International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 1 (2025)
https://doi.org/10.31436/ijpcc.v11i1.526

Surveys on the Security of Ethereum and Hyperledger Fabric Blockchain Platforms

Nik Nor Muhammad Saifudin Nik Mohd Kamal, Safwah Afiqah, Sara Khadeja, Aliya Nasuha, Wan Muhammad Haziq Nur Iman Wan Mohd Azman, Wan Zul Irfan Wan Zulkifli, Wan Shafiq Aiman Wan Anuar, Muhammad Faizul Isyraf Md Nazri, Ahmad Anwar Zainuddin*
Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Gombak, Malaysia.

*Corresponding author anwarzain@iium.edu.my

(Received: 16th December, 2024; Accepted: 29th December, 2024; Published on-line: 30th January, 2025)

Abstract—Ethereum and Hyperledger are two popular and well-known block chain platforms which represent two kinds of application differentiation. Ethereum is a decentralized platform that also allows DApps to operate on it; many of the conditions for performing functions on Ethereum's blockchain do not require permission to be granted, but smart contracts are available. On the other hand, the Hyperledger Fabric, an enterprise grade blockchain solution, provides the permission to access, update, and apply scalability, privatization, and mandatory access control mechanisms. Due to the decentralized nature and the capacity of performing smart contracts using Ethereum Virtual Machine (EVM), it has been used in a number of areas across the world in financial transactions and DApp. Hyperledger fabric, on the other hand, is pursuant to the permissioned network standards and is centred on providing the set of components that suffice the requirement of an enterprise thereby making it easier for the organization to build a blockchain, which is both highly scalable and security conscious. Several studies have explored Ethereum and Hyperledger Fabric in various contexts. From these studies, it explains how blockchain has the potential in increasing volume in various areas while enhancing its characteristics such as, openness, origin and audibility. Analysing the concrete features of the Ethereum and Hyperledger Fabric platforms, it is almost obligatory for the companies interested into the implementation of the blockchain technology to understand the possibilities offered by one system and the drawbacks some complexity or singularity of the other. That is why, the features of each platform are distinctive and could be utilized for the development of business processes in specific spheres when designing problem-solving approaches.

Keywords— IoT, Blockchain, Ethereum, Hyperledger, Security, Interoperability

I. Introduction

Ethereum and Hyperledger Fabric are two prominent blockchain platforms that have significantly impacted the landscape of decentralized technologies. Ethereum, often considered a second-generation blockchain platform, stands out for its open and decentralized nature, enabling the development of Decentralized Applications (DApps) [1] . It has become a widely used financial application platform, with its native cryptocurrency, Ether, being one of the largest cryptocurrencies in terms of market capitalization [2] . Ethereum's smart contracts are tamper-proof, offering robust protection against attacks that aim to manipulate application execution flows [3].

On the other hand, Hyperledger Fabric is recognized for its focus on enterprise applications, providing a secure and scalable environment for executing smart contracts within secured Docker containers [4] . It emphasizes immutability, transparency, and cryptographic verifiability without the need for a single point of trust, thanks to its decentralized architecture [5]. Hyperledger Fabric has been explored for applications like resilient load balancing, demonstrating its potential for various use cases beyond traditional [6].

Both Ethereum and Hyperledger Fabric have been subjects of security assessments and surveys, highlighting the importance of understanding their vulnerabilities, attacks, and defences [7]. Researchers have delved into the security challenges faced by major blockchain applications, including Ethereum and Hyperledger, emphasizing the need for robust security and privacy techniques to safeguard blockchain-based systems [8]. Additionally, studies have focused on detecting fraudulent schemes like Ponzi schemes implemented as smart contracts on Ethereum, showcasing the importance of ensuring the integrity of blockchain applications [7].

In conclusion, Ethereum and Hyperledger Fabric represent two distinct yet influential blockchain platforms, each catering to different use cases and industries. While Ethereum excels in decentralized applications and cryptocurrency transactions, Hyperledger Fabric shines in enterprise applications and secure smart contract execution.

Understanding the nuances of these platforms is crucial for harnessing the full potential of blockchain technology in various domains.

This paper employs a systematic approach to explore the development and assessment of blockchain platforms for secure and efficient applications. Section I covers the background, fundamental concepts, and objectives of the research. Section II examines previous studies on blockchain technology, with a focus on its evolution, applications, and associated challenges. Section III delves into blockchain technology by highlighting the main features and architectures of Ethereum and Hyperledger Fabric. Section IV analyses the implications, comparisons, and potential applications of these platforms. Lastly, Section V concludes the study by summarizing its key findings and contributions to the blockchain field.

II. Literature Review

Several studies looked at blockchain within the context of IT; they examined security and compatibility of leading blockchains such as Ethereum and Hyperledger Fabric. His previous work [9] provides an assessment of one proposed use of blockchain for PHR, converses more on the usage of specific reference platforms like Ethereum and Hyperledger in related works. Similarly, [10] discussed permissioned DP block chain for private data sharing in Industrial IoT employing encryption strategies using Hyper ledger fabric to manage privateness concerns seasoned at consensus level.

[11] has outlined a reference model of supporting a Hyperledger Fabric to adopt which it asserted the need to deploy an EHR sharing system based on the Hyperledger composer. In addition, [12] utilized Hyperledger Fabric's simulation to determine the detailed aspects of performance and aspects of it.

Interoperability has also been aimed at in the blockchain sphere by employing interoperability solutions. [13] utilized yet another conventional gateway- based architecture for DLT cross boarding and claimed the message specification and created a concrete implementation on Hyperledger Fabric, and Ethereum. Furthermore, [14] also expounded on the actualization of the coupling process between the Ethereum, Hyperledger Fabric and the Tender mint blockchain via inter Blockchain communication.

More specifically in the field of healthcare several authors as discussed in this paper have used the blockchain for privacy-preserving frameworks. The following novels were also recently published: [15] describe a privacy-preserving health care system based on a blockchain implementation, known as Hyperledger Fabric; [16] discuss Health chain as use of blockchain-based solutions anonymous EHRs through which blockchain solutions can be adopted.

These research papers in combination with each other enable to gain precious information about several methods in security, interoperability and privacy of blockchain platforms, along with potential solutions that could enhance efficiency and effectiveness of blockchain systems.

TABLE I
COMPARATIVE ANALYSIS OF BLOCKCHAIN APPLICATIONS IN VARIOUS DOMAINS.

Articles	Key Findings	Supporting Evidence	Strength and Limitations	Significance and Implications
[2]	Proposed a method for tracking Ethereum transactions using a temporal-amount snapshot multigraph approach.	Theoretical framework and validation through simulations.	Strength: Innovative tracking method. Limitation: Requires further real-world validation.	Enhances the ability to trace transactions in the Ethereum network, improving security and transparency.
[3]	Reviewed upgradeable smart contract patterns based on the Open Zeppelin technique.	Literature review of smart contract patterns.	Strength: Focuses on upgradeability. Limitation: Limited to Open Zeppelin patterns.	Provides insights into the design of more flexible and maintainable smart contracts.
[4]	Developed a recommender system leveraging blockchain and deep learning for reusing and recycling.	System design and empirical validation.	Strength: Integrates blockchain and AI. Limitation: Specific to recommender systems.	Demonstrates the application of blockchain and AI in creating efficient and secure recommender systems.
[17]	Explored blockchain applications, challenges, and research opportunities in supply chain operations.	Literature review and analysis of supply chain applications.	Strength: Broad coverage of supply chain issues. Limitation: Lacks empirical validation.	Provides a roadmap for future research and applications of blockchain in supply chain management.

[18]	Investigated blockchain's potential in biomedical and healthcare applications.	Review of biomedical applications.	Strength: Early exploration of blockchain in healthcare. Limitation: Outdated, requires updates with new findings.	Sets the foundation for blockchain applications in biomedical and healthcare sectors.
[19]	Explored the integration of blockchain and AI in e- health applications.	Review and analysis of e-health applications.	Strength: Combines blockchain with AI. Limitation: Specific to e-health applications.	Highlights the synergies between blockchain and AI in enhancing e-health services.
[20]	Proposed a blockchain-based architecture for managing distributed renewable energy resources.	Gap analysis and proposed architecture.	Strength: Practical application in energy management. Limitation: Requires real-world validation.	Enhances renewable energy management through a blockchain-based approach.
[21]	Comprehensive survey on the evolution, architecture, and security of blockchain technology.	Literature review and analysis.	Strength: Broad and comprehensive coverage. Limitation: High-level overview, lacks specific focus.	Offers a detailed overview of blockchain's evolution, architecture, and security aspects.
[22]	Surveyed blockchain applications in business and finance in Vietnam.	Case studies and literature review.	Strength: Specific regional focus. Limitation: May not generalize globally.	Provides insights into how blockchain is being adopted in business and financial sectors in Vietnam.
[23]	Proposed a DNS cache resources trusted sharing model based on consortium blockchain.	System design and validation through simulations.	Strength: Practical DNS sharing model. Limitation: Requires further scalability testing.	Enhances the security and reliability of DNS cache resource sharing through a consortium blockchain model.
[24]	Surveyed various consensus mechanisms used in consortium blockchains.	Literature review and comparative analysis.	Strength: Comprehensive survey of consensus mechanisms. Limitation: General overview, lacks specific focus.	Provides a detailed comparison of different consensus mechanisms for consortium blockchains.
[25]	Proposed a consortium blockchain framework for remote health monitoring.	System design and case study analysis.	Strength: Specific focus on remote health monitoring. Limitation: Needs real-world validation.	Enhances the reliability and security of remote health monitoring systems through consortium blockchain.
[26]	Proposed a service for immutable log storage on both private and public blockchains.	System design and theoretical analysis.	Strength: Versatile log storage solution. Limitation: Needs practical implementation and testing.	Provides a framework for secure and immutable log storage across different blockchain platforms.
[27]	Reviewed various consensus algorithms used in blockchain technology.	Literature review and comparative analysis.	Strength: Broad overview of consensus algorithms. Limitation: High-level review, lacks in-depth analysis.	Provides a comprehensive overview of consensus algorithms, guiding future research and development efforts.
[28]	Reviewed privacy-preserving technologies in blockchain systems.	Literature review and comparative analysis.	Strength: Focus on privacy- preserving techniques.	Provides insights into various privacy-preserving techniques, guiding the development

			Limitation: Primarily theoretical, needs practical applications.	of more secure blockchain systems.
[29]	Developed a web archiving system that preserves content integrity using blockchain.	System design and empirical validation.	Strength: Practical web archiving solution. Limitation: Focused on web content, needs broader application testing.	Enhances the integrity and reliability of web archiving systems through blockchain technology.
[30]	Explored the use of blockchain and smart contracts for managing higher education records in Brazil.	System design and case study analysis.	Strength: Practical application in education. Limitation: Focused on a specific use case.	Demonstrates the potential of blockchain in improving the management and security of higher education records.
[31]	Proposed a high-performance hybrid blockchain system for traceable IoT applications.	System design and empirical validation.	Strength: Practical IoT application. Limitation: Needs further scalability testing.	Enhances the traceability and performance of IoT applications through a hybrid blockchain approach.
[32]	Proposed an enhanced method for detecting P2P botnets through network-flow level community behaviour analysis.	Theoretical framework and empirical validation.	Strength: Effective botnet detection method. Limitation: Needs further real-world validation.	Improves the detection and mitigation of P2P botnets in network systems.
[33]	Analysed threats and security issues in mobile peer-to-peer networks.	Threat analysis and evaluation framework.	Strength: Detailed threat analysis. Limitation: Specific to mobile P2P networks.	Provides a comprehensive threat analysis for securing mobile peer-to-peer networks.
[34]	Developed a decentralized electricity market model with prosumer-centric coordination and grid security.	System design and simulation validation.	Strength: Practical electricity market model. Limitation: Needs real-world implementation.	Enhances the coordination and security of decentralized electricity markets through blockchain technology.
[35]	Proposed a new chaotic encryption model using diffractive techniques.	Theoretical development and validation through simulations.	Strength: Innovative encryption model. Limitation: Needs practical implementation.	Introduces a new encryption model that enhances data security through chaotic techniques.
[36]	Developed a data integrity auditing mechanism for secure cloud storage using Hyperledger Fabric.	Designed and tested auditing mechanisms; empirical validation with performance metrics.	Strength: Improved data integrity mechanisms. Limitation: Focus on cloud storage, may not address other security concerns.	Enhances the security of cloud storage systems using Hyperledger Fabric, ensuring data integrity.
[37]	Investigated the feasibility of Proof of Authority as a consensus protocol model.	Theoretical analysis and simulation validation.	Strength: Focus on Proof of Authority. Limitation: Needs real-world testing.	Provides insights into the feasibility and efficiency of Proof of Authority as a consensus protocol.
[38]	Empirical analysis of Ethereum's gas mechanism and its implications for network performance.	Collected and analysed data on gas usage in Ethereum.	Strength: Empirical data analysis. Limitation: Focus on gas mechanism, may not address other aspects of Ethereum performance.	Offers insights into the efficiency and potential improvements of Ethereum’s gas mechanism.

