IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 September 2023, accepted 8 October 2023, date of publication 30 October 2023, date of current version 3 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3328536

SURVEY

A Review of Blockchain Approaches for KYC

NAFEES MANSOOR[1], (Senior Member, IEEE), KANIZ FATEMA ANTORA[1], (Member, IEEE), PRIYATA DEB[1], TAREK AHAMMED ARMAN[1], AZIZAH ABDUL MANAF[2], AND MAHDI ZAREEI[3], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, University of Liberal Arts Bangladesh, Dhaka 1209, Bangladesh
[2]Department of Internet Engineering and Computer Science, Lee Kong Chian (LKC) Faculty of Engineering and Science, Universiti Tuanku Abdul Rahman (UTAR), Kajang 43000, Malaysia
[3]School of Engineering and Science, Tecnologico de Monterrey, Zapopan 45201, Mexico

Corresponding authors: Mahdi Zareei (m.zareei@ieee.org) and Nafees Mansoor (nafees@ieee.org)

ABSTRACT The traditional Know Your Customer (KYC) procedure used by banks is deemed unreliable and costly. Therefore, the adoption of emerging technologies is essential for banking firms' future prospects. One such technology that has gained widespread acceptance is Blockchain, which is known for its reliability and security across various fields. This study aims to investigate how the implementation of Blockchain technology can modify the existing banking business, particularly the KYC document verification process, by storing and monitoring of information. The current need for an optimized KYC system is paramount; one that is coupled with a secure and trustworthy technology like Blockchain that can withstand fraudulent activities while also overcoming scalability and privacy challenges. The article analyzes previous relevant works, which highlight how the implementation of Blockchain technology eliminates the need for intermediaries, thereby reducing the possibility of malicious activities and errors that may occur when there are multiple manual tasks involved.

INDEX TERMS Blockchain, decentralization, distributed ledger technology, know your customer (KYC), verification.

I. INTRODUCTION

Both researchers and professionals have identified blockchain as a viable solution to address various concerns in the banking industry [1]. This technology operates as a distributed ledger structure where decentralization is introduced. In other words, data is stored across a network of nodes that are chained together by peer-to-peer connections [2]. Consequently, the chances of data manipulation are significantly reduced. Blockchain technology offers numerous benefits to the banking industry, such as making KYC documents immutable and allowing accurate customer data [3].

The use of blockchain technology will not only solve many document verification problems but also assist banks and customers in tracking their outcomes [4], [5]. Identity verification is crucial for building trust between businesses and their customers. The process is the first step in establishing a business relationship. In the beginning, banking industries follow the KYC procedure to complete their verification process, then they move forward to other steps [5]. The KYC process may vary from country to country; however, it is mandatory in the investment industry. The process verifies an individual's information, such as name, address, utility bills, and more. In the investment industry, KYC ensures employers have access to detailed information about their clients' financial knowledge and investment activities [6]. This crucial step is often cumbersome and inconvenient for both clients and banks.

The current KYC process requires physical attendance at banks to provide personal information such as identity cards, photos, utility bills, and more. The system has weaknesses and vulnerabilities as it is time-consuming, repetitive, and prone to error [7]. Significant financial institutions must use the current centralized KYC system for their application and authentication processes, despite its flaws [8], [9]. This procedure aids in combating money laundering and suppressing the financing of terrorism. Many nations have

The associate editor coordinating the review of this manuscript and approving it for publication was Ali Kashif Bashir.

made it essential to undergo this process, ensuring that the clients are who they claim to be [1].

In the conventional KYC process, banks gather customer information as the first step in opening an account. However, the second step poses a significant disadvantage to the customer, as they may not be fully aware of who has access to their data [10]. Insufficient information leads to less informed choices [1]. As a result, any relevant information that banks would like to include in their analysis of a potential customer's identity must have been acquired with consent.

In recent years, the field of blockchain for KYC has seen the emergence of several survey papers, each offering unique contributions and areas of focus. The article [11] presents a systematic literature review (SLR) focusing on blockchain-based e-KYC systems in the financial services industry. The paper investigates the intersection of blockchain and e-KYC, analyzing various research perspectives and implementations. In this research, the authors examine the effectiveness of various blockchain based systems in terms of storage, cost, technology stack, etc. By using the PRISMA model, the article aims to provide future recommendations for enhancing e-KYC processes through blockchain technology, considering its rapid adoption in the banking sector. In another systematic review [12], the use of Blockchain technology for KYC and its research application areas since 2014 are explored. The authors categorize research works into three types: framework, case study, and review. Framework-based works are further classified into storage-based and encryption-based approaches. The study suggests that profit-based organizations may not significantly benefit from a completely decentralized KYC system, while academic and non-profit organizations may find value in such systems.

The survey article in [13] highlights the growing significance of blockchain technology, particularly in the banking sector. It emphasizes that blockchain's foundational role in Bitcoin and cryptocurrencies contributes to its importance in the financial industry. The paper introduces blockchain as a secure ledger for data transfer, eliminating the need for intermediaries. It distinguishes three main types of blockchains: public, private, and consortium (federated), and discusses various use cases in banking, including KYC procedures, clearing and settlement, trade finance, payments, smart contracts, and syndicated loans. The main objective of this survey is to showcase the potential benefits and impact of adopting blockchain technology in banking operations. On the other hand, the paper in [14] presents a systematic literature review focused on the current state of blockchain technology in the finance sector. It highlights the potential for blockchain to provide a competitive advantage and identifies various dimensions of its application in finance, including its benefits and challenges. However, this review does not specifically delve into the application of blockchain in areas like e-KYC, data security, and integrity.

The existing surveys on blockchain-based KYC lack certain critical elements that would enhance their effectiveness. For instance, [11] lacks a detailed analysis of e-KYC solutions for standardized comparisons and insights into blockchain effectiveness, while also needing uniform performance metrics for blockchain-based e-KYC systems. Similarly, [12] would benefit from a deeper examination of framework-based works to understand their practical applicability. On the other hand, [13] fails to address specific challenges and limitations in implementing blockchain-based KYC systems, and [14] lacks a comprehensive analysis of challenges and recommendations for regulatory compliance, interoperability, scalability, and data privacy.

