Sci., vol. 135, pp. 55–72, 2023, doi: 10.1016/j.jcss.2023.02.001.

[6] A. R. Mahlous and A. Ara, "The Adoption of Blockchain Technology in IoT: An Insight View," Proc. - 2020 6th Conf. Data Sci. Mach. Learn. Appl. CDMA 2020, pp. 100–105, 2020, doi: 10.1109/CDMA47397.2020.00023.

[7] U. Narayanan, V. Paul, and S. Joseph, "Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec," J. Ambient Intell. Humaniz. Comput., vol. 13, no. 2, pp. 769–787, 2022, doi: 10.1007/s12652-021-02929-z.

[8] A. Monrat, O. Schelen, and K. Andersson, "Performance Evaluation of Permissioned Blockchain Platforms," 2020 IEEE Asia-Pacific Conf. Comput. Sci. Data Eng. CSDE 2020, 2020, doi: 10.1109/CSDE50874.2020.9411380.

[9] V. Khetani, Y. Gandhi, S. Bhattacharya, S. N. Ajani, and S. Limkar, "INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Cross-Domain Analysis of ML and DL : Evaluating their Impact in Diverse Domains," vol. 11, pp. 253–262, 2023.

[10] Al-Barazanchi et al., "Blockchain-Technology-Based Solutions for IOT Security," Iraqi J. Comput. Sci. Math., vol. 3, no. 1, pp. 53–63, 2022, doi: 10.52866/ijcsm.2022.01.01.006.

[11] A. Alfa, J. K. Alhassan, O. M. Olaniyi, and M. Olalere, "Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions," J. Reliab. Intell. Environ., vol. 7, no. 2, pp. 115–143, 2021, doi: 10.1007/s40860-020-00116-z.

[12] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues," Cluster Comput., vol. 24, no. 1, pp. 37–55, 2021, doi: 10.1007/s10586-020-03137-8.

[13] N. Adhikari and M. Ramkumar, “IoT and Blockchain Integration: Applications, Opportunities, and Challenges,” Network, vol. 3, no. 1, pp. 115–141, 2023, doi: 10.3390/network3010006.

[14] Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, “Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review,” IEEE Access, vol. 10, no. November, pp. 122679–122695, 2022, doi: 10.1109/ACCESS.2022.3223370.

[15] Z. Rahman, X. Yi, S. T. Mehedi, R. Islam, and A. Kelarev, “Blockchain Applicability for the Internet of Things: Performance and Scalability Challenges and Solutions,” Electronics, vol. 11, no. 9, p. 1416, Apr. 2022, doi: 10.3390/electronics11091416.

[16] Benet, “IPFS - Content Addressed, Versioned, P2P File System,” pp. 2021–2022, 2014, [Online]. Available: http://arxiv.org/abs/1407.3561.

[17] Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in internet of things: Challenges and Solutions,” 2019 Int. Conf. Electron. Information, Commun., pp. 1–2, 2016, [Online]. Available: http://arxiv.org/abs/1608.05187.

[18] Song, J. Nang, and J. Jang, “Design of anomaly detection and visualization tool for iot blockchain,” Proc. - 2018 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2018, pp. 1464–1465, 2018, doi: 10.1109/CSCI46756.2018.00292.

[19] Minoli and B. Occhiogrosso, “Blockchain mechanisms for IoT security,” Internet of Things (Netherlands), vol. 1–2, pp. 1–13, 2018, doi: 10.1016/j.iot.2018.05.002.

[20] A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Futur. Gener. Comput. Syst., vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[21] H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente, “Towards secure and decentralized sharing of IoT data,” Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019, pp. 176–183, 2019, doi: 10.1109/Blockchain.2019.00031.

[22] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, “Blockchain-based Remote Patient Monitoring in,” pp. 87–91, 2019.

[23] Tseng, X. Yao, S. Otoum, M. Aloqaily, and Y. Jararweh, “Blockchain-based database in an IoT environment: challenges, opportunities, and analysis,” Cluster Comput., vol. 23, no. 3, pp. 2151–2165, 2020, doi: 10.1007/s10586-020-03138-7.

[24] R. A. Memon, J. P. Li, J. Ahmed, M. I. Nazeer, M. Ismail, and K. Ali, “Cloud-based vs. blockchain-based IoT: a comparative survey and way forward,” Front. Inf. Technol. Electron. Eng., vol. 21, no. 4, pp. 563–586, 2020, doi: 10.1631/FITEE.1800343.