https://doi.org/10.31436/ijpcc.v11i1.526

[38]	Proposed a secure and efficient Delegated Proof of Stake consensus algorithm with a downgrade mechanism.	Theoretical development and empirical validation.	Strength: Innovative consensus algorithm. Limitation: Needs further practical validation.	Enhances the security and efficiency of Delegated Proof of Stake consensus algorithms.
[39]	Developed a node selection algorithm for consortium blockchains using a genetic method based on PBFT.	System design and simulation validation.	Strength: Effective node selection method. Limitation: Specific to PBFT consensus.	Improves node selection efficiency and reliability in consortium blockchains using a genetic algorithm.
[40]	Proposed a resource slicing model for blockchain consensus in real-time distributed energy trading.	System design and simulation validation.	Strength: Innovative consensus model. Limitation: Needs further real-world validation.	Enhances the efficiency and reliability of blockchain consensus in energy trading systems.
[41]	Explored blockchain's role in facilitating inter-organizational collaboration, specifically in healthcare during COVID-19.	Case studies of healthcare providers using blockchain for collaboration during the pandemic.	Strength: Timely and relevant case studies. Limitation: Focused on a specific use case, may not generalize.	Demonstrates the potential of blockchain for enhancing collaboration in crisis situations.
[42]	Proposed a formal model for ledger management systems based on contracts and temporal logic.	Developed formal models and provided theoretical proofs.	Strength: Strong theoretical foundation. Limitation: Lack of practical implementation and testing.	Provides a theoretical basis for developing more robust ledger management systems.
[43]	Conducted a systematic review of security vulnerabilities in Ethereum smart contracts.	Analysed various security vulnerabilities through literature review.	Strength: Comprehensive overview of vulnerabilities. Limitation: Lacks new empirical data.	Provides a detailed understanding of common security vulnerabilities in Ethereum, guiding future security improvements.
[44]	Developed visualization techniques for Ethereum's peer-to-peer network topology.	Utilized network analysis tools; visualized Ethereum's P2P network.	Strength: Improved understanding of P2P network structure. Limitation: Visualization focused, may not address other network issues.	Enhances understanding of Ethereum's network structure, aiding in network optimization and security.
[45]	The study introduces a system combining blockchain and machine learning to improve cybersecurity by detecting intrusions more accurately and ensuring data integrity.	The system uses blockchain for secure data sharing and machine learning to identify threats. Simulations validate its performance.	Strengths: Enhanced detection accuracy, robust data integrity, collaborative threat detection. Limitations: Computational complexity, scalability concerns.	This hybrid IDS model offers a promising solution for securing sensitive data and detecting cyber threats in real-time, potentially transforming cybersecurity practices.
[46]	Developed methods for detecting illicit accounts on the Ethereum blockchain.	Utilized machine learning techniques; tested on Ethereum transaction data.	Strength: Advanced detection techniques. Limitation: Requires large datasets and may not detect all types of illicit activities.	Improves the ability to detect and mitigate fraudulent activities on the Ethereum blockchain.
[47]	Evaluated the effect of the uncle block mechanism on selfish and stubborn mining in Ethereum.	Theoretical analysis and simulations of uncle block effects.	Strength: Addresses a specific mining strategy issue. Limitation: Primarily theoretical, requires empirical validation.	Provides insights into improving Ethereum's mining strategies and security.

[48]	Proposed a blockchain-based architecture for secure IoT-based health monitoring systems.	Designed and tested the architecture; empirical evaluation in health monitoring scenarios.	Strength: Practical application in health monitoring. Limitation: Specific to health monitoring, may not generalize.	Enhances the security and reliability of health monitoring systems using blockchain technology.
[49]	The article discusses the development of AppxChain, a platform designed to facilitate application-level interoperability among different blockchain networks. It argues that seamless communication and data exchange are essential for enhancing the scalability and utility of blockchain technology.	The article provides insights into AppxChain's architecture and functionalities, demonstrating its ability to enable communication between various blockchains such as Ethereum, Hyperledger Fabric, and Binance Smart Chain. The methods used likely include descriptive explanations of AppxChain's features and potential use cases.	Strength:AppxChain's innovative approach focuses on application-level interoperability, enhancing collaboration and innovation in blockchain applications. Limitation: Technical challenges may arise in implementing and maintaining interoperability across diverse blockchain networks.	The article's findings have significant implications for the future of blockchain technology, as AppxChain's interoperability features can mitigate fragmentation, improve scalability, and encourage cross-platform collaboration. These outcomes could accelerate innovation and utility in industries relying on blockchain applications.
[50]	The article reviews the concept of Digital Twin (DT), highlighting its definitions, key characteristics, and various applications across industries. It emphasizes the potential of DT in improving system design, monitoring, and maintenance.	The authors conduct a comprehensive literature review to classify and analyse existing DT definitions, applications, and design frameworks.	Strengths: Broad coverage of DT concepts, identification of key characteristics, extensive application examples. Limitations: Evolving field, varying definitions may cause inconsistencies.	This survey provides a foundational understanding of DT, aiding researchers and practitioners in leveraging DT for innovative solutions in system optimization and predictive maintenance.
[51]	Presented Hyperledger Fabric as a distributed operating system for permissioned blockchains.	In-depth architectural analysis of Hyperledger Fabric.	Strength: Comprehensive architectural overview. Limitation: May be too technical for non-specialists.	Offers a detailed understanding of Hyperledger Fabric's architecture, aiding developers and researchers.
[52]	Reviewed the application of Hyperledger Fabric in IoT contexts.	Surveyed existing literature and case studies on Hyperledger Fabric implementations in IoT.	Strength: Comprehensive literature review. Limitation: Limited new empirical data.	Provides a broad overview of how Hyperledger Fabric can be utilized in IoT, guiding future implementations.
[53]	Proposed a blockchain-based framework for medical image sharing and critical-results notification using Hyperledger Fabric.	Developed and tested a framework; empirical testing in medical imaging scenarios.	Strength: Practical application in healthcare. Limitation: Specific to medical imaging, may not generalize.	Demonstrates the practical utility of Hyperledger Fabric in securely sharing medical data.
[54]	Proposed a private and trustworthy lending model using Hyperledger Besu.	Designed a new lending model; empirical validation in financial scenarios.	Strength: Practical application in finance. Limitation: Specific to lending, may not generalize to other financial services.	Enhances the security and trustworthiness of financial lending services using blockchain.

[55]	Developed an AI-enabled consensus protocol for blockchain-based IoT networks.	Applied AI techniques to consensus protocols; tested in IoT scenarios.	Strength: Innovative use of AI for consensus. Limitation: Computationally intensive, requires significant resources.	Improves the efficiency and security of consensus protocols in blockchain-based IoT networks.
[56]	The article proposes a framework for efficient clinical data sharing using blockchain technology to ensure data security, integrity, and interoperability.	The framework is validated through a combination of theoretical analysis and simulation experiments. It involves the use of blockchain to create a decentralized and immutable ledger for clinical data transactions.	Strengths: Enhanced data security and privacy, improved interoperability, and reliable data sharing. Limitations: High computational costs and potential scalability issues.	This framework can revolutionize clinical data sharing by providing a secure, transparent, and efficient method for managing patient records, potentially improving healthcare outcomes.
[57]	The article explores how integrating multiple blockchain ledgers can improve control and security in IoT systems. It discusses the use of interledger technologies to facilitate secure and efficient interactions between different blockchain networks.	The authors propose a framework for combining various blockchain ledgers, emphasizing interoperability and security. They validate their approach through use case scenarios and performance evaluations.	Strengths: Enhanced security, improved control, and flexibility in IoT applications. Limitations: Potential complexity in implementation, need for robust interoperability standards.	This approach can significantly enhance IoT systems' security and efficiency by allowing better control over multiple interconnected blockchain networks.
[58]	The article discusses the development of a blockchain-assisted patient-owned system for electronic health records (EHRs), emphasizing the potential benefits of blockchain technology in enhancing data security, privacy, and patient control over their health information.	The authors likely conducted a comprehensive review of existing literature on blockchain applications in healthcare and electronic health records. They may have also presented case studies or prototypes demonstrating the feasibility and effectiveness of their proposed system.	Strength: The article's strength lies in its innovative approach to leveraging blockchain technology to empower patients with greater ownership and control over their EHRs, potentially improving data integrity and patient outcomes. Limitations: Potential challenges may include technical complexities in implementing blockchain- based EHR systems on a large scale, as well as regulatory and privacy concerns that need to be addressed for widespread adoption.	The findings of this article have significant implications for the healthcare industry, as a blockchain-assisted patient-owned EHR system could enhance data security, privacy, and patient engagement. This could lead to improved healthcare outcomes, reduced medical errors, and increased trust between patients and healthcare providers.
[59]	The article surveys blockchain interoperability, highlighting past efforts, current methods, and future trends. It identifies three main categories: cryptocurrency-directed	The authors reviewed 332 documents, analysing 80 in detail to classify and discuss various interoperability approaches.	Strengths: Comprehensive overview, systematic classification. Limitations: Fragmented knowledge, evolving standards.	This work provides a foundation for future research, emphasizing the importance of interoperability for blockchain technology's growth.

	approaches, blockchain engines, and blockchain connectors.			
[60]	Improved key management in LoRaWAN networks using permissioned blockchain.	Developed a blockchain-based key management scheme; tested in LoRaWAN scenarios.	Strength: Enhances security in IoT networks. Limitation: Specific to LoRaWAN, may not generalize to other networks.	Strengthens IoT network security through improved key management techniques.

III. Overview of Blockchain Technology

A. Functioning

In Figure 1, explained the foundation of blockchain was laid using Bitcoin in 2009, but a lot of changes have been observed in the modern blockchain platforms that provide secure, transparent and efficient solutions in various domains. They discovered that in the context of the supply chain logistics of blockchain technology has been considered as an opportunity to advance the opportunity and manage the challenges and new research areas [17]. Therefore, it has found application in supply chain management solving areas because it enhances visibility, audibility, and security of products in supply chains [18].

In healthcare, the application of the blockchain technology is where it can used to observe the future that it would bring into management of data and its security and ability to interconnect. Advantages in biomedical or health care domains include better security of information, better documentation and relative higher levels in terms of database handling as against normal databases [18]. Further, and as discussed briefly above, blockchain has been considered for IoT as a solution for the creation of a distributed ledger that could upgrade the communication and information exchange readily [61].

An effort has been made to contextualize blockchain in e-Health cooperated with AI performance, opening possibilities of enabling effective and patient-centric healthcare. The study found out that problems like scalability, interoperability and regulatory issues are some of the concerns that may hinder large scale implementation [19]. However, overcoming these challenges can open numerous opportunities for using blockchain technology as a decentralized and safe platform for various purposes, for instance, supply chain management in the healthcare sector, collaborative and project-based healthcare initiatives, and state-supported patient-oriented projects [62].

In conclusion, the use of blockchain technology is still advancing and penetrating essence to various industries to come up with solution-facilitating solutions. Blockchain must be warmly welcomed for its ability to bring innovative disruptive solutions to institutions, improve managing data systems, and advance collaborative societal causes and missions.

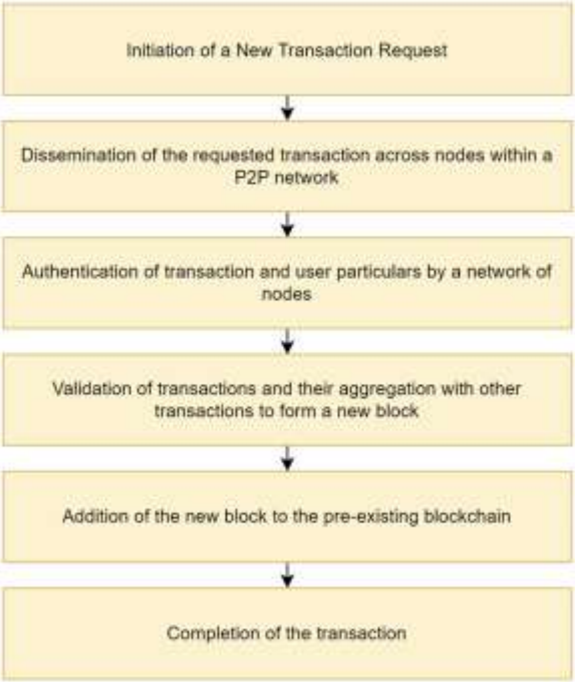
Initiation of a New Transaction Request
Dissemination of the requested transaction across nodes within a P2P network
Authentication of transaction and user particulars by a network of nodes
Validation of transactions and their aggregation with other transactions to form a new block
Addition of the new block to the pre-existing blockchain
Completion of the transaction

Fig. 1 An overview of blockchain flow

B. Classification of Blockchain Technology

1) Public Blockchain

In Figure 2, explained the simplified blockchains or centralized blockchains are some of the original concepts of blockchains that allow the visitors to the same system to have full control over the chain. They are the anonymous messaging type where no one requires authorization to subscribe, provide/forward information or endorse the transactions. Every transaction that will take place within the network has to be well understood by other people within that same network, since as mentioned earlier, within public blockchains everyone and anything is transparent and therefore, has to be answerable.