The study conducts a comprehensive review of articles on KYC and blockchain in the banking and finance industries, contributing significantly to the advancement of knowledge in KYC document verification. It provides valuable insights that can lead to future enhancements in the KYC process. The key contributions of this research are highlighted below, setting it apart from existing studies:

- Comprehensive Analysis: The study conducts an in-depth exploration and analysis of various KYC methods currently used by banks. It takes into account the unique characteristics and challenges associated with KYC in the banking industry.
- New Performance Metrics: This research introduces innovative performance metrics to assess the efficiency of KYC procedures. These metrics focus on evaluating both the accuracy and reliability of KYC processes, enabling a standardized comparison across different approaches.
- Performance Analysis Based on the Metrics: The article thoroughly evaluates the strengths and limitations of existing KYC procedures, utilizing the newly introduced performance metrics. By doing so, it provides a comprehensive understanding of the effectiveness and shortcomings of various KYC methods.
- Identification of Open Research Areas: The study identifies and highlights potential research gaps and areas for improvement in KYC practices. It offers insights into the aspects of KYC that require further attention and exploration to enhance the overall process.

The rest of this article is structured as follows: In Section II, the prospects of blockchain in KYC are examined, shedding light on the technology's potential to revolutionize the KYC process in the banking and financial sectors. Section III refers to the literature review of KYC approaches, blockchain-based KYC approaches, and non-KYC approaches. Section IV discusses the description of relevant parameters for this domain. Section V is devoted to further explanation of existing works explained in Section III. The article provides a discussion of open research areas, presenting opportunities for future exploration and improvements in the integration of blockchain and KYC processes in Section VI. And finally, the paper is concluded in Section VII.

II. PROSPECTS OF BLOCKCHAIN FOR KYC

The prime objective of policies toward KYC is to prevent financial fraud through financial institutions. Failing to

follow the regulations may result in significant additional costs for the KYC process [15]. Other organizations, on the contrary, consider KYC as an opportunity since it allows them to try and understand customers, analyze their needs and patterns, deliver customized goods, and build customer loyalty, all of which result in greater profitability [4]. The KYC procedure has been split into two categories: the traditional KYC procedure and the eKYC procedure for digital modes. eKYC and KYC appear to have very similar processes. KYC onboarding begins with a prospective customer requesting the opening of an account, followed by completing a registration form, identification card verification, and logging into a financial services dashboard to obtain the desired account [16].

A. THE TRADITIONAL KYC

The traditional KYC (FIGURE 1) is a face-to-face approach. Branch offices carry out the entire procedure on paper without any technology used [15]. In this approach, customers have to go directly to the nearest branch office of any financial institution. In the beginning, customers will send the institute a copy of the required paperwork [17]. After that, they will fill out the paper registration form and wait for the verification process to complete [18].

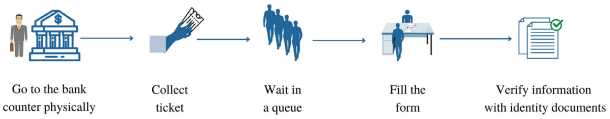

FIGURE 1. Traditional KYC process.

B. eKYC ONBOARDING PROCESS

In order to help with the onboarding process, eKYC (FIGURE 2) converts repetitive manual steps into digital steps. Through this digitization, eKYC is able to revolutionize many financial service business models, such as digital banking, electronic money, fintech lending, and so on [19]. The process increases scalability and provides a concise user experience, even providing instant verification.

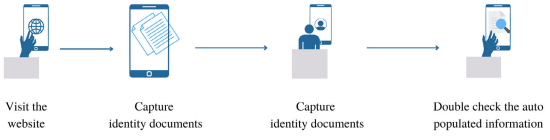

FIGURE 2. eKYC onboarding process.

Regardless of the advantages financial institutions provide to complete the KYC process, they both maintain the papers in a centralized manner such that the customer has no awareness of the status of their documents. The lengthy and repeated registration process at several banks also contributes to the less-than-optimal user experience for corporate customers of banks. The re-usability of a customer's KYC data across multiple banks is particularly limited by the absence of common protocols and institutions' unwillingness to disclose customer information to competitors [1]. Considering the limitations and drawbacks of centralized systems, banks have begun to explore alternatives, one of which is distributed ledger technology [20].

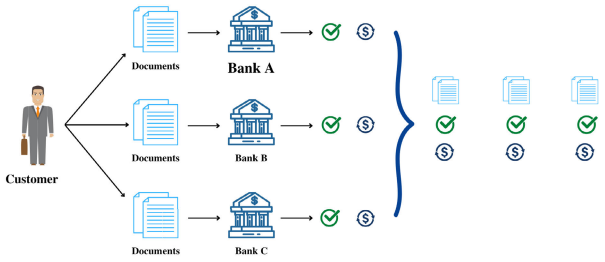

FIGURE 3. Traditional KYC process (without blockchain).

The process shown in FIGURE 3 demonstrates how the current KYC system is implemented in every financial sector. In this system, each financial institute independently confirms the user's identity. For instance, if you intend to open accounts with multiple banks, each bank will carry out its own identity check. The core issue of current KYC systems is that each verification must be tested from the bottom up, which takes time and money. Furthermore, this strategy raises security problems because personal data is transferred from the client to the server with each inspection and can be confiscated.

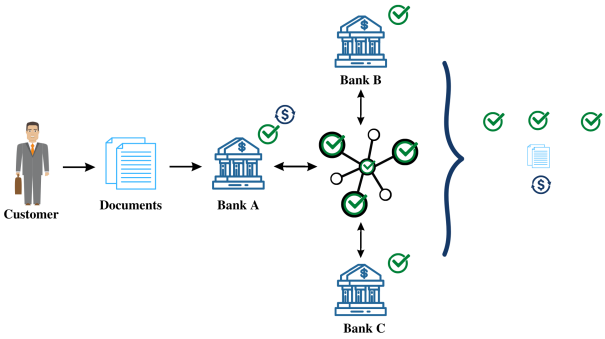

FIGURE 4. Blockchain approaches for KYC.