[25] P. Patil, M. Sangeetha, and V. Bhaskar, “Blockchain for IoT Access Control, Security and Privacy: A Review,” Wirel. Pers. Commun., vol. 117, no. 3, pp. 1815–1834, 2021, doi: 10.1007/s11277-020-07947-2.

[26] Attkan and V. Ranga, “Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security,” Complex Intell. Syst., vol. 8, no. 4, pp. 3559–3591, 2022, doi: 10.1007/s40747-022-00667-z.

[27] S. S. Hameedi and O. Bayat, “Improving IoT Data Security and Integrity Using Lightweight Blockchain Dynamic Table,” Appl. Sci., vol. 12, no. 18, 2022, doi: 10.3390/app12189377.

[28] W. Liang and N. Ji, “Privacy challenges of IoT-based blockchain: a systematic review,” Cluster Comput., vol. 25, no. 3, pp. 2203–2221, 2022, doi: 10.1007/s10586-021-03260-0.

[29] Nehme, R. El Sibai, J. Bou Abdo, A. R. Taylor, and J. Demerjian, “Converged AI, IoT, and blockchain technologies: a conceptual ethics framework,” AI Ethics, vol. 2, no. 1, pp. 129–143, 2022, doi: 10.1007/s43681-021-00079-8.

[30] D. Ravi, S. Ramachandran, R. Vignesh, V. R. Falmari, and M. Brindha, “Privacy preserving transparent supply chain management through Hyperledger Fabric,” Blockchain Res. Appl., vol. 3, no. 2, p. 100072, 2022, doi: https://doi.org/10.1016/j.bcra.2022.100072.

[31] T. Ye, M. Luo, Y. Yang, K. R. Choo, and D. He, “A Survey on Redactable Blockchain: Challenges and Opportunities,” IEEE Trans. Netw. Sci. Eng., pp. 1–15, 2022, doi: 10.1109/TNSE.2022.3233448.

[32] M. Akhtar, D. R. Rizvi, M. A. Ahad, S. S. Kanhere, M. Amjad, and G. Coviello, “Efficient data communication using distributed ledger technology and iota-enabled internet of things for a future machine-to-machine economy,” Sensors, vol. 21, no. 13, pp. 1–38, 2021, doi: 10.3390/s21134354.

[33] S. Shalaby, A. A. Abdellatif, A. Al-Ali, A. Mohamed, A. Erbad, and M. Guizani, “Performance Evaluation of Hyperledger Fabric,” 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, no. April, pp. 608–613, 2020, doi: 10.1109/ICIoT48696.2020.9089614.

[34] C.-C. Chou, N.-C. Richard Hwang, C.-W. Li, T. Wang, and Y.-Y. Wang, “Implementing a multichain framework using hyperledger for supply chain transparency in a dynamic partnership: A feasibility study,” Comput. Ind. Eng., vol. 175, p. 108906, 2023, doi: https://doi.org/10.1016/j.cie.2022.108906.

[35] De Vries, “Cryptocurrencies on the road to sustainability: Ethereum paving the way for

Bitcoin," Patterns, vol. 4, no. 1, p. 100633, 2023, doi: 10.1016/j.patter.2022.100633.

[36] Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," J. Parallel Distrib. Comput., vol. 134, pp. 180–197, 2019, doi: 10.1016/j.jpdc.2019.08.005.

[37] W. F. Silvano and R. Marcelino, "Iota Tangle: A cryptocurrency to communicate Internet-of-Things data," Futur. Gener. Comput. Syst., vol. 112, pp. 307–319, 2020, doi: https://doi.org/10.1016/j.future.2020.05.047.

[38] L. Vishwakarma and D. Das, "SCAB - IoTA: Secure communication and authentication for IoT applications using blockchain," J. Parallel Distrib. Comput., vol. 154, pp. 94–105, 2021, doi: https://doi.org/10.1016/j.jpdc.2021.04.003.

[39] Sahoo, D. K. . (2021). Improved Routing and Secure Data Transmission in Mobile Adhoc Networks Using Trust Based Efficient Randomized Multicast Protocol. Research Journal of Computer Systems and Engineering, 2(2), 06:11. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/25

[40] Aoudni, Y., Donald, C., Farouk, A., Sahay, K. B., Babu, D. V., Tripathi, V., & Dhabliya, D. (2022). Cloud security based attack detection using transductive learning integrated with hidden markov model. Pattern Recognition Letters, 157, 16-26. doi:10.1016/j.patrec.2022.02.012