In the words of [20], the term is used to repeat the fact that it is possible to open it to the public and they congregate around features that are public as well as opened. Similarly, [21] has also discussed the differentiation between public and private blockchains in terms of the fact that in public blockchain everyone has the ability to join the network of the respective blockchain network and even participate in the process of validation of the blocks in order to make consensus along with decentralizing the network.

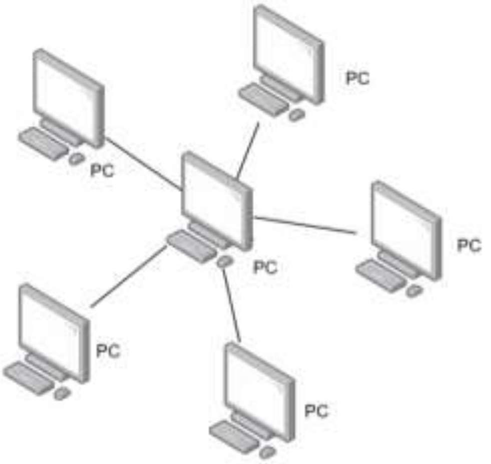

Fig. 2 Example of Public Blockchain

In addition, [22] continue with the elaboration on the features of the permission less or public blockchains they argue that they are clear records meaning that the records are accessible by anyone and one can join the network at any given time. This open-accessing ensures that the blockchain is more secure and less likely to be an entry point for hackers to attack as more people will be adding to the size and complexity of the book.

Hence the adoption of public blockchains in the pursuit of these goals of transparency, decentralization and most importantly, trust within the blockchain participants. The open and permission less nature of two layers demonstrates that it is possible to facilitate a high number of participants to be involved in consensus to validate a number of different transactions and in the process enhancing the security of the entire Blockchain solution.

2) Private Blockchain

In Figure 3, explained the other categories of DLT may incorporate private distributed ledgers also known as enterprise blockchains and compliance with lawful standards including data security regulation GDPR [63]. The interference of third parties on the transactions or records which they have no right to do so is also true with private key blockchains since there are no governing bodies or owners who are always hungry to manipulate or delete entries on the chain. This kind of control is extremely stringent because only particular consensus algorithms can be employed, and the model will function strictly as wished by the governments behind it.

Moreover, except for various or public blockchains, the values of data are only accessible to members/fixed or selected only [64]. Regarding the node access feature in the private blockchain, only specific individuals who are allowed to gain access to the platform are the only ones who can access it, and this can be considered as efficient in terms of limiting the number of nodes that can access a given system. In contrast to all such traditional electronic databases this access prevents or restricts the dissemination of information within the blockchain network that provides a higher level of protection for the data that is being exchanged in the network; this is acceptable for those cases only where such exchange in the information is limited only to only a few parties.

By extension, permission-based or private ledgers involve a limited and confined network with well-established gates or walls for the players. These blockchain networks have fairly well-developed self-organization and anonymity that are necessary and sufficient for applications that allow limited data exchange and compatibility with different legal rules and requirements.

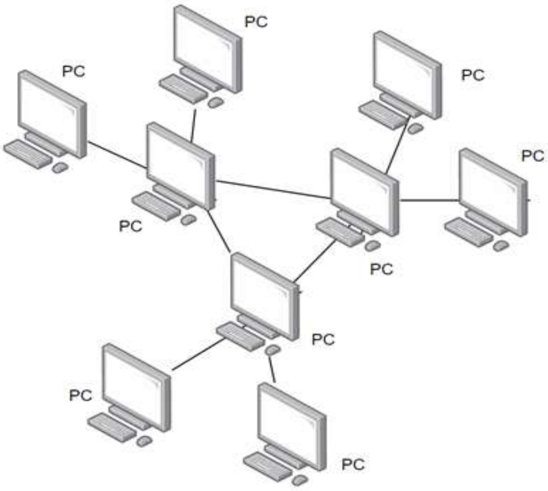

Fig. 3 Example of Private Blockchain

3) Consortium Blockchain

In Figure 4, explained the consortium block chain also known as an enterprise block chain is a type of private block chain whereby the block chains are developed with the collaboration of several organisations in a consortium manner. To some extent, these blockchains are open, enabling crossover between the public and private blockchains although not exactly [65]. Finally, in consortium blockchains people can join the participate only in case they belong to the consortium and the structure that defines the blockchain contains read, write, or participating permissions according to the rules of the consortium [23]. Such blockchains are often founded on decisions by some number of preselected clients from these organizations with consensus being the agreed choice. The overall goal of consortium blockchains is that, while some other set of organizations that are very relevant in the context of the given consortium and at the same time sufficiently decentralized, achieve some value added by cooperation. This notion called as 'partial decentralization' explains consortium blockchains in that only a few stakeholders manage the network [23]. Compared to the public blockchain, the consortium does not have the problem of supplying a resource that would support a demanding global consensus protocol [24].

All nodes are known and selected in a consortium Blockchain which greatly reduces the risk and opens up trusted and viable partnerships [25]. These blockchains are also similar to the public blockchains with a catch in which only the entered set of nodes involves the consensus part [26]. Thus, even though it remains unclear whether consortium blockchains will eventually be recognized and adopted on the global level, it becomes apparent that they seem to be more advantageous when it comes to the range of potential uses compared to private blockchains [27].

Therefore, consortium blockchains provide a consensus of the middle ground between the public and private distribution and the users with limited access to the blockchain database while making decentralization and transparency applicable in the consortium scenario.

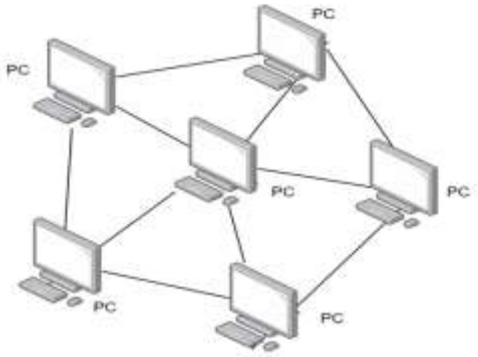

Fig. 4 Example of Consortium Blockchain

C. Classification of Blockchain Technology

Security is the immunization process given in the centre of the blockchain technology to safeguard against threats like unauthorized access, leakage of information, and unwanted revelation of privacy. It is also worth to emphasize that blockchain systems are developed targeting for many security aspects that potentially could help to protect from IT threats and risks.

According to [28], for the blockchain systems to have a reasonable level of security they need to have the following features: Randomness, the system cannot be replaced or modified, there are different users with different pseudonyms, the system is consistent, and the system is immune to DDoS and double spending.

Additionally, [29] proposed that blockchain has been considered to be a high-quality security system owing to its distinct security features, reviewing the security qualities that make it highly useful in averting cyber-risk and ensuring veracity of records.

Furthermore, [30] have supported that transactions within block-chain environment are secure, can always be relied on, unmodifiable thus could always be traced making these security provisions vital for facilitating the solidity and openness of block-chain activities.

Furthermore, [31] have pointed towards the fact private keys are essential to make Blockchain secure as it machines against identify forging attack stressing that those key must need to be secured so that nobody without permission can alter the transaction in the Blockchain ledgers.

Thus, it can also offer a number of protection mechanisms such as, data authenticity meaning that data within block chain cannot be manipulated, parties' immunity to deny having conducted a certain transaction, where necessary, parties' immunity to keep certain transaction information secret, bio availability, where necessary, and secure storage and encryption as well as access to keys which are evidence of existence of a secure platform to store data or perform a transaction.

1) P2P network

Security in P2P networks ensures message confidentiality, integrity, and accessibility. Recent studies address threats from physical addressing and highlight encryption's role in mitigating vulnerabilities, with growing interest in decentralized P2P network management.

[32], discuss on the P2P network structure and emphasize the use of physical addressing threats on the basis of diversification of physical network P2P connections. [33], also described a comprehensive security model of the impact of web threats that may be experienced by mobile P2P networks, limitations and types of network attacks that might be experienced as well as the measures such as encryption.

Further, it contains an overview of the still very much nascent research area of P2P-based Network Management (P2PBNM) with a clear focus on the use of P2P technology to further decentralize and secure basic network management architecture. [34], emphasize the importance of the grid security measures to the peer-to-peer (P2P Electricity Market) where the prosumers will be organized through the security measures deemed as being reflected in the tariff-based security and product discrimination.

Security in P2P networks is essential to mitigate threats arising from their decentralized and anonymous nature. Consequently, with the open-to-all all security for a P2P network in combination with other unification measures, as well as encryption and other threat avoidance measures, the risk of the overall range of threats in the form of cyber threats may be reduced to a negligible level, including through the regulation of the provision of access to the network.

2) Cryptography

Cryptographic security ensures that data is immutable and accessible only to authorized users, while verifying the authenticity of the information. Only a few of them are recent and they attempted to give some information on a variety of aspects related to security features and employments of cryptography.

[35], The authors employed the use of diffractive encryption as a subset of the chaotic encryption model and regarding diffuse sensitive issues pointed out the problems associated with the identification of initial conditions and control parameters and noted the essential feature of key sensitivity within the area of cryptology. [36] indicated that agility, decentralization, honesty, and verifiability were the four core values promoted by blockchain and cryptography.

In [66], the authors provided the assessment of the security aspects concerning quantum cryptography, and concerning the given work, the major focus had been paid to the understanding of the paradigms such as unconditional security and measurability of the Quantum Cryptography technique. [67], presented a new secret sharing encryption method which is based on the polarization sample feature, and proved that the current method was more secure and less complex in decrypting the encrypted information.

3) Smart contract

Certain functions must be coded into the smart contracts to allow specific types of transactions to occur while at the same time maintaining the security and secrecy of the transaction. The studies carried out in the past few years have brought about the following main areas that focus on aspects of security in smart contracts.

[68], defined the necessity of creating high-quality, efficient, and high-security codes while designing smart contracts because it is connected with the feature of the impossibility of alteration of the developed software codes after distribution on the blockchain net. Another thing that scholars [69] said is that there is a need to capture the international dimension in the dance of smart contract security and appears to be urging those who analyse smart contracts to have a broad view of contracts' flaws and lapses.

Some other works that are related to security aspects of quantum cryptography include other works that discuss the same or related issues. [70], discussed the question of unconditional security of quantum cryptography and the problem of making the eavesdropper's presence recognizable to enhance the degree of security protection. This is how a new polarization-based secret sharing encryption also featured in [71], adding extra security as well as a less complicated process of decryption, was created.

In other words, the security characteristics of smart contracts involve the quality of the smart contract code, international security issues, no direct reliance on the external environment, and a very complex algorithm to secure the datatype and transaction data to minimize the risks of the transaction.

4) Blockchain Consensus Algorithms

Consensus algorithms are the core facilitators of blockchains' reliability, security, and operational performance. [37] discusses the applicability of PoA as the consensus making protocol model to solve consensus issue in decentralized computing systems with assurance of correctness and security of the system. [38] also talk about the Delegated Proof of Stake with Downgrade as one of the safe and effective consensus algorithms of the blockchain network, mentioning that it's important to note that consensus algorithms are subjected to changes to fit the new needs.

[39] have developed the node selection algorithm based on genetic method in consortium blockchains that adopted Practical Byzantine Fault Tolerance (PBFT), another evolution in consensus mechanism. Further, [40] gives the real-time DE trading CRSM model to illustrate how consensus resource slicing greatly influences the blockchain system efficiency because of the consensus algorithms.

Therefore, it can be understood that consensus algorithms in Blockchain are critical for determining the nodes' consensus as well as security, reliability, and efficiency of Blockchain networks.

5) Power of Work (PoW)

The basic model used in many blockchains to check transactions and to add new blocks to the chain is Proof of Work consensus method. Pow assigns miners to solve complicated mathematical problems, hashes, related to the transaction addition to the blockchain. PoW algorithms make use of a difficult hash function, taking a lot of processing time to solve and hence successfully add a block to the chain. In the contest to obtain a solution first, the winner is that initial miner, which receives newly generated bitcoin.

6) Power of Stake (PoS)

The general process of operating on the blockchain networks involves use of a consensus mechanism called Proof of Stake (PoS), for approving operations as well as adding more chains blocks. Unlike PoW, which requires miners to solve complex problems, Proof intends to get random individuals to embed their computer's computational power into a hashing algorithm.

Proof of Stake (PoS) work on the basis of a set of tokens of a particular cryptocurrency, for example, Bitcoin, to receive new blocks and confirm transactions.

IV. Overview of Ethereum

A. Security Ethereum

One of the issues that has been explored in the Ethereum ecosystem is security; In fact, various papers have explored the vulnerability, threat, and countermeasure that exists in the Ethereum domain. Of the components that make up Ethereum has smart contracts been investigated because of their security(discuss)mostly because they handle large amounts of cryptocurrencies which else would have notable monetary value and become ideal bait for an attacker [72]. The current study also reveals that new weakness has been found in the smart contracts of Ethereum hence the need to apply proper security measures that would avoid these areas being exploited [72].

Nonetheless, because Ethereum has become more and more complex over time and evolves at a high rate, it is critically important to get constant expert feedback and adhere to strict SSDLC not to encounter such issues at the protocol level, such as replay attacks or some shortcomings of using elliptic curve cryptography that provides only partial forward secrecy [73]. As the described ecosystem does not have central points of control and management, and is constantly developing, then the analysis and monitoring should be continuous to ensure that the transactions are protected from hacking and that the fulfillment of smart contracts is correct [73].