In the bank example from FIGURE 4, the identity confirmation algorithm will work like this: In order to get any service provided by the bank, a user must submit the necessary paperwork to one of the banks for the KYC procedure. If everything is in order, the bank verifies and confirms that KYC has been completed. The user's information is entered by the bank into the blockchain platform, which is accessible to other banks. When a user requests the services of a different bank, that second bank connects to the system and verifies the user's identity, reducing all the risks and hassles that occur during this process. You can use blockchain architecture to combine data from multiple financial institutes into a single, cryptographically secure, and immutable database,

eliminating the requirement for a third party to certify the data's accuracy. As a result, a system can be developed whereby a user only needs to go through the KYC process once before using this platform to verify his identity. In this system, access to the user's data will only be permitted with his or /her own consent.

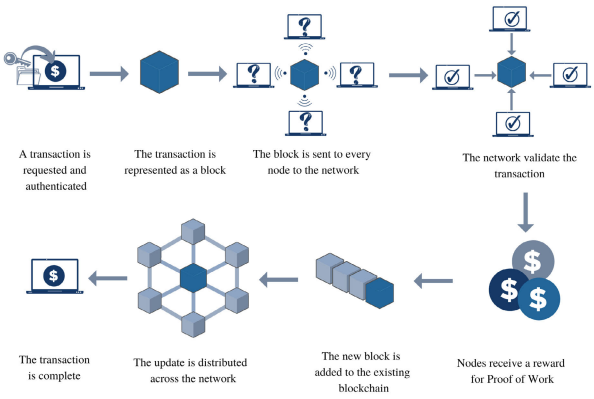

FIGURE 5. The blockchain process.

In FIGURE 5, a peer-to-peer network with many peers that replicates all data and a linked key agreement run by particular nodes to validate state transactions and synchronize all copies are vital ingredients of the DLT [1], [21], [22], [23]. Distributed ledgers are resistant to crashes and malicious behavior by a small set of nodes, giving them a highly accessible and decentralized digital infrastructure. However, DLT has several downsides regarding scalability and privacy. Blockchains are a subset of DLT and are likely the most extensively utilized [22]. The main feature of the blockchain is that transactions are bundled into blocks, and each block of data carries the hash value of the preceding block [21], [23]. As a result, the blocks create a chain with the objective of creating a tamper-resistant record [3]. A blockchain-based, unbiased platform for banks to collaborate on eKYC appears highly tempting because it eliminates the prospect of intermediaries [3].

III. EXISTING WORKS

This section of the paper consists of two parts: The initial part is related to existing works of KYC with the implementation of Blockchain, and the latter part is about KYC without the involvement of Blockchain.

A. KYC RELATED EXISTING WORKS

The ongoing KYC process is tedious and heavily reliant on manual documentation. It lacks a system to monitor the entire process end-to-end, resulting in the potential for deceptive practices. The following example demonstrates the drawbacks of the current KYC system. In the current financial system, banks are obligated to verify their customers' identities. This is an unavoidable and necessary method to prevent illicit practices, known as the KYC process. Financial institutions must undergo this process to verify the identity and credibility of the documents, ensuring that the customer provides no illicit data. Various attempts have been made to address privacy and security concerns associated with confidential documents. The latter part of this section discusses some recently developed systems that propose solutions to the existing problems.

In [24], the authors proposed working with the IPFS protocol and Gpg4win on the Kleopatra platform for privacy. The IPFS system is a peer-to-peer file-sharing protocol that connects computer devices to share files. The main focus of the authors is the implementation of a KYC blockchain system with the help of the IPFS protocol and Gpg4win to solve the system's scalability issues. The authors of the paper have shown results for a scenario in which the bank encrypts the customer's verified documents, uploads them to the IPFS network, and with the help of the hash keys, customers can open another bank account without the repetitive hassle.

The authors in [15] demonstrated the architecture of centralized and decentralized blockchain KYC solutions, with the division of processing expenses among multiple institutions. The authors first collected feedback from senior executives in the banking sector. Their feedback emphasized the importance of interbank interaction and cooperation with the government, as well as the need to begin the process in a specific, relatively small country and ensure the system runs smoothly. After presenting the problems and analyzing related work from other papers, the authors presented a new DLT-based scheme to reduce the cost of core KYC verification while improving the user experience. They primarily focused on proportionality, irrelevance, privacy, and non-minting. The authors' concept was effective, but they did not address the fact that block data would expand over time and increase expenses.

In [25], the authors recommended implementing regtech (regulatory technology) in the banking industry to lessen the burden of the KYC procedure on both financial institutions and regulatory institutions. According to [25], the scope and business model of Regtechs differ from those of Fintechs. Instead of competing with financial institutions, they provide solutions to them. Tax reporting can also be done using this method. This procedure requires banks to identify the client's tax status concerning the country in which they are a financial resident. The client will provide this data to the bank as part of their identification information. However, the author did not reveal the full deployment of blockchain and the costs associated with the process.

The authors began by analyzing [26] comparable works, illustrating the various outcomes and platforms employed. This paper addresses the trust issues that arise during transactions between banks. The authors have planned an effort to ensure anonymity and accountability between parties by reducing the inconvenience for customers and staff due to unnecessary repetitive procedures. Both have used mathematical tools to describe their planned tasks. Bhatti Pralhad Rankhambe and Dr. Harmeet Kaur Khanuja have developed an approach using Blockchain and smart

contracts to enable financial organizations to enhance their anonymity. Following an extensive investigation, they have decided that the system should be divided into two parts: the application layer and the code base. The application layer is concerned with the user interface, through which documents are submitted by the customer. To improve confidentiality, all programming takes place in the code base, which begins with the local database of each bank and is saved on the Blockchain network of the system.

The paper [27] analyzes the challenges and opportunities of integrating Blockchain technology across the banking industry and providing food. The article highlights two weaknesses: the large-scale energy usage and expensive hardware costs. The effective Bitcoin system practice assesses the network's hash rate and electrical power over time. The authors have identified three quantities addressing the Bitcoin system's drawbacks and Blockchain's consequences. The quantities are Economic Efficiency (EE), operational efficiency (OE), and efficient service (ES). Due to the popularity of Bitcoin and the network's power consumption, which is currently increasing as a result of the rise in the value of bitcoin, EE, the ratio of the number of bitcoins generated to the power consumed per kWh, is defined by significant variation. The growth of OE shows fees are becoming increasingly crucial to ensuring the sustainability of the Bitcoin system. In reality, mining operations won't be paid out until there are 21 million bitcoins in circulation. ES is the ratio between the number of transactions validated by the power consumption of 1 kWh. It describes the amount of electricity the network spends to perform its principal service, i.e., to transfer bitcoin. The number of transactions per block is constrained due to the size restriction on transaction blocks (1 MB), and the ES is unable to expand.

The article [16] has used the Hyperledger Composer to test the performance of the proposed system. The experiment result confirms the proposed system can speed up KYC clearing transfers, challenge inefficiencies caused by the duplicated performance of similar tasks, secure data sharing, be cost-effective, and ultimately bring transparency to the traditional KYC system due to the robust and identity features of Hyperledger Fabric. The authors in [16] have suggested a Blockchain Hyperledger Fabric network for client KYC optimization. The global difficulty is shouldering the regulatory costs paid by all financial institutions as a result of the KYC verification process. Besides, KYC demands can also delay transactions, with the customer verification procedure lasting 30 to 50 days. Blockchain technology would enable banks to implement a decentralized KYC system. All KYC archives created by smart contracts could be encrypted and stored on distributed ledgers.

KYC is a verification process used to authenticate customers and verify their identity. Institutions examine users' information through KYC in various ways. Reference [28] demonstrated the advantage of KYC with blockchain technology and explained with mathematical reasoning how institutions benefit from blockchain implementation. In every application, the smart contract design of blockchain technology reduces the verification cost of identification documents from $c \times n$ to $\frac{c}{n-1}$. However, the blockchain-based system returns cost $\frac{c}{n(n-1)}$ to the institutions. So, the blockchain-based verification system costs

$$\frac{c}{n-1} - \frac{c}{n(n-1)} = \frac{c}{n} \tag{1}$$

Here, in (1), c defines cost; n defines the total number of institutions, and 1 is for the first institution that verifies customers' documents for the very first time. The traditional process does not return any amount for verifying the same identity documents multiple times. The system emphasizes the impact of KYC document verification with blockchain in financial institutions and gives a clear sense of the work behind blockchain implementation in a system. Moreover, it analyzed the Accreditation, Verification, revocation, privacy, and Accessibility parameters presented in the context of specific schemes.

Authors of the paper [29] showed that medical reports are sensitive. In most cases, medical reports are partially accessible in the research and insurance sectors. Users share their data to get medical services. Users provide necessary documents to insurance companies. Insurance companies investigate and provide services accordingly. The process between medical service and user reports is complex. A Blockchain-based hyper-ledger framework is a solution to the hassle. Integrating the system into the service creates trust and transparency. User-centric Blockchain technology for personal health data is highly interoperable and compatible with current systems. Access control policies might have privacy issues in the system. Requesting healthcare providers and health insurance companies to insert data in the Blockchain network makes personal healthcare data accountable.

The authors of the paper [30] highlight the risks of KYC in a country with a large population. Instead of approaching Blockchain technology, Anurag Soni and Reena Duggal have experimented to reduce the risk with the help of big data analysis. Both authors identify several problems that might be considered to be fraud-related activities. For instance, a customer could report multiple addresses, resulting in the creation of multiple identities. Due to this, banks are having a very difficult time tying together the various accounts and services that a customer has used while doing business with them and offering a truly unique customer code. The customer is responsible for linking every account. Thus, big data analysis was conducted by them, where it first performs the KYC process, then compares ID proof of consistency, and after that, compares address proof for a customer by the addresses of different cities and keeps tabs on scores. The authors then used the fuzzy matching technique to generate a key-value pair to compare easily. After analyzing each method, the MapReduce technique has been used to execute massive amounts of data into chunks and compare big data

according to names, addresses, cities, and phone numbers as well.

The paper presents ''Casper,'' a novel blockchain-based system designed to enhance the efficiency and security of customer credential verification processes [31]. In response to challenges such as data breaches and inefficiencies in traditional verification methods, Casper leverages blockchain technology to create a decentralized and tamper-resistant platform. Furthermore, smart contracts in Casper automate the verification process, ensuring the integrity and immutability of customer credentials stored on the blockchain. The system's reputation-based consensus mechanism incentivizes honest participation and enhances efficiency by encouraging resource contribution. Furthermore, privacy features, including zero-knowledge proofs and data encryption, safeguard sensitive information during the verification process. The paper has also highlighted that comprehensive simulations and experiments demonstrate Casper's better performance compared to existing centralized and decentralized systems. Casper's versatility enables applications in various domains, such as healthcare, banking, and governmental organizations. It serves as an inter-bank KYC platform for banking customers, providing them control over their data and enabling secure sharing of identity information with other entities. The evaluation studies show that Casper is scalable and can provide high transaction throughput. The authors further claims that the proposed system exhibits increased efficiency, lower costs, and enhanced security.

This study explores the implementation of a decentralized energy datahub [32]. The authors propose a blockchain-based platform to facilitate secure and transparent communication of energy data among stakeholders in the energy sector. Emphasizing the importance of a robust business ecosystem, the paper further discusses governance frameworks, incentive systems, data privacy and security, interoperability, and stakeholder cooperation. The Model introduces a semi-open ecosystem where participants, especially end-users, can actively engage and monetize their data on the blockchain. To meet regulatory requirements, a Hybrid Permissioned blockchain approach is employed, enabling KYC protocols and addressing scalability challenges. According to the article, control is distributed across different levels, with government or regulators orchestrating at the control level to address issues like regulation for monopolistic players. Furthermore, Consensus among blockchain participants governs the system at the business model level, ensuring decision-making is decentralized and driven by the participants' protocols.