Furthermore, Ethereum an open-source distributed computing engine designated famous for smart contract attracted investors researchers' and attackers since it hosts the decentralized application (Dapps) [74]. This makes it possible to develop Dapps not only in the field of financial transactions but also it creates a basis for creating many applications for the platform environment of [74], [75]. The current threats in the ethereal domain have shaped the research on the anomaly detection systems, which conduct intrusion detection mechanisms to eliminate the threats [76].

Hence, one can presume that the aspect of security in Ethereum has multiple problems and concerns, which include threats to smart contracts, threats to the Ethereum networks, and an important aspect that has to do with the constant emergence of new threats and the subsequent improvement of current security measures. Haven broadly and susceptibly, Ethereum and its partitions continue to be maintained by academics and professionals in respect to the specific security aspects of Ethereum and in respect towards the methods that render it secure for protecting users' and their trade's assets.

B. Main Benefits of Security Ethereum

More recently, certain factors have been made different from one another, that can account for the observed gain of Security in Ethereum. Privileged benefit is the ability to execute smart contracts securely through reliance on Ethereum's blockchain. When executed, smart contracts on Ethereum operate within a context known as the Ethereum Virtual Machine, EVM, which regulates consensus and security in the system [76]. Compared to typical smart contract execution mechanisms, this secure one is a solid foundation for many purposes, including financial and other safe transactions and DApps [76].

Furthermore, if using Ethereum or other blockchain techniques, IoT applications have been introduced to enhance the security parameter. From the perspective of the literature review, the blockchain can solve security issues of IoT including confidentiality, integrity, availability, authentication, authorization, and accountability [41]. By leveraging two features namely, the immutability and the transparency of the blockchain, Ethereum can achieve and enhance the security levels of the IoT environment.

Also, the use of the formal verification of the security problem of smart contracts in blockchain like the application of Ethereum has been considered in order to ensure the dependability and security of smart contracts [42]. The certainty of the blockchain assurance is manifested by methods, but interfaces and possible hacking attempts do not indicate concern since the smart contract has formal verification.

First and last, Ethereum has certain over rivals for security in performing smart contracts, integrated IoT applications for making smart contracts safer, and finally use of formal verifications, for ensuring, that smart contracts on the stage are secure and non-interference.

C. Disadvantages of Security Ethereum

Thus, according to numerous research works, the disadvantages of security in Ethereum have been revealed, which explains the possible risks and difficulties within the platform. The major drawback observed is the existence of prominent security issues detected in Ethereum Smart Contracts. These vulnerabilities can lead to unpredictable behaviour and take-over of the applications that are implemented on the Ethereum platform [43]. Smart contract programming is not simple and systematic security practices are missing or not followed, which leads to the fact that there are a lot of vulnerabilities in Ethereum smart contracts that endanger their security [43].

A third drawback mentioned in the studies is the following effect of the Gas mechanism in Ethereum on the decentralization of the nodes. The present Gas cost model of Ethereum may cause a lot of inconveniences to nodes with ordinary computational capacity compared to other powerful nodes hence a threat to the centralization of nodes in the Ethereum network [38]. Such a significant difference in the count of computational units could potentially foster centralization of decision-making processes in the network, which goes a significant contrast against Ethereum's decentralized approach.

Also, it has established that the consensus mechanism known as Proof of Work (PoW), which is currently in use for Ethereum, has a security vulnerability. It is worth mentioning that any PoW-based network including Ethereum can be prone to some of the attacks like double spending, 51% attack, Distributed Denial of Service (DDoS) attacks, and Sybil attacks because they depend upon influential nodes for mining and verifying the data [44]. These vulnerabilities present various security threats to the network and affect its trustless consensus mechanism of Ethereum.

Also, the security threshold of Ethereum has been noted to be affected by selfish mining and stubborn mining approaches. All the above strategies have the potential of lowering the stringency of security in Ethereum and thus, expose the network to attacks and manipulations. The existence of such strategies points to the difficulties of preserving the blockchain network's security and reliability not to mention when confronted with strategic mining actions.

Altogether, Ethereum has several security drawbacks, which consist of protection weaknesses in smart contracts, issues linked to the Gas procedure, perilous associated with PoW consensus procedure, and the influence of mining procedures on community security. Mitigating these security issues is important in improving the security and the dependability of the Ethereum network.

D. Roles of Security Ethereum

Ethereum security measures are rather diverse, following the idea to keep Ethereum safe from threats of various types: internal or external, technical or social. The platform's security is underpinned by enhanced cryptography and consensus mechanism; the one responsible for safe and secure data transfer [45]. The platform improves the protection level by using hash functions, decentralized computation, and a large number of developers that can use the platform for many purposes [46].

Just like with any blockchain application, protocols of security measures are followed to avoid the presence of loopholes and hacking on Ethereum smart contracts. ContractFuzzer is the tool that has been created to find security vulnerabilities that provide fuzzing inputs derived from the specification of the smart contract [77]. Ethereum has also the architecture of a blockchain that facilitates decentralized application DApp on the blockchain network beyond money transfers [74].

In addition, Ethereum addresses the privacy issue in multi-stakeholder applications by providing confidentiality, integrity, and availability of the data [78]. The extraordinarily widespread adoption of the decentralization model of the platform and the consensus mechanisms that are used help to improve protection from vulnerabilities and threats [47]. The level of security adopted in Ethereum is intended to forestall all these and effectively reduce incidences of fraud, alteration of records, and unauthorized entry in block-chained transactions [77].

Thus, it is possible to conclude that Ethereum is protected from various kinds of threats and weaknesses by the use of advanced cryptographic solutions, decentralized consensus algorithms, smart-contract auditing tools, and PETS that bolster the security of Ethereum and its environment.

E. Issues of Security Ethereum

Weaknesses in security have been considered in Ethereum with some researchers analysing certain problems and weaknesses of the platform. Out of all the Ethereum concerns, problems concerning smart contracts, which entail contracts with the business terms coded into them can be considered as a major one. Such smart contracts will contain coding bugs, coding errors and different types of attacks where hackers can manipulate the transactions or even steal funds from smart contracts [79]. For example, last year, an exploit in the Ethereum Development Platform in the form of smart contracts was discovered in the DAO and as a result, millions of Ethereum tokens were lost which was indeed create a major financial loss [79].

Also, Ethereum which at the moment uses the mechanism known as Proof of Work (PoW) has security concerns regarding scalability and energy consumption. The PoW consensus algorithm applied to Ethereum, just like in Bitcoin, has flaws in relation to the transaction processing rate and energy consumption that affects the security and functionality of the platform [80]. Finally, high load of transactions and popularity of a certain object can cause the network load and super high commissions, which disrupts the idea of the security and efficiency of the Ethereum platform [80].

Moreover, the decentralisation of Ethereum enabled by open-source necessary for decentralised applications is no less dangerous from the security point of view because of the lack of data protection and confidentiality. Due to the inherent public characteristic of the blockchain all transactions contained in the block are public to anyone and hence may create a loophole for violation of privacy of some of the transactions [78]. Preserving data confidentiality and privacy of the data obtained within the Ethereum network still poses a major security challenge that should not be underestimated and for which efficient solutions should be sought [78].

Thus, there are threats and vulnerabilities of Ethereum's security that come from smart contract flaws, consensus algorithms and distributed ledger technologies, network capacity and transaction fees, and sensitive data leakage. Solving these problems is essential to increase the stability and reliability of the platform and its usability in the changing environment of blockchain technologies.

Interoperability Ethereum

On the meaning of Interoperability specific to Ethereum, it can be described as the ability of Ethereum to freely interact with other inter connected networks, systems and other blockchains. Interconnectivity allows Ethereum to exchange information, money and data with different blockchain systems, DApps, and the fundamental world. This interconnectivity is done through various intermediate layers as the smart contracts, the oracles, and the interoperability layers.

Smart Contracts in Ethereum actively contribute to the interoperability process as they follow previously predetermined conditions or transactions regarding other established correspondence systems. They can be programmed to call other APIs on their own, process the results based on information they receive from the outer world, or even act as cross-chain transactions which allows Ethereum to work with other block chain networks [81].

There are some other components that need for the interoperation and the oracles are one of them and which is associated with Ethereum. While smart contracts in one platform are awakened to make a particular decision, data providers transfer data from different platforms to Ethereum blockchain and to/from other platforms with the assistance of oracles. Therefore, through oracles Ethereum can process other information such as fiat prices for Ether, weather conditions or IoT devices, which enable it to interface with other systems [48]. Interoperability covers the protocols, standards, and frameworks that have the mandate of facilitating a seamless and organized interaction between Ethereum and other modern blockchains and networks. It defines the standard, spec, and design of how to carry out cross chain, asset exchange and information transaction between different platforms [82].

Therefore, through communication, Ethereum is able to connect to almost any other networks and systems, thus adding more possibilities to the Ethereum network and, potentially, allowing for various new use cases where the Ethereum is to interact with other platforms and seamlessly share data.

F. Interoperability Advantages Ethereum

Benefits of interoperation for the Ethereum based DApp derive partially from the general architecture of Ethereum as it is a predominantly open system that provides more opportunities for the interaction with the external environment and other blockchains. To be specific, the integration of Ethereum with a few systems has the following significant advantages.

DA Apps are convenient to use because Ethereum is integrated, meaning you can use decentralized applications regardless of your location in the world. Therefore, meaning and usage of Ethereum rises globally through the use of trustless interactions and transactions. This capability alone gives Ethereum a much larger pool of users apart from opening up cross border transactions hence making it a World platform for decentralized applications and financial commerce [49].

Interoperability of Ethereum has other advantages and one of this is security. Due to its improved encryption frameworks and consensus algorithms, Ethereum offers a certain high level of information security, sent between systems. This tight security framework is vital for maintaining the data importance and its uniqueness when being processed and while interacting with other networks that have a different security level [45].

It also opens up new combinations of use cases and applications in many more quadrants than could be previously seen. Thanks to Ethereum, it is possible to link different systems and networks together, and such an environment is an open space for experimentations and novelties. 'Of course, this integrative capability make developers able to apply together number of technologies and platforms to create new applications that will be beneficial for Ethereum environment more [49].

Also, its connectivity makes the data retrievable easing the enhancement of Ethereum to bring data from the external environment. This capability goes a long way in enhancing the accountability of financial transactions with reference to the capability of the blockchain to incorporate actual and real time data. Besides, the overall quality of data is greatly enhanced to assist the user get accurate and reliable information; in addition, it gives more credence to the system [83].

In addition, Ethereum is compatible; that is, a single blockchain can share with other blocks the manner of exchanging assets and data. This is ideally important for complementary characteristics of two or multiple blockchain systems to facilitate in forming a rather interwoven blockchain community [49].

Lastly, focusing on the Ethereum framework for the decentralized environment based on interoperability comes to decentralized trust. In this case, it means that regardless of the system it interacts with it keeps decentralisation standards for making the interactions/trade thrustless; decentralised trust is imbedded in Ethereum's values and approaches and that remain the stable ground for all Ethereum's work/ventures [49].

In conclusion, the interoperability advantages contributed to the hands of Ethereum enables the platform to communicate with the exterior environment, receive info, execute operations with other underpinning structures and contribute to the further evolution of the segment. They also enhance not only Ethereum but also build the decentralized applications and transactions' broad abilities as well.

G. Interoperability Disadvantages Ethereum

With regard to Ethereum specifically, one might say that interoperability problems can be quite an issue for the net ion in one direction and communication as well as integration with other systems or Blockchains. Therefore, it is clear that if the above elements are considered, the advantages of blockchain interoperability are apparent, but as always, the problem when implementing such a connection is that attention should be paid to the fact that the Ethereum network should not be affected by stability, functionality, and security.

The main issue with the interoperability in Ethereum is that, often, they cannot be easily scaled upward. When it started interacting with data on the other chain or engaging in transactions, the complexity raises the traffic and load on the network's platforms. This scalability issue arises because of other mechanisms of communication and coordination in different systems that involve blockchain technology. Hence the 'transaction times may be high and other certain operation may reduce thereby posing a negative impact on business development and more so it become hard for the platform to expand the number of users at a very fast rate [50].

Interoperability is also defined with a certain set of security threats that its utilization seems to be doomed with anyway. Thus, giving it a place within the external systems and networks introduces the new risks and threats with the Ethereum usage. All these interactions might impact the general security of the blockchain platform as either the attackers utilize the interdependent structures or all such transactions have to be verified to be safe while simultaneously, the integrity of Ethereum needs to be increased [50].

The final characteristic that was discussed, interoperability, also adds to the complexity of smart contracts, especially if the smart contracts have to move between different blockchain networks – in which code could become a lot more complex and not easy to manage at all in this case, it is possible to get issues with managing and documenting the code, and also with the auditing and protection of the interactions of smart contracts As part of the debates, developers are presented with additional challenges [50].

Another issue of interoperability, which is spelt out in Ethereum is the issue of data privacy In as much as it is possible to share data with external systems of Ethereum there is always the concern of data leakage, unauthorized access to data, access to records and documents This is because as the data transmits from one network to the other there is always the issue of data privacy which becomes hard to enforce The users and organisations should also devote equal attention to protect sensitive information [50].