The article [33] explores implementing KYC processes using blockchain technology, focusing on the e-KYC solutions. The authors have highlighted the challenges in the traditional KYC methods, such as time-consuming manual processes and data redundancy across institutions. The article later proposes leveraging blockchain's decentralized and secure nature to create a single, cryptographically protected database for KYC data, enabling verified financial institutions to share and access information efficiently. The proposed system aims to use blockchain to enhance compliance outcomes, efficiency, and customer service. As blockchain gives systems transparency, immutability, and data privacy in the KYC process, the authors claim that the proposed system supports a user-centric, decentralized, and blockchain-based solution for quick and safe consumer identification verification in financial institutions.

The study [34] analyzes the use of blockchain technology to enhance the KYC procedure, in particular the Ethereum-based Optimized KYC Blockchain system with Fully Homomorphic Encryption (FHE) and other cryptographic techniques. The manual KYC process is deemed time-consuming, costly, and less secure, which the proposed solution aims to address through blockchain's characteristics like consistency, security, and geographic variety. In the article. KYC is described as a regulated practice used by banks to gather customer information, verify identities, and prevent service abuse. The proposed solution aims to streamline the KYC identification process, reducing costs, time, and improving client satisfaction. The use of FHE enables secure processing of sensitive information without exposing it in plaintext, enhancing transparency in the customer transport network. Additionally, the Vickrey auction on the Blockchain ensures honest bidding based on assessed worth, while Smart Contracts facilitate fair and confidential bidding among participants.

CODE is a decentralized blockchain-based solution or compliance with FATF recommendations. Reference [35] CODE uses Corda to provide safe data exchange and storage within essential parties as the underlying blockchain technology. The system proposes an address-search technique without involving all VASPs in information sharing. The technique fastens beneficiary's identification confirmation and gives the reliability of elimination intermediaries, which enable the secure administration of personal information for compliance with travel regulations. The authors intend to undertake a performance evaluation to align with the expectations.

B. EXISTING WORKS WITHOUT KYC

The use of blockchain technology is increasing over time for building secure, scalable, efficient, and reliable systems. KYC is giving the technology extra advantages in authentications. Besides finance industries, this technology is also getting popular in other sectors. Various sectors have integrated Blockchain technology; however, not all systems have KYC advantages.

The article [36] focuses on the shortcomings of the previously offered approaches. To begin with, it commenced with an overview of Blockchain's qualities and characteristics that cannot be overlooked. The authors are primarily concerned with authentication, authorization, confidentiality, ownership, and privacy. The author prepares a comparison table based on related work to the KYC area and highlights

the shortcomings of each solution offered. Based on the findings, the authors have proposed a better and more efficient approach for certifying educational certificates using Hyperledger. As per the authors, Hyperledger would provide greater security because it is a private Blockchain framework that keeps records locked. With the support of the Hyperledger Fabric Framework and the benefits of Hyperledger, authors have come up with a proposal for a Blockchain-based framework to verify educational degrees depending on some specific parameters.

The authors of the article [37] have proposed a blockchain-based document verification system for job applicants. The authors proposed a consortium blockchain in which universities, businesses, law enforcement, doctors, and certifying organizations have the ability to upload information to the blockchain. All of these papers will be reviewed by an administrator node before the hash values are calculated and saved to the blockchain. Once the transaction is accepted, the hash value of the document in the transaction, as well as the hash value of the identifier, are determined and then sent to the consensus mechanism to update the blockchain. When a job candidate presents his documents to the hiring manager during the recruiting process, the hiring manager uploads the documents to the blockchain-based hash verification web application and compares both hash values for a match. If the results come otherwise, then it would be obvious for the recruiter whether the job applicant is suitable for the post or not.

This paper [38] talks about the Value Added Tax system that is still centralized and is at high risk to be hacked. The authors of this paper proposed a better and more secure system using Blockchain. Their proposed system authenticates the transactions, calculates the VAT, and approves payments too. They planned to use the decentralized storage system network amalgamated with smart contracts. Their system runs on a host PC for encrypting and decrypting data. The smart contract works on the Ethereum platform to increase privacy. They have used the Remix IDE which helps in scripting, compiling, and debugging the smart contract with solidarity language.

The authors in [2] have attempted to solve the problem of manually forged educational documents, which has increased the anticipation of paper load. As millions of students graduate each year, such issues arise. The proposed framework consists of a multi-node private Blockchain built on the Ethereum platform and an off-chain storage system such as IPFS. On open stock, they have carried the Ethereum network using Geth. The proposed system also demonstrated the impact of load, network size, and difficulty in analyzing node stability, complexity level, and consensus mechanism.

The article is about the complications and safety issues of the existing payment method. The authors [39] have proposed an automatic gas payment system using Blockchain where the bitcoin transaction platform will ensure safety. Additionally, the authors' experiment result shows the feasibility of bitcoin gas payment and better performance using a hardware crypto chip instead of a software crypto library.

Electric vehicles require charging to operate properly. The analysis of the article [40] shows a chance of owner location rather than the user who charges the electric car. It will be charged when an electric vehicle is charged from a power source at a location other than the user's house. Furthermore, charging in public areas makes it much more difficult to track down the person who has charged the electric car, making the situation even more complicated. As a result, the present international standard for mobile issue charging for electric cars is inadequate and includes several unresolved problems that must be resolved. For example, deciding on how to apply the billing to real users is one of them. Relying on financial institutions, people may suffer from the trust-based model's fundamental flaws. Findings the authors of the paper proposed a mobile charger billing system using lightweight Blockchain for business dealings that take place directly between trade partners and do not involve a reliable third party.

This article's [41] discussion centers on switching manual learning systems to digital ones. The authors have shown the problem of manual certification that can be forged easily and shown to anyone, anywhere. Given the importance of certificates in education and professional growth, it's essential that the records be secure and always accessible. In this study [41], the authors discuss the Blockchain for education platforms as a potential method for creating, exchanging, and authenticating certificates. The platform prototype is constructed on the Ethereum Blockchain, and along with this, two solidity smart contracts are created. The IdentityMgmt contract is for access control managed by the accreditation authority. The CertMmgt contract is for storing records in the Blockchain and is managed by the certification authorities. The Interplanetary Filesystem (IPFS) is utilized as a public, distributed read-only storage system for certifying authority profile information. Finally, the certificate is stored and validated by the Basic Support for Cooperative Work (BSCW) document management system. However, the missing part in the authors' proposal is that even though it's Blockchain-based, it still follows the hierarchical centralization model where the accreditation authorities are the main source. Thus, if the private key is somehow compromised, then the whole system would be affected.

The authors in [42] displayed that in most cases, third parties steal original audio and music files, images, and video/movies and releases before productions release. This situation causes a significant loss for distributors, producers, and artists. Furthermore, unauthorized release hampers privacy. Multimedia relies upon and permits sharing of data with third parties to maintain their publicity in multimedia. As insertion from the user end is vital, a media person should have the authority over controlling his data. In this case, a user has to be aware of accessing his data and when it is happening. A Blockchain-based Data Lake framework proposal can ensure data privacy and control without

compromising authenticity to third parties. Additionally, once the Blockchain network verifies data, it can be used in sales and distribution without concern over security and copywriting.

NovidChain, introduced in [43], is an innovative blockchain-based platform aiming to enhance the security and privacy of COVID-19 test and vaccine certificates. The proposed system utilizes blockchain technology's characteristics of immutability, transparency, and decentralization to ensure the integrity and privacy of health data by eliminating the need for a central authority, reducing data tampering and unauthorized access risks. The platform prioritizes privacy preservation through advanced cryptographic techniques like zero-knowledge proofs and homomorphic encryption, enabling verification without compromising personal data. The proposed system comprises a smart contract layer, distributed ledger, and user interface, with a consensus mechanism ensuring transaction validity. Therefore, the platform offers potential benefits such as reduced fraud, streamlined verification processes, and improved data interoperability in healthcare systems. Nonetheless, challenges like scalability, adoption barriers, and regulatory considerations are acknowledged in this article. According to the article, this proposed system offers a promising solution for secure and privacy-focused management of COVID-19 test and vaccine certificates, empowering individuals, healthcare providers, and authorities during the pandemic.

This study proposes a Proof of Transaction (PoTx)-based traceability solution for the agricultural supply chain [44]. A decentralized and transparent network for following agricultural products from their point of origin to consumers has been created by the system using the blockchain technology. The solution ensures real-time data collection, secure data exchange, and automated transaction verification by combining smart contracts and cryptographic methods. The article claims that this improves supply chain accountability and transparency while addressing the drawbacks of current tracing solutions. The design and implementation of the PoTx system using smart contracts and blockchain components form the core technique of the proposed traceability solution. By leveraging these technologies, the system ensures real-time data collection, secure data exchange, and automated transaction verification, enabling a decentralized and transparent network for tracking agricultural products in the supply chain. This approach enhances supply chain accountability and transparency, providing stakeholders with reliable and dependable information. Thus, it improves the overall trust and efficiency of the agricultural supply chain.

The article introduces a framework for blockchain-based multi-level marketing (MLM) platforms that prioritizes privacy [45]. The proposed framework aims to enhance privacy and security within the MLM sector by leveraging the blockchain technology. The paper also highlighted that the proposed system employs various methods, including encryption, pseudonymity, and selective disclosure, to safeguard participant data, transaction data, and confidential company information. The framework for blockchain-based multi-level marketing (MLM) platforms prioritizes openness and accountability while protecting sensitive data by leveraging the decentralized and transparent nature of blockchain. The system enforces automated regulations through smart contracts, ensuring a trustworthy and secure MLM environment. To tackle scalability challenges, the platform adopts techniques like sharding and off-chain solutions, optimizing performance and accommodating a growing user base. This comprehensive approach enhances privacy, security, and efficiency in the MLM platforms.

The paper introduces SmartDID, a decentralized identity system aimed at addressing privacy issues in IoT applications [46]. The authors identify shortcomings in current identity management systems used in the Internet of Things and propose SmartDID as a privacy-preserving alternative. The system leverages blockchain technology and cryptographic methods to ensure tamper-proof identity data storage and privacy protection. Notably, it incorporates key features like zero-knowledge proofs, user-centered control, and selective attribute disclosure. The paper delves into the architecture, components, and applications of SmartDID, providing a comprehensive understanding of how this decentralized identity system can be integrated seamlessly within diverse IoT ecosystems. By implementing SmartDID, IoT applications can benefit from heightened privacy and security measures, fostering greater trust and confidence among users, service providers, and stakeholders.

The paper introduces a blockchain-based healthcare platform designed to securely and efficiently manage electronic health records (EHRs) [47]. The system utilizes smart contracts for automated and tamper-proof record management, ensuring the integrity and reliability of health data. To address scalability challenges, off-chain storage is employed, enhancing the platform's ability to handle a large volume of records. Emphasizing data privacy, user-centricity, and access control, the platform enables secure and regulated exchange of health information among various healthcare professionals and patients. By placing a high priority on these aspects, the system fosters trust and confidentiality in healthcare data sharing.

IV. PERFORMANCE METRICS

Blockchain technology is a combination of many different technologies, including distributed consensus algorithms, cryptography, and mathematics [15], [36]. Certain requirements must be met for KYC document verification and insertion into the blockchain network, including,

A. AUTHENTICITY

The capacity to verify requesters' identities before granting access to critical information [36]. With blockchain authentication, the block's hash containing personal data must confirm a person's identity, such as a unique identification number.

B. ANONYMITY

Anonymity has lackings in identifying recognizable identifiers for an entity to identify a user [48]. For instance, the bank can examine the anonymous user's online behavior, such as transactions, without identifying personal information.

C. ACCOUNTABILITY

A person or a business can be subject to an audit and held accountable for any improper action [49]. Accountability is a concept that establishes a ''relationship of duties'' between two or more entities [50], [51]. Accountability reflects a concept that affects organizations, individuals, and society in general, [52].

D. AVAILABILITY

Enables blockchain nodes to check whether data for a proposed block is available without downloading the entire block [53]. In other words, it is the assurance that a block applicant released all transaction data for a block and that the data is accessible to other network participants [7].

E. CONFIDENTIALITY

Private information about the consumer is covered by confidentiality standards, and financial institutions can keep this data safe. Here, the client is in charge of disclosing information to third parties (banks) for verification as necessary [39], [53].