Also, there is a difference in consensus protocols used in Ethereum and the other blockchain systems and this is another challenge related to interoperation. Often, various blockchain networks employ distinct consensus means and do not allow for making consensus about the defined transactions and data sharing. Such a misconfiguration can increase the difficulty in co-integration and interaction with other network as attaining finality and solidity in multi – system architecture is not easy [50].

Hence, it is possible to seem that there is a number of advantages which are regarded in transition to the concept of interoperability including the consideration of the various disadvantages and problems in this sphere. The last issue on smart contract is that it becomes complex; they have scalability issues; Smart contracts bring new security threats; concerns with data privacy; and violation of consensus protocol. The challenges encountered with Ethereum's open source nature when interfacing with other systems indicate the necessity for security and hence quality solutions must be implemented. Solving these challenges can on the one hand reinforce over the benefits of interoperability, on the other hand it can sustain high efficiency, high security and reliability features of Ethereum.

V. Overview of Hyperledger

A. Security Hyperledger

The security of Hyperledger Fabric remains sensitive to discussion, while improving the platform's resistance to possible threats is studied actively. Hyperledger Fabric, which is a permissioned blockchain technology has been described as having enhance privacy, throughputs, as well as negligible latency than some other private, permissioned technologies such as Quorum, Multichain, and R3 [84]. Designing of the platform focuses on the high-security encryption, easy scalability, deployment capabilities, and pluggability; the distributed ledger solutions offered by the Ethereum platform are versatile solutions that meet the needs of different applications [85].

Some works have proposed application of security features on Hyperledger Fabric, including access control of the personal data shared within the distributed ledger, as well as key transfer of User Characteristic Secret Keys, to make certain the protection of users' privacy [86]. Furthermore, Hyperledger Fabric's design is to build a blockchain solution for the growing number of business applications on an industrial level while addressing different sectors and purposes [8]. Incidentally, the platform's security measures include mechanisms such as encryption, restricted access, and cryptographic algorithms that safeguard the validity and confidentiality of the transactions [87].

In addition, theoretical studies have revealed the effectiveness of this platform in various meaningful organizations, including supply chain management and healthcare organizations combined with acceptance and popularity [88]. Width reference to the coding of smart contract, Hyperledger Fabric also outperforms other blockchain platforms in that it allows the writing of smart contracts in general purpose programming languages such as Java [89]. Besides, because of security measures integrated to the platform and its flexibility along with effectiveness, it can be essential in the ecosystem of the blockchain for different purposes and applications [6].

Finally, the security analyses of Hyperledger Fabric conclude that this platform is devoted to the security of users' data, providing privacy, and scalability while including numerous enterprise-grade security solutions that would help organizations adapt blockchain securely and proficiently.

B. Advantages of Security Hyperledger

It is this security that is offered in Hyperledger that counts for a lot and which paves the way for them to choose the same in their various endeavours. They include; holding that Hyperledger Fabric is privatized meaning it can be owned by some organizations in a way that only accredited individuals, communities, or companies are allowed to transact on the blockchain. Another benefit of this permission blockchain is that the participants are also known and more over-screened for fraud like the other participants also reduces the probability of engaging in unauthorized or fraudulent activities [51].

Additionally, Hyperledger Fabric boasts about having flexible CP models which can be easily extended or even customized depending on what the organization prefers for a particular use case or level of trust. About this flexibility can implement consensus mechanisms that are effective, thus enhancing security for the application of the network [51].

Compared with other existing platforms, the Hyperledger-based system has smaller response time and stronger scalability, but stronger traceability and audibility. These attributes are crucial in the security and privacy aspects of the IoT also the fulfilment of transactions particularly in the eventuality that a considerable volume of information is generated and transferred by and among different gadgets [51].

For the same reason, since Hyperledger Fabric messages respond to privacy and confidentiality attributes such as private transactions and channels; it brings about security and only permits the exchange of information between parties in an authorized channel. This capability is very crucial in areas of concern like the medical field and the financial sector this data is sensitive [52].

Also, Hyperledger Fabric is integrated with other advances in the sphere of security, for instance protocols concerning secure data integrity validation and innovations of key management system to contribute to the boosting of a security level of the platform. These integrations help in dealing with the threats and challenges to security therefore the reliability of the data in the blockchain [53].

Consequently, it can be stated that according to the described permissioned architecture, the non-fixed consensus solutions, scalability, privacy, and compatibility with the new protective systems, Hyperledger offers a vast potential for further enhancement of the security. Thus, the specific advantages of the presented models can be formulated as the following: Through the application of the above benefits of the proposed models, an organization is in a better position to create well-designed and secure blockchain solutions that addresses various security concerns.

C. Disadvantages of Security Hyperledger

Concerning the failure heuristic for Security, some of the failure cases are also included in the recent studies contemplating the Hyperledger forum that point out the issues or threats that were pretty visible on the surface. Two main disadvantages; Security because even though it comes under the label of a Hyperledger which is more of a permission blockchain. The permission type has a better handle and control over the people that are allowed to register with the network or even transact some functions within the network. On the other hand, permission type has issues in managing the permission and the identities than the permissionless one, which at one time may lead to misconfiguration This in a way makes the network vulnerable and can easily be compromised if the network is through to look for [75].

Then there is the level of security that comes by default with various portions of HL including Hyperledger Besu or Hyperledger Orion. These components may not have similar subcomponents needed for base defence or specific decentralised application or DApps security as key assignments, IDS. Furthermore, the unprotected privacy group identifier in Hyperledger Besu is by default and with an easily hackable hard code, which elevates the Security weakness, and also permits some of the data to be seen by unauthorized individual [54].

However, the integration of the Hyperledger Fabric to IoT-based systems has posed more security challenges in relation to damaging interaction as far as IoT networks are concerned. This restriction therefore entails that an attack or manipulation can take place within the parameters of Hyperledger Fabric, and this impacts the IoT component communication networks that have been established [55].

However, there still exists a blatant security aspect observed in the preceding section whenever utilizing Hyperledger Fabric as the one mentioned to not fit IoT-based Health Monitoring systems that brings all the above challenges together. Maybe, it could be nonoptimal to use traditional ways for protection from threats from the outside to the IoT nodes to pursue arrays of questions on the IoT nodes because the complicated computations with high energy demands are not at all suited to the IoT nodes [48].

In such a connection, it locates such security issues directly with which Hyperledger is connected and these issues are related to some of the key points of permissioned blockchain, some of them are inherently not protected, and the problem of IoT security mentioned here as a topic of protection in IoT based systems. Hence, it can be deduced that more effort and ways should be employed in enhancing the security and more so the resiliency of the Hyperledger-based applications and systems that tackle such security challenges.

D. Functions of Security Hyperledger

For instance, Hyperledger Fabric has integrated security functions to provide some protection for the platform's actions against all types of threats and keep the generality of the key processes more secretive. Hyperledger Fabric is another type of blockchain that was designed for B2B commerce and has several features that distinguish it from the example above, such as limited access [90]. Read has a general fare of security that can provide some level of detail for access control targeting at protecting data [7].

Some cryptographic approaches adopted by Hyperledger Fabric area used for the purpose of transaction security, while other are used for maintaining the holiness of the blockchain system. It is also architectural flexible and modular in nature which are important features that in turn enhances its pluggability, which makes it easy to specify the required security settings based on the various applications [91]. In addition, the management claims the possibility of being able to offer certain levels of communication assurance, as well as ensuring the channels and the encryption as means to regulate and/or restrict both the input and the output of information for the sake of enhancing the overall security [92].

Furthermore, one must note that Hyperledger Fabric contains components such as anomaly detector and intrusion detector to help with quick identification and management of Data breaches and Cyberattacks within the network [93]. With inventions of such powerful techniques like machine learning, Hyperledger Fabric is well placed to enhance its security intelligence to deal with any looming breakthrough to block the blockchain transactions and information security, thus offering continuous security on the blockchain deals and data [43].

Therefore, the security element incorporated in Hyperledger Fabric includes the privacy aspect, the capacity and detailed regulation of permissioned access control, cryptographic security, and a highly efficient method for the identification of breakthroughs and intrusion for enhancing the platform against security threats and risks.

E. On Security Hyperledger

The security aspects in Hyperledger Fabric have been proposed to highlight the area of interest in the research to expose the vulnerabilities and challenges in the network. However, one of the critical problems that can arise in Hyperledger Fabric has to do with the fact that it is essentially permissioned. While having completely restricted access to the participants, permissioned blockchains bring some problematics and challenges in matters of granting access control and permissions securely and in a systematic way that can, indeed, misconfigure the system to thereby make it vulnerable to bad application and data applications [94].

It is safer to use particular Hyperledger consensus mechanisms, for example, PBFT or Raft which, however, if incorrectly applied, can negatively affect security inherent to Fabric. To ensure the validity of transactional consensus, consensus protocols are important and necessary for mining, and consensus-related problems or configuration issues could threaten the blockchain network [94].

The last security risk concern that should be accorded attention in Hyperledger Fabric has to do with smart contracts that are implemented on Hyperledger Fabric. There is no doubt that smart contracts are automatic and transparent, but they inherit the same problems as other software: coding errors that can potentially open a space in a program where bugs can be exploited by malicious actors. As for the security and the integrity of smart contracts within the HP context and specifically in the Hyperledger Fabric, code reviews, functional testing, as well as the adoption of the best practices all minimize the conceivable overall risks that may take place [94].

Second of all, the fact that FAB has a built environment and that this enables it to function more freely or easily also affords the possibility of an adjustable design, there are security implications to do with the use of multiple components. This shall be of significant importance in order to avoid the compromising of security every time that there is inter- module interactions & communications, peer endorsement, ordering of services and any activity at the application layer in the blockchain [94].

Summing up, dealing with the issues in the present article, it can be stated that the enhancement of security in Hyperledger Fabric can be possible only when the problem will be solved on various levels beginning with the access control and ending with consensus, smart contract security and using more reliable and more credible modular components to form the further staking of the Hyperledger Fabric-oriented platform for the subsequent enterprise applications based on the blockchain technology.

F. Hyperledger Fabric Architecture

Hyperledger fabric is an enterprise grade platform to build highly officinal and reliable distributed ledgers based on seven principles that provides optimized concealing, reliability, flexibility and scalability features. It refers to a decentralized ledger technology based on the concept of blockchain it uses smart contracts to facilitate the enforcement of trust from across various parties/ systems. Hyperledger Fabric eliminates mining but retains the beneficial properties of typical cryptocurrency blockchains such as Bitcoin and Ethereum like State developmental/regulation, fixed/acausal, and anti-counterfeiting amongst others. It has been established that in the throughput capability of certain numbers of transactions per second; thousands [95], Hyperledger Fabric is better off than others. Some of these include: These characteristics and others that will be described below make Hyperledger Fabric completely appropriate for complex multiple physical/ logical supply chain arrangements, that encompass several physical and/or logical supply chain processes and actors. The smart contracts here are built utilizing general-purpose programming languages. Java, Go, NodeJS The smart contracts are created with general-purpose languages of programming to make it easily accessible to as many organizations as possible with the aim of increasing the adoption rate of this technology against technologies that require the use of certain programming languages, for instance, solidity in the Ethereum platform.

In this paper an attempt was made to give first proposal of how the drug traceability should look like in Hyperledger Fabric for the discussed enterprise-level blockchain-based system for the support of the pharmaceutical supply chain management; the account of different stakeholders with indication of their relations based on different channels to provide the maximal privacy and confidentiality and data protection. This notion of channels in the context of Hyperledger is entirely different and such a concept is missing in other regular platforms. Organizationally, channels offer both conceptual, tangible, and feasible structural clear line separating business contents/functions and policies governing the use of sensitive user data owned by different stakeholders who operate under one platform/system. In fact, Hyperledger Fabric synthesizes a Crash Fault Tolerant Transaction Ordering Service to bring deterministic characteristic when an event is being recorded, as well as for a secured way of transmitting or sharing medication related transactions among a group of people or institutions who cannot be trusted. This aids in establishing a sound track and trace system of origin to policy make the way ahead regarding stocking counterfeit medication in PSC. In this proposed scheme for the architecture of the new building blocks for the creation of a blockchain architecture, there is modularity for flexibility, security on layers, and the privacy for growth.

In the prospective Hyperledger Fabric model, the possible private blockchain network setup being permissioned, all the user entities and their identities/party details like the Indian pharmaceutical company and customers/end-users can be authenticated and identified by the Health Authority using the Membership service provider (MSP) component of Hyperledger Fabric. The MSP component is designed as the plug-in feature: in the default, an MSP part can be the one provided/delivered along with Hyperledger Fabric as Local MSP or it can be the external one (for example, generate OpenSSL certificates and use them, integrate with Active Directory, and so on). As far as the formation of the trust relationship within the untrusted participants is concerned, the Hyperledger fabric just draws the necessity simply to use the MSP (local/external) that sets the rules and regulatory frameworks that would govern the various stakes/identity-seeking to access the blockchain resources. They ensure that the identities of the people interacting in the network are protected, and also allow easier identification of actions (such as when a malicious transaction has been carried out). It is a unique approach in the context of a freemium business model that revisits non-determinism, exhaustion of resources, and performance checks at all the participants of the chain of supply of pharmaceutical products through decentralisation of identity [95].