F. CONSENSUS BASE

All nodes are qualified to transfer and update data safely, providing a consensus basis for the system. This is because nodes are publicly connected on blockchains and modifications can only occur when a majority of nodes accept the change [39].

G. DATA AUDITING

Audit logs can be used when conflicts emerge as evidence to hold requestors responsible for their interactions with KYC. Some systems use blockchain technology and smart contracts to maintain records for audibility. The blockchain ledger saves all transactions and requests, which can all be retrieved at any time [53].

H. IMMUTABILITY

By using a one-way cryptographic hash algorithm, it is extremely challenging to delete or edit any entry in any block within the blockchain [39], [48]. This feature displays the ability of a blockchain ledger to preserve a lasting, irreversible, and unchangeable record of data [54].

I. SYSTEM COMPLEXITY

The interaction between a system and an observer results in the dependent property of system complexity. It is a quality revealed only through the interaction of one system with another. Complexity is not an inherent feature of a closed system; it is only manifested by the system's interaction with another, typically during the measurement and control process [55], [56].

J. NON-REPUDIATION

Participants cannot dispute the transaction and behavior within a transaction in a blockchain due to non-repudiation. Non-repudiation technology serves the objective of gathering, preserving, providing, and confirming irrefutable proof of transmissions from the transmitter to the recipient [22].

K. OFF-CHAIN

Users can quickly locate KYC data and escape the storage restrictions of the blocks by exchanging data between multiple banks [57]. Off-chain transactions are those verified away from the central blockchain system, typically resulting in a cheaper and faster transaction for the user.

L. PSEUDONYMITY

The identity of a user is unknown in a transaction; however, it is possible to identify and track the individual behind every action they take [58]. In this case, the banks are pseudonyms as their names will be unknown to other banks, but their transaction history will be available and linked to the same individual.

M. PRIVACY

Personal details will be used in confidence, and therefore, only individuals with consent may access the required information [53]. Blockchain technology allows individuals to own data by using private and public keys. When private information is stored on the blockchain, the owner has control over when and how a third party can access it.

N. ROBUSTNESS

If a blockchain is resilient, it can sustain the network and its nodes, running smoothly. All nodes should be running effectively and doing transactions without interruption in order to maintain the overall blockchain's health [59], [60].

O. SCALABILITY

A network is said to be scalable if it can expand in response to user demand [53], [61]. In the case of banking, it shows how well the system can manage the increasing number of data like the number of bank accounts [62].

P. LIGHTWEIGHT SOLUTION

A lightweight solution is a simplified algorithm that reduces data size and stores them within the blockchain network without sacrificing users' data privacy. This algorithm provides significant efficiency enabling quick and direct access to the blockchain network. Besides that, the solution has the advantage of simplifying unparallel symmetric digital solutions [63].

Q. TRANSACTION LATENCY

A blockchain performance metric evaluates the time frame of completing the transaction in a blockchain network and is measured in milliseconds (ms) or microseconds (µs). The total time of adding a transaction in a block and blockchain by mining is Transaction Latency [64].

R. TRANSACTION THROUGHPUT

A critical blockchain performance metric to measure the total successful transaction within a period of time that measures in transactions per second (TPS) or transactions per minute (TPM) unit. [65] Other factors such as block size, block time, consensus mechanism, network latency, and scalability solution influence transaction throughput for a better outcome [66].

S. BLOCK CREATION TIME

the average time of creating a block for traction in a blockchain is referred to as the block creation time. The block generation time may differ for its consensus mechanism and design choice. The shortest period of time is the best for the best performance. The unit of it is measured in s [67].

T. CONSENSUS ALGORITHM EFFICIENCY

Blockchain consensus algorithm efficiency describes how quickly and efficiently a network obtains consensus on transactions. To ensure optimal blockchain performance, it involves speed, scalability, resource utilization, and security. Different algorithms, like Proof-of-Work (PoW) and Proof-of-Stake (PoS), try to find the ideal balance for various networks [68].

U. DATA STORAGE EFFICIENCY

Blockchain data storage efficiency entails optimizing storage to reduce redundancy and overhead while maintaining scalability and sustainability. Blockchain data storage efficiency involves optimizing storage to reduce redundancy and overhead while maintaining scalability and sustainability. Techniques like pruning, compression, and sharding are essential for achieving this. Off-chain solutions and incentive systems also enhance efficiency. Balancing scalability, security, and decentralization is crucial for maximizing storage effectiveness [69], [70], [71].

V. PERFORMANCE ANALYSIS

Existing works have been reviewed in Section III. This section refers to a thorough investigation of Section III. The study of this section provides a clear sense of the advantages and disadvantages of existing work having specific parameters, as defined in Section IV.

A. KYC RELATED EXISTING WORKS

Considering system complexity, [24], banks have integrated Blockchain into their system to reduce privacy violations and ensure transparent user data. Data sharing accessibility allows one bank to access another's data with limitations, and private information is shared according to users' requirements for service. Smart contracts of Blockchain eliminate third parties and ensure privacy. On the other hand, KYC confirms the identity of financial institutions associated with the system. The IPFS protocol and Gpg4win in the Kleopatra platform can be used to maintain privacy. The verification system confirms the encryption mechanism for verifying customer documents and uploading verified documents to the IPFS network. Once the information is verified, private keys make data visible without the repetitive hassle. Anonymity makes data visible in the system without exposing information. In contrast, the system's Pseudonymity makes the transaction process anonymous in the stage when it is necessary. The lightweight solution feature ensures data transactions without compromising privacy. Additionally, off-chain technology ensures external data is shared with concern. In a bank, various types of transactions occur, and end users need a clear understanding of them. Blockchain technology is transparent and requires a high demand in society; transactions may have user-centric accountability. The banking system's immutability feature keeps data transparent with transaction history. Edition and deletion of data are only allowed with validators' concerns. IPFS and Blockchain Technology used in banking employ consensus mechanisms and PoW to insert information into the Blockchain. Data auditing assures the confirmation of validity before inserting it into the blocks. The article [24] lacks an examination of the system performance in key aspects of a blockchain network, such as transaction latency, transaction throughput, block creation time, consensus algorithm efficiency, and data storage efficiency. Without precise performance measures, evaluating and improving the system becomes challenging. It remains unclear whether the network can support real-time transaction processing or if delays may arise due to a lack of visibility into transaction latency. Additionally, the absence of transaction throughput data hinders analyses of scalability, preventing us from understanding how many transactions the network can handle concurrently. Moreover,the lack of information on block creation time further complicates assessing the overall network efficiency and transaction confirmation speed. Moreover, without metrics for consensus algorithm efficiency, it is difficult to evaluate the security and effectiveness of the consensus protocol. Lastly, the absence of assessments on data storage efficiency makes it harder to estimate the blockchain network's scalability and sustainability, potentially leading to inefficient resource utilization and restricted accessibility.

KYC without blockchain is costly, and 89 percent of customers do not have a good experience with this process. However, KYC is fundamental to building trust between customers and businesses. The current KYC process requires the same document to verify individuals multiple times when financial institutions need to work with individuals for multiple purposes. As a result, financial institutions must deal with the same document when customers need any service.

Distributed Ledger Technology (DLT) allows KYC to track down which documents customers have submitted, which saves KYC from redundancy [15]. System complexity is low for integrating DLT technology into the existing KYC process. Data sharing and access control are ensured using a private blockchain in the proposed system of [15]. The total KYC verification cost (2) of an institution without DLT is $c \times i$ where $i \geq 1$. Here, c refers to the cost of verification, and i refers to the number of institutions. An Ethereum-based smart contract design reduces the verification cost for institutions up to $\frac{c}{i-1}$ where $i \geq 3$, and $i-1$ refers to the institutions that have already worked with the same customers. As a result, an individual has to pay $\frac{c \times i}{i}$ for his verification, where $i \geq 1$. The advantage of optimizing KYC with DLT returns money to each financial institute $\frac{c}{i(i-1)}$ where $i \geq 2$ refers to the number of institutions in the system being more than 1. As a result of this, the cost of verification against each financial institution is

$$\frac{c}{i-1} - \frac{c}{i(i-1)} = \frac{c}{i} \tag{2}$$

The off-chain facility gives the system the advantage of inserting verified data from the 'home bank' into the local document package. The process also stores the verified hash value in the blockchain later. The lightweight solution helps the system not to compromise any data while managing regulators, such as regtech (a combination of Regulation and Technology). The feature of user-centric design presents a seamless interface between the user and the user management module. Pseudonymity allows the system to identify transactions without revealing complete information about the verifier, which is not considered. The anonymous document transaction gives financial institutions more control over the system regarding verification. The immutability feature works as a reference for trustworthiness among financial institutions and helps execute interbank transactions. The privacy of the system serves as a center of confidentiality, and concern is required for data sharing. Cluster analysis over the network helps the system authenticate and find potential customers. The system's structure allows for the advantage of accountability by giving feedback to KYC practitioners. Confidentiality ensures the privacy of financial institutions, their customer transactions, and personal data. Financial institutions do not agree to share all financial information available in the network. The proposed system of authors moves the verified hash value of documents from the local database to the DLT first. Then the available information helps to sort out unnecessary occurrences quickly.

The scalability of the system can perform with the growing transaction list, a feature that is absent in the system. DLT gives the system transparency, an advantage of reliance for both customers and financial institutions. As a result, financial institutions can track down ethical and unethical transactions and protect themselves from Anti-Money Laundering (AML), external hacking, and terrorist attacks. Instead of PoW and PoS, a different type of consensus mechanism is used in the system to build trust, security, and transparency. Data auditing helps verify the authenticity and root of transactions over the network and increases its effectiveness. Non-Repudiation provides undeniable evidence for every transaction from the transmitter to the receiver. The robustness of DLT helps the system operate properly. Additionally, the feature notifies of imbalances inside nodes and keeps transactions unhidden. The article lacks precise numerical data on block formation time, consensus algorithm efficiency, transaction throughput, and data storage efficiency [15]. This hampers the comprehensive evaluation of the DLT-based KYC solution's effectiveness and efficiency. The absence of specific metrics restricts our understanding of transaction speed, capacity, responsiveness, and data storage capabilities.

The current KYC process is time-consuming and becoming a burden for financial institutions. REGTECH can offer a solution to this issue. Additionally, it can verify identity and monitor transactions [25]. The system complexity is low for the implementation structure of REGTECH. Data sharing and access control are highly maintained for individual identity verification and tracking down against tax calculation by the government. The pre-defined program, designed with contractual conditions, enables the system to operate individual identification and verification effectively. Apart from financial documents, many other types of information may be shared regarding tax calculation, which only needs to be shared with some entities. The off-chain facility allows the system to do so. A lightweight solution is not considered in the system from the perspective of government involvement in the financial sectors of the proposed approach. The user-centric design of REGTECH provides the advantage of utilizing the system within the context of society. Pseudonymity is not available due to no necessity for anonymous transactions in tax reporting. Anonymity is strictly ensured in terms of the verification process. Besides organizational verification, sometimes the leaders of an organization might have to verify on behalf of the organization. Exceptional cases can occur when significant transactions happen against an individual. The REGTECH solution scans individuals' financial transactions and checks them against their regulations, making the system immutable. In terms of privacy assurance, blockchain compliance gives the system extra security for professional entities (KYC). The digital signature ensures the authentication of individual identity verification. Accountability is maintained in REGTECH integration with Blockchain because regularity is the main priority. Tax and other financial sectors have confidential documents of their own. The system manages high confidentiality against individuals' financial statements. REGTECH integration on Blockchain gives authorities the advantage of investigating individuals' statements with the help of availability. Scalability ensures the whole system's performance, measuring processing demand and non-parallel transaction growth. The transparency of REGTECH on Blockchain increases the system's reliability by providing real-time financial

transaction records. The consensus mechanism gives the system the advantage of operating successfully without third parties involved, which needs to be more noticed in the system. The data auditing feature gives the system the advantage of account on the transaction against individual accounts. The Non-Repudiation feature of the system refers to regular users' specific access to detailed financial data. Robustness