Finally, the ordering service (OS) and peer nodes (peers), in different levels, are seen as the basic modules of Hyperledger Fabric. Peers have several utilities including replicating the ledger including copies, executing smart contracts better understood in Hyperledger Fabric as the chain code, endorsing, and also logging the transaction. These transactions are then forwarded to the OS from the client's app after which they are grouped into blocks by the endorsement signature of other peers in a blockchain network and only after that are sent to the committing peers to check against the endorsement policies of the blockchain network.

G. Interoperability Hyperledger Fabric

Interoperability in Hyperledger Fabric refers to the seamless exchange of data, assets, and information between the Hyperledger Fabric blockchain network and external systems or other blockchain platforms. This capability is crucial for enabling cross-platform communication and collaboration, expanding the range of potential use cases and applications.

A significant aspect of achieving interoperability in Hyperledger Fabric is through the support of interoperability protocols and standards. These protocols establish common rules and formats for data exchange and transactions, ensuring compatibility and smooth communication between Hyperledger Fabric and other blockchain networks [56].

Smart contracts are essential for facilitating interoperability within Hyperledger Fabric. They can be programmed to interact with external systems, respond to external data inputs, or facilitate cross-chain transactions, thereby enabling Hyperledger Fabric to engage with a variety of networks and platforms [56].

Oracles also play a vital role in achieving interoperability within Hyperledger Fabric. By serving as bridges between the blockchain network and external data sources, oracles provide smart contracts with real-world data from off-chain sources. Through oracles, Hyperledger Fabric gains access to external information, enhancing its interoperability with external system [56].

In conclusion, Hyperledger Fabric's interoperability capabilities, supported by interoperability protocols, smart contracts, and oracles, facilitate seamless communication and data exchange between the blockchain network and external systems. This fosters collaboration and innovation in decentralized applications and transactions.

H. Interoperability Advantages Hyperledger Fabric

Hyperledger Fabric's interoperability capabilities bring a myriad of advantages that significantly enhance its functionality and utility within the blockchain ecosystem. By enabling seamless communication with other blockchain networks, Hyperledger Fabric ensures that data and as sets can be exchanged effortlessly across different platforms, thereby boosting scalability and performance. This ability to interact with various systems not only expands the platform's reach but also optimizes its operational efficiency, allowing it to handle increased volumes of transactions and data exchanges more effectively [57].

One of the most impactful applications of Hyperledger Fabric's interoperability is in healthcare data sharing. The platform supports efficient and secure information exchange between patients, physicians, and healthcare providers. This feature ensures that sensitive medical data can be shared transparently and traceably, enhancing the quality of care and ensuring that medical professionals have access to accurate and up-to-date patient information [58]. Such capabilities are crucial for creating integrated healthcare systems that prioritize patient safety and data integrity.

Hyperledger Fabric's ability to facilitate cross-blockchain transactions is another significant advantage. By enabling the transfer of assets and data between disparate blockchain networks, Hyperledger Fabric fosters greater collaboration and interoperability within the blockchain space. This cross-chain capability is essential for creating a more cohesive and interconnected blockchain ecosystem, where different platforms can work together seamlessly to achieve common goals [56].

The development of decentralized applications (Dapps) is also greatly enhanced by Hyperledger Fabric's interoperability. These applications can interact with multiple blockchain networks, significantly increasing their versatility and functionality. This cross-platform interaction allows developers to create more robust and flexible Dapps that can leverage the strengths of various blockchain networks, providing users with a richer and more comprehensive experience [96].

Moreover, the interoperability features of Hyperledger Fabric facilitate smart contract interactions between different blockchain networks. This capability ensures that agreements and transactions can be executed seamlessly across various platforms, enhancing the reliability and efficiency of these processes. The ability to interact with smart contracts from different networks opens new possibilities for automating and streamlining complex transactions, making blockchain solutions more powerful and versatile [97].

In the realm of supply chain management, Hyperledger Fabric's interoperability offers significant advantages. The platform supports the integration of various components within the supply chain, promoting the secure and efficient exchange of data and assets. This integration ensures that all participants in the supply chain have access to accurate and timely information, improving transparency and accountability. As a result, businesses can better manage their supply chains, reducing costs and increasing efficiency [98].

In conclusion, Hyperledger Fabric's interoperability advantages empower the platform to collaborate effectively with diverse blockchain networks. This capability enhances scalability and performance, supports healthcare data sharing, enables cross-blockchain transactions, facilitates the development of decentralized applications, and streamlines supply chain management solutions. By leveraging these interoperability features, Hyperledger Fabric not only improves its own functionality but also contributes to the broader advancement of the blockchain ecosystem.

I. Interoperability Disadvantages Hyperledger Fabric

Interoperability challenges for Hyperledger Fabric can indeed pose significant obstacles in achieving seamless communication and integration with external systems and other blockchain platforms. While the potential benefits of interoperability are well-recognized, various inherent complexities and risks must be managed effectively to maintain the functionality and security of Hyperledger Fabric.

One of the primary challenges associated with interoperability in Hyperledger Fabric is the complexity involved in implementing interoperability protocols. The process requires intricate protocols and standards to ensure compatibility and smooth data exchange with diverse blockchain networks. This complexity can lead to difficulties in creating a unified approach for interoperability, as different blockchain platforms may have varying specifications and requirements. Ensuring that Hyperledger Fabric can effectively communicate and integrate with other networks demands considerable effort in developing and maintaining these interoperability protocols [59].

Security concerns are another significant challenge when it comes to interoperability. Interactions with external systems can introduce new vulnerabilities and attack vectors, potentially compromising the overall security of the Hyperledger Fabric network. As the platform opens to cross-chain transactions and data exchanges, it becomes crucial to implement robust security measures to protect against potential threats. The challenge lies in ensuring that all interactions are secure, and that the integrity of the Hyperledger Fabric network is maintained despite the increased exposure to external risks [59].

The misalignment of consensus mechanisms between Hyperledger Fabric and other blockchain platforms also poses a substantial hurdle to interoperability. Different blockchain networks may utilize various consensus protocols, making it challenging to achieve consensus and transaction finality across these disparate systems. This misalignment can impede the seamless integration of Hyperledger Fabric with other networks, as ensuring consistent and reliable transaction processing across different platforms becomes increasingly complex [59].

Data privacy and confidentiality concerns are also paramount in the context of interoperability. The exchange of information between Hyperledger Fabric and external systems can lead to potential data leakage or unauthorized access to sensitive information. Protecting user privacy and ensuring that confidential data remains secure during cross-chain interactions is a critical challenge. It requires robust data protection measures and strict privacy protocols to prevent breaches and maintain trust in the platform [59].

Furthermore, ensuring the compatibility and functionality of smart contracts across different blockchain networks is a significant challenge for interoperability in Hyperledger Fabric. Smart contracts need to be designed and executed in a manner that is compatible with the various environments they interact with. This necessitates careful consideration of contract logic and execution, ensuring that smart contracts can function seamlessly and securely across heterogeneous blockchain platforms. The complexity of achieving this compatibility can hinder the development and deployment of interoperable smart contracts [59].

In conclusion, while interoperability offers numerous benefits, such as enhanced collaboration and data exchange, it also presents several challenges and complexities. The complexity of interoperability protocols, security risks, consensus mechanism misalignment, data privacy concerns, and smart contract compatibility issues are significant challenges that need to be addressed. Ensuring the secure and efficient integration of Hyperledger Fabric with external systems requires meticulous planning and the implementation of robust solutions to mitigate these challenges. By addressing these issues, Hyperledger Fabric can continue to leverage the advantages of interoperability while maintaining its performance, security, and reliability.

VI. DISCUSSION

It is entirely worth emphasizing that even the highest levels of security must be introduced in this respect, as it is one of the key measures if it comes to threats and risks characteristic of blockchain-type computer systems.

Monitoring activity attempts to seek to spy on the network to look for indications of activity that might be considered a distortion or any other activity that will be regarded as insecure. Another form of security is there where an automatic process happens, and artificial intelligence and machine learning are there to guide the process to detect threats beforehand and it acts as a swipe to prevent intrusion if it has been planned. These policies, plans, and frameworks prevent any security breach in the first place but in case a security breach occurs, then there is a well-formulated and defined strategy on how to minimize or avoid the adverse effects on the blockchain systems. Implementation of such measures when has the effect of building a strong energy of security that guards not only the Ethereum but also Hyperledger Fabric Blockchain and is among the best measures that can help to reduce the possibility of an attack breakthrough and hence strengthen the chance of the blockchain platform.

Interoperability is another element that cannot be considered as a topic that should be left beyond the scope of the performed activities. It is hence necessary to engage and calibrate the Ethereum and the multiple blockchains within the Hyperledger Fabric to sustain directional interactions with standards for interoperability. Also, it could be explained concerning the fact that interoperation could also be defined as the degree of effectiveness, whereby the greater number of distinct systems could interconnect and recreate, the efficiency of which has been observed to be significantly enhanced, because of the greater standardized on the communication processes [59]. It boosts the effectiveness of blockchains while decreasing those interfaces which are normally needed which is the amazing increase of organizations that use this blockchain technology as they try to integrate so many systems.

Therefore, to consider controlling the interactions with the smart contracts as an important job that should be performed after a certain time to ensure that the smart contract forms are devoid of any circumstance of the malicious corruption. Smart contract audit effectively examines the contracts that are created and then checked for possible flaws that can also be maliciously exploited by hackers. Therefore, when using services of smart contracts threats can be avoided since using this tool one can check all security aspects of the blockchain platform for the purpose of full-fledged safety assessment of all characteristics of its security. Ideally, it is important that they start developing such a positive action to contribute towards the creation of principles based on trust and confidence in the use of blockchain platform [59], [14] .

A. Scalability Challenges and Solutions between Ethereum and Hyperledger Fabric

Ethereum's scalability has long been hindered by the limitations of its Proof of Work (PoW) consensus mechanism, which requires significant computational resources and limits transaction throughput. To address these challenges, Ethereum's transition to Proof of Stake (PoS), finalized with Ethereum 2.0, represents a fundamental shift in its architecture. PoS reduces energy consumption by replacing miners with validators who propose, and attest blocks based on their staked Ether. This transition enables faster block finalization, improves network efficiency, and scales the number of transactions per second (TPS), alleviating congestion and lowering gas fees.

Hyperledger Fabric takes a different approach to scalability by leveraging a modular and permissioned architecture. Unlike Ethereum, which operates on a single chain, Hyperledger Fabric allows for the parallel execution of smart contracts (chaincode) across different channels. This separation of transaction execution, ordering, and validation streamlines processing and minimizes bottlenecks. The flexibility to use pluggable consensus mechanisms further allows organizations to customize Fabric deployments based on performance requirements, resulting in greater scalability across enterprise environments.

Ethereum's PoS model focuses on achieving scalability in a public, decentralized environment, addressing the needs of decentralized applications (DApps) and financial services. In contrast, Hyperledger Fabric's modular design prioritizes scalability within private, permissioned networks, catering to enterprises that require high throughput and efficient resource allocation. These distinct approaches to scalability reflect the diverse use cases that blockchain platforms aim to serve, highlighting the evolving landscape of distributed ledger technologies.

B. Artificial Intelligence and Machine Learning for Blockchain Security and Anomaly Detection

As blockchain networks grow in complexity and scale, the need for robust security mechanisms becomes paramount. Artificial intelligence (AI) and machine learning (ML) have emerged as essential tools for enhancing blockchain security, offering capabilities such as anomaly detection, fraud prevention, and threat mitigation. By analysing large datasets of blockchain transactions, ML algorithms can identify patterns indicative of malicious activity, such as double-spending attempts, smart contract exploits, and network attacks.

In Ethereum, AI-driven security solutions monitor decentralized applications (DApps) and smart contracts for vulnerabilities. These systems detect irregularities in transaction flows, identify potentially fraudulent addresses, and flag deviations in gas usage that may signal malicious intent. Similarly, Hyperledger Fabric integrates AI models to monitor permissioned networks, ensuring that access control policies are enforced and anomalies in chaincode execution are promptly addressed. Fabric's modular architecture facilitates the deployment of custom anomaly detection models tailored to specific enterprise needs.

AI enhances blockchain security by providing predictive insights into potential threats. Machine learning models, trained on historical data, predict future vulnerabilities, enabling pre-emptive measures to secure blockchain ecosystems. In the context of Ethereum, AI systems proactively identify risky smart contract deployments, while in Hyperledger Fabric, AI-driven security analytics assess network health, ensuring that consensus mechanisms and node interactions remain uncompromised.

Integrating AI and ML into blockchain networks strengthens resilience against evolving cyber threats. This convergence represents a critical step towards creating autonomous, self-healing blockchain infrastructures capable of mitigating risks in real time. As blockchain adoption accelerates, the synergy between distributed ledger technologies and AI will play a pivotal role in safeguarding decentralized and enterprise blockchain solutions.

VII. CONCLUSION

Among the key stakeholders present within the context of a blockchain platform, two are of considerable importance, Ethereum and Hyperledger Fabric. Ethereum is widely recognized for its smart contracts and its significant role in advancing decentralized finance (DeFi), which has been instrumental in shaping the blockchain landscape [99]. Moreover, Hyperledger Fabric has also been identified to be among the favorite solutions for enterprise implementation because of qualities such as improved security, chances of decentralized operation, and inherent modularity [85].

Finally, about the performance benchmarking, the research has left to discuss the comparison of such platforms as Ethereum and Hyperledger Fabric by using the different benchmarks [100], [101]. These assessments are critical because they shed light on the approaches' advantages and disadvantages when it comes to making accurate, situation-specific determinations. In addition, there was explication about how different blockchain platforms can interconnect, for example, it may enable Ethereum or Hyperledger Fabric and other networks to interface [13], [14].

On the other hand, in terms of security, Hyperledger Fabric has always emerged as superior because it comes with excellent security and privacy features; thus, it has been deployed in, for instance, the storage of healthcare data [11], [102]. Additionally, the application of even higher-level technologies, including such ones as Hyperledger Fabric or any other types of blockchains described in this research, provide assured impermeability for the organizational data as it cannot be modified in any way [3].

Therefore, it may be easy to establish that Ethereum and Hyperledger Fabric are two distinct but essential types of a continuously developing blockchain platform. The current features of smart contract and Decentralized finance place Ethereum in the front line of industry while Hyperledger Fabric has all every enterprise solution and high security solutions that makes them suitable for usage in Health informatics records, 5G interoperability solutions.

ACKNOWLEDGMENT

This work is supported by the FRGS24-327-0936 under Ministry Project ID: FRGS/1/2024/ICT02/UIAM/02/4, Centre of Excellence Cybersecurity, KICT, IoTeams, KICT and Silverseeds Lab Network.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] H. Chen, M. Pendleton, L. Njilla, and S. Xu, “A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses,” 2019, *arXiv*. doi: 10.48550/ARXIV.1908.04507.

[2] Y. Xie, J. Jin, J. Zhang, S. Yu, and Q. Xuan, “Temporal-Amount Snapshot MultiGraph for Ethereum Transaction Tracking,” 2021, *arXiv*. doi: 10.48550/ARXIV.2102.08013.

[3] S. A. Amri, L. Aniello, and V. Sassone, “A Review of Upgradeable Smart Contract Patterns based on OpenZeppelin Technique,” *The JBBA*, vol. 6, no. 1, pp. 1–8, Apr. 2023, doi: 10.31585/jbba-6-1-(3)2023.

[4] S. Pandey *et al.*, “Do-It-Yourself Recommender System: Reusing and Recycling With Blockchain and Deep Learning,” *IEEE Access*, vol. 10, pp. 90056–90067, 2022, doi: 10.1109/ACCESS.2022.3199661.

[5] J. Kim, K. Lee, G. Yang, K. Lee, J. Im, and C. Yoo, “QiOi: Performance Isolation for Hyperledger Fabric,” *Applied Sciences*, vol. 11, no. 9, p. 3870, Apr. 2021, doi: 10.3390/app11093870.

[6] R. Alotaibi, M. Alassafi, Md. S. I. Bhuiyan, R. S. Raju, and M. S. Ferdous, “A Reinforcement-Learning-Based Model for Resilient Load Balancing in Hyperledger Fabric,” *Processes*, vol. 10, no. 11, p. 2390, Nov. 2022, doi: 10.3390/pr10112390.

[7] H. Chen, M. Pendleton, L. Njilla, and S. Xu, “A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses,” 2019, *arXiv*. doi: 10.48550/ARXIV.1908.04507.

[8] R. Zhang, R. Xue, and L. Liu, “Security and Privacy on Blockchain,” *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, May 2020, doi: 10.1145/3316481.

[9] A. Roehrs, C. A. Da Costa, R. Da Rosa Righi, V. F. Da Silva, J. R. Goldim, and D. C. Schmidt, “Analyzing the performance of a blockchain-based personal health record implementation,” *Journal of Biomedical Informatics*, vol. 92, p. 103140, Apr. 2019, doi: 10.1016/j.jbi.2019.103140.

[10] M. Islam, M. H. Rehmani, and J. Chen, “Differential Privacy-based Permissioned Blockchain for Private Data Sharing in Industrial IoT,” 2021, *arXiv*. doi: 10.48550/ARXIV.2102.09857.

[11] Q. Wang and S. Qin, “A Hyperledger Fabric-Based System Framework for Healthcare Data Management,” *Applied Sciences*, vol. 11, no. 24, p. 11693, Dec. 2021, doi: 10.3390/app112411693.

[12] L. Foschini, A. Gavagna, G. Martuscelli, and R. Montanari, "Hyperledger Fabric Blockchain: Chaincode Performance Analysis," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland: IEEE, Jun. 2020, pp. 1–6. doi: 10.1109/ICC40277.2020.9149080.

[13] G. Llambias, B. Bradach, J. Nogueira, L. González, and R. Ruggia, "Gateway-based Interoperability for DLT," Feb. 22, 2023. doi: 10.36227/techrxiv.22120520.

[14] D. L. Dinesha and B. Patil, "Achieving Interoperability in Heterogeneous Blockchain Users Through Inter-Blockchain Communication Protocol," Nov. 22, 2022. doi: 10.36227/techrxiv.21532953.v2.

[15] C. Stamatellis, P. Papadopoulos, N. Pitropakis, S. Katsikas, and W. Buchanan, "A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric," *Sensors*, vol. 20, no. 22, p. 6587, Nov. 2020, doi: 10.3390/s20226587.

[16] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," *PLoS ONE*, vol. 15, no. 12, p. e0243043, Dec. 2020, doi: 10.1371/journal.pone.0243043.

[17] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, p. 102067, Oct. 2020, doi: 10.1016/j.tre.2020.102067.

[18] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017, doi: 10.1093/jamia/ocx068.

[19] P. Tagde *et al.*, "Blockchain and artificial intelligence technology in e-Health," *Environ Sci Pollut Res*, vol. 28, no. 38, pp. 52810–52831, Oct. 2021, doi: 10.1007/s11356-021-16223-0.

[20] A. Henninger and A. Mashatan, "Distributed Renewable Energy Management: A Gap Analysis and Proposed Blockchain-Based Architecture," *JRFM*, vol. 15, no. 5, p. 191, Apr. 2022, doi: 10.3390/jrfm15050191.

[21] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[22] T. G. Bao and D. M. Phan, "Blockchain applications in business and financial activities in Vietnam: Situation, trends, opportunities and challenges," *irjmis*, vol. 9, no. 6, pp. 766–776, Sep. 2022, doi: 10.21744/irjmis.v9n6.2187.

[23] Z. Yu, D. Xue, J. Fan, and C. Guo, "DNSTSM: DNS Cache Resources Trusted Sharing Model Based on Consortium Blockchain," *IEEE Access*, vol. 8, pp. 13640–13650, 2020, doi: 10.1109/ACCESS.2020.2966428.

[24] W. Yao, F. P. Deek, R. Murimi, and G. Wang, "SoK: A Taxonomy for Critical Analysis of Consensus Mechanisms in Consortium Blockchain," 2021, doi: 10.48550/ARXIV.2102.12058.

[25] V. Upadrista, S. Nazir, and H. Tianfield, "Consortium Blockchain for Reliable Remote Health Monitoring," Jan. 04, 2024, *In Review*. doi: 10.21203/rs.3.rs-2297411/v1.

[26] W. Pourmajidi, L. Zhang, J. Steinbacher, T. Erwin, and A. Miranskyy, "Immutable Log Storage as a Service on Private and Public Blockchains," 2020, doi: 10.48550/ARXIV.2009.07834.

[27] J. Yusoff, Z. Mohamad, and M. Anuar, "A Review: Consensus Algorithms on Blockchain," *JCC*, vol. 10, no. 09, pp. 37–50, 2022, doi: 10.4236/jcc.2022.109003.

[28] D. C. G. Valadares, A. Perkusich, A. M. Falcão, and C. Seline, "Privacy-Preserving Blockchain Technologies," May 26, 2023, *Computer Science and Mathematics*. doi: 10.20944/preprints202305.1874.v1.

[29] H. C. Hwang, J. G. Shon, and J. S. Park, "Design of an Enhanced Web Archiving System for Preserving Content Integrity with Blockchain," *Electronics*, vol. 9, no. 8, p. 1255, Aug. 2020, doi: 10.3390/electronics9081255.

[30] L. M. Palma, M. A. G. Vigil, F. L. Pereira, and J. E. Martina, "Blockchain and smart contracts for higher education registry in Brazil," *Int J Network Mgmt*, vol. 29, no. 3, p. e2061, May 2019, doi: 10.1002/nem.2061.

[31] X. Wang *et al.*, "A High-Performance Hybrid Blockchain System for Traceable IoT Applications," in *Network and System Security*, vol. 11928, J. K. Liu and X. Huang, Eds., in Lecture Notes in Computer Science, vol. 11928. , Cham: Springer International Publishing, 2019, pp. 721–728. doi: 10.1007/978-3-030-36938-5_47.

[32] D. Zhuang and J. M. Chang, "Enhanced PeerHunter: Detecting Peer-to-Peer Botnets Through Network-Flow Level Community Behavior Analysis," *IEEE Trans.Inform.Forensic Secur.*, vol. 14, no. 6, pp. 1485–1500, Jun. 2019, doi: 10.1109/TIFS.2018.2881657.

[33] A. A. Mohammed and D. J. Kadhim, "Analysis of threats and security issues evaluation in mobile P2P networks," *IJECE*, vol. 10, no. 6, p. 6435, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6435-6445.

[34] D. Kazacos Winter, R. Khatri, and M. Schmidt, "Decentralized Prosumer-Centric P2P Electricity Market Coordination with Grid Security," *Energies*, vol. 14, no. 15, p. 4665, Aug. 2021, doi: 10.3390/en14154665.

[35] A. Hu, X. Gong, and L. Guo, "Diffractive Encryption: A Brand-New Chaotic Encryption Model," Feb. 28, 2022, *In Review*. doi: 10.21203/rs.3.rs-1389312/v1.

[36] C. Yang, B. Song, Y. Ding, J. Ou, and C. Fan, "Efficient Data Integrity Auditing Supporting Provable Data Update for Secure Cloud Storage," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, Mar. 2022, doi: 10.1155/2022/5721917.

[37] S. Joshi, "Feasibility of Proof of Authority as a Consensus Protocol Model," 2021, *arXiv*. doi: 10.48550/ARXIV.2109.02480.

[38] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019, doi: 10.1109/ACCESS.2019.2935149.

[39] J. Zhang, Y. Yang, D. Zhao, and Y. Wang, "A node selection algorithm with a genetic method based on PBFT in consortium blockchains," *Complex Intell. Syst.*, vol. 9, no. 3, pp. 3085–3105, Jun. 2023, doi: 10.1007/s40747-022-00907-2.

[40] M. Hu, T. Shen, J. Men, Z. Yu, and Y. Liu, "CRSM: An Effective Blockchain Consensus Resource Slicing Model for Real-Time Distributed Energy Trading," *IEEE Access*, vol. 8, pp. 206876–206887, 2020, doi: 10.1109/ACCESS.2020.3037694.

[41] I. E. Kassmi and Z. Jarir, "Blockchain-oriented Inter-organizational Collaboration between Healthcare Providers to Handle the COVID-19 Process," *IJACSA*, vol. 12, no. 12, 2021, doi: 10.14569/IJACSA.2021.0121294.

[42] P. Bottoni, A. Labella, and R. Pareschi, "A formal model for ledger management systems based on contracts and temporal logic," 2021, *arXiv*. doi: 10.48550/ARXIV.2109.15212.

[43] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[44] S. Maeng, M. Essaid, C. Lee, S. Park, and H. Ju, "Visualization of Ethereum P2P network topology and peer properties," *Int J Network Mgmt*, vol. 31, no. 6, p. e2175, Nov. 2021, doi: 10.1002/nem.2175.

[45] F. Jemili and O. Korbaa, "Hybrid Collaborative Intrusion Detection System Based on Blockchain &amp; Machine Learning," May 24, 2023, *In Review*. doi: 10.21203/rs.3.rs-2963689/v1.

[46] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the Ethereum blockchain," *Expert Systems with Applications*, vol. 150, p. 113318, Jul. 2020, doi: 10.1016/j.eswa.2020.113318.

[47] Y. Liu, Y. Hei, T. Xu, and J. Liu, "An Evaluation of Uncle Block Mechanism Effect on Ethereum Selfish and Stubborn Mining Combined With an Eclipse Attack," *IEEE Access*, vol. 8, pp. 17489–17499, 2020, doi: 10.1109/ACCESS.2020.2967861.

[48] F. P. Oikonomou, G. Mantas, P. Cox, F. Bashashi, F. Gil-Castineira, and J. Gonzalez, "A Blockchain-based Architecture for Secure IoT-based Health Monitoring Systems," in *2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, Porto, Portugal: IEEE, Oct. 2021, pp. 1–6. doi: 10.1109/CAMAD52502.2021.9617803.

[49] Y. Madhwal, Y. Yanovich, S. Balachander, K. H. Poojaa, R. Saranya, and B. Subashini, "Enhancing Supply Chain Efficiency and Security: A Proof of Concept for IoT Device Integration With Blockchain," *IEEE Access*, vol. 11, pp. 121173–121189, 2023, doi: 10.1109/ACCESS.2023.3328569.

[50] M. J. M. Chowdhury *et al.*, "A Comparative Analysis of Distributed Ledger Technology Platforms," *IEEE Access*, vol. 7, pp. 167930–167943, 2019, doi: 10.1109/ACCESS.2019.2953729.

[51] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," 2018, doi: 10.48550/ARXIV.1801.10228.

[52] Z. Leng, K. Wang, Y. Zheng, X. Yin, and T. Ding, "Hyperledger for IoT: A Review of Reconstruction Diagrams Perspective," *Electronics*, vol. 11, no. 14, p. 2200, Jul. 2022, doi: 10.3390/electronics11142200.

[53] J. Randolph *et al.*, "Blockchain-based Medical Image Sharing and Automated Critical-results Notification: A Novel Framework," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, Los Alamitos, CA, USA: IEEE, Jun. 2022, pp. 1756–1761. doi: 10.1109/COMPSAC54236.2022.00279.

[54] P. Praitheeshan, L. Pan, and R. Doss, "Private and Trustworthy Distributed Lending Model Using Hyperledger Besu," *SN COMPUT. SCI.*, vol. 2, no. 2, p. 115, Apr. 2021, doi: 10.1007/s42979-021-00500-3.

[55] M. Salimitari, M. Joneidi, and M. Chatterjee, "AI-Enabled Blockchain: An Outlier-Aware Consensus Protocol for Blockchain-Based IoT Networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Waikoloa, HI, USA: IEEE, Dec. 2019, pp. 1–6. doi: 10.1109/GLOBECOM38437.2019.9013824.

[56] K. Kanagi, C. C.-Y. Ku, L.-K. Lin, and W.-H. Hsieh, "Efficient Clinical Data Sharing Framework Based on Blockchain Technology," *Methods Inf Med*, vol. 59, no. 06, pp. 193–204, Dec. 2020, doi: 10.1055/s-0041-1727193.

[57] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger Approaches," *IEEE Access*, vol. 7, pp. 89948–89966, 2019, doi: 10.1109/ACCESS.2019.2926880.

[58] T. Fatokun, A. Nag, and S. Sharma, "Towards a Blockchain Assisted Patient Owned System for Electronic Health Records," *Electronics*, vol. 10, no. 5, p. 580, Mar. 2021, doi: 10.3390/electronics10050580.

[59] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," 2020, *arXiv*. doi: 10.48550/ARXIV.2005.14282.

[60] V. Ribeiro, R. Holanda, A. Ramos, and J. J. P. C. Rodrigues, "Enhancing Key Management in LoRaWAN with Permissioned Blockchain," *Sensors*, vol. 20, no. 11, p. 3068, May 2020, doi: 10.3390/s20113068.

[61] Zainuddin, A. A., Handayani, D., Ridza, I. H. M., Rahman, S. H. A., Kamarudin, S. I., Ahmad, K. Z., ... & Dhuzuki, N. H. M. (2024, May). Converging for Security: Blockchain, Internet of Things, Artificial Intelligence-Why Not Together?. In 2024 IEEE 14th Symposium on Computer Applications & Industrial Electronics (ISCAIE) (pp. 181-186). IEEE.

[62] S. Dhingra, R. Raut, K. Naik, and K. Muduli, "Blockchain Technology Applications in Healthcare Supply Chains—A Review," *IEEE Access*, vol. 12, pp. 11230–11257, 2024, doi: 10.1109/ACCESS.2023.3348813.

[63] D. V. Dimitrov, "Blockchain Applications for Healthcare Data Management," *Healthc Inform Res*, vol. 25, no. 1, p. 51, 2019, doi: 10.4258/hir.2019.25.1.51.

[64] P. F. Wong, F. C. Chia, M. S. Kiu, and E. C. W. Lou, "Potential integration of blockchain technology into smart sustainable city (SSC) developments: a systematic review," *SASBE*, vol. 11, no. 3, pp. 559–574, Nov. 2022, doi: 10.1108/SASBE-09-2020-0140.

[65] S. Lu *et al.*, "CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle," *Sensors*, vol. 23, no. 4, p. 1864, Feb. 2023, doi: 10.3390/s23041864.

[66] R. Zhao, J. Zhou, R. Shi, and J. Shi, "Unidimensional Continuous Variable Quantum Key Distribution under Fast Fading Channel," *Annalen der Physik*, vol. 536, no. 5, p. 2300401, May 2024, doi: 10.1002/andp.202300401.

[67] Z. Li *et al.*, "Polarization-Assisted Visual Secret Sharing Encryption in Metasurface Hologram," *Advanced Photonics Research*, vol. 2, no. 11, p. 2100175, Nov. 2021, doi: 10.1002/adpr.202100175.

[68] Y. Ding, C. Wang, Q. Zhong, H. Li, J. Tan, and J. Li, "Function-Level Dynamic Monitoring and Analysis System for Smart Contract," *IEEE Access*, vol. 8, pp. 229161–229172, 2020, doi: 10.1109/ACCESS.2020.3046005.

[69] M. Pustisek, J. Turk, and A. Kos, "Secure Modular Smart Contract Platform for Multi-Tenant 5G Applications," *IEEE Access*, vol. 8, pp. 150626–150646, 2020, doi: 10.1109/ACCESS.2020.3013402.

[70] N. Minsky and C. Cong, "Scalable, Secure and Broad-Spectrum Enforcement of Contracts, Without Blockchains," 2019, *arXiv*. doi: 10.48550/ARXIV.1904.09940.

[71] Y. Huang, Y. Bian, R. Li, J. L. Zhao, and P. Shi, "Smart Contract Security: A Software Lifecycle Perspective," *IEEE Access*, vol. 7, pp. 150184–150202, 2019, doi: 10.1109/ACCESS.2019.2946988.

[72] N. Lu, B. Wang, Y. Zhang, W. Shi, and C. Esposito, "NeuCheck: A more practical Ethereum smart contract security analysis tool," *Softw Pract Exp*, vol. 51, no. 10, pp. 2065–2084, Oct. 2021, doi: 10.1002/spe.2745.

[73] J.-P. Aumasson, D. Kolegov, and E. Stathopoulou, "Security Review of Ethereum Beacon Clients," 2021, *arXiv*. doi: 10.48550/ARXIV.2109.11677.

[74] A. H. H. Kabla *et al.*, "Applicability of Intrusion Detection System on Ethereum Attacks: A Comprehensive Review," *IEEE Access*, vol. 10, pp. 71632–71655, 2022, doi: 10.1109/ACCESS.2022.3188637.

[75] N. T. Anthony, M. Shafik, F. Kurugollu, and H. F. Atlam, "Anomaly Detection System for Ethereum Blockchain Using Machine Learning," in *Advances in Transdisciplinary Engineering*, M. Shafik and K. Case, Eds., IOS Press, 2022. doi: 10.3233/ATDE220608.

[76] O. Alpos, C. Cachin, G. A. Marson, and L. Zanolini, "On the Synchronization Power of Token Smart Contracts," 2021, *arXiv*. doi: 10.48550/ARXIV.2101.05543.

[77] J.-L. Ferrer-Gomila and M. F. Hinarejos, "A Multi-Party Contract Signing Solution Based on Blockchain," *Electronics*, vol. 10, no. 12, p. 1457, Jun. 2021, doi: 10.3390/electronics10121457.

[78] O. Debauche *et al.*, "RAMi: A New Real-Time Internet of Medical Things Architecture for Elderly Patient Monitoring," *Information*, vol. 13, no. 9, p. 423, Sep. 2022, doi: 10.3390/info13090423.

[79] X. Gu, H. Yang, S. Liu, and Z. Cui, "Smart Contract Vulnerability Detection Based on Clustering Opcode Instructions," presented at the The 35th International Conference on Software Engineering and Knowledge Engineering, Jul. 2023, pp. 398–403. doi: 10.18293/SEKE2023-183.

[80] A. Dhar Dwivedi, R. Singh, K. Kaushik, R. Rao Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," *Trans Emerging Tel Tech*, vol. 35, no. 4, p. e4329, Apr. 2024, doi: 10.1002/ett.4329.

[81] F. Pelekoudas-Oikonomou, J. Ribeiro, G. Mantas, F. Bashashi, G. Sakellari, and J. Gonzalez, "A Tutorial on the Implementation of a Hyperledger Fabric-based Security Architecture for IoMT," in *2023 IFIP Networking Conference (IFIP Networking)*, Barcelona, Spain: IEEE, Jun. 2023, pp. 1–6. doi: 10.23919/IFIPNetworking57963.2023.10186443.

[82] Y. Khan *et al.*, "BlockU: Extended usage control in and for Blockchain," *Expert Systems*, vol. 37, no. 3, p. e12507, Jun. 2020, doi: 10.1111/exsy.12507.

[83] X. Zheng, Y. Zhu, and X. Si, "A Survey on Challenges and Progresses in Blockchain Technologies: A Performance and Security Perspective,"

Applied Sciences, vol. 9, no. 22, p. 4731, Nov. 2019, doi: 10.3390/app9224731.

[84] R. Gangula, S. V. Thalla, I. Ikedum, C. Okpala, and S. Sneha, "Leveraging the Hyperledger Fabric for Enhancing the Efficacy of Clinical Decision Support Systems," *BHTY*, Feb. 2021, doi: 10.30953/bhty.v4.154.

[85] Y. G. Liu, Y. Duan, and Y. Zheng, "Blockchain-based label coverage storage query scheme," in *Third International Conference on Green Communication, Network, and Internet of Things (CNIoT 2023)*, S. Zhang and H. Wang, Eds., Chongqing, China: SPIE, Oct. 2023, p. 15. doi: 10.1117/12.3010265.

[86] N. Deb, M. A. Elashiri, T. Veeramakali, A. W. Rahmani, and S. Degadwala, "A Metaheuristic Approach for Encrypting Blockchain Data Attributes Using Ciphertext Policy Technique," *Mathematical Problems in Engineering*, vol. 2022, pp. 1–10, Feb. 2022, doi: 10.1155/2022/7579961.

[87] A. Iftekhar, X. Cui, Q. Tao, and C. Zheng, "Hyperledger Fabric Access Control System for Internet of Things Layer in Blockchain-Based Applications," *Entropy*, vol. 23, no. 8, p. 1054, Aug. 2021, doi: 10.3390/e23081054.

[88] D. Khan, L. T. Jung, M. A. Hashmani, and M. K. Cheong, "Empirical Performance Analysis of Hyperledger LTS for Small and Medium Enterprises," *Sensors*, vol. 22, no. 3, p. 915, Jan. 2022, doi: 10.3390/s22030915.

[89] "Optimal Deployment of Energy Based on Blockchain," *RE*, vol. 3, no. 1, Mar. 2022, doi: 10.38007/RE.2022.030104.

[90] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses," *ACM Comput. Surv.*, vol. 53, no. 3, pp. 1–43, May 2021, doi: 10.1145/3391195.

[91] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020, doi: 10.1109/COMST.2020.2975999.

[92] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.

[93] K. Li *et al.*, "PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains," *Front. Blockchain*, vol. 3, p. 11, Mar. 2020, doi: 10.3389/fbloc.2020.00011.

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

[95] M. Uddin, K. Salah, R. Jayaraman, S. Pesic, and S. Ellahham, "Blockchain for drug traceability: Architectures and open challenges," *Health Informatics J*, vol. 27, no. 2, p. 14604582211011228, Apr. 2021, doi: 10.1177/14604582211011228.

[96] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The Role of Blockchain Technology in Telehealth and Telemedicine," Sep. 19, 2020. doi: 10.36227/techrxiv.12967748.

[97] M. Madine, K. Salah, R. Jayaraman, Y. Al-Hammadi, J. Arshad, and I. Yaqoob, "appXchain: Application-Level Interoperability for Blockchain Networks," Jun. 21, 2021. doi: 10.36227/techrxiv.13903010.

[98] S. Loss, H. P. Singh, N. Cacho, and F. Lopes, "Using FIWARE and blockchain in smart cities solutions," *Cluster Comput*, vol. 26, no. 4, pp. 2115–2128, Aug. 2023, doi: 10.1007/s10586-022-03732-x.

[99] C. Soto-Valero, M. Monperrus, and B. Baudry, "The Multibillion Dollar Software Supply Chain of Ethereum," 2022, doi: 10.48550/ARXIV.2202.07029.

[100] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, Milwaukee, WI: IEEE, Sep. 2018, pp. 264–276. doi: 10.1109/MASCOTS.2018.00034.

[101] Q. Nasir, I. A. Qasse, M. Abu Talib, and A. B. Nassif, "Performance Analysis of Hyperledger Fabric Platforms," *Security and Communication Networks*, vol. 2018, pp. 1–14, Sep. 2018, doi: 10.1155/2018/3976093.

[102] D. Wang, Y. Zhu, Y. Zhang, and G. Liu, "Security Assessment of Blockchain in Chinese Classified Protection of Cybersecurity," *IEEE Access*, vol. 8, pp. 203440–203456, 2020, doi: 10.1109/ACCESS.2020.3036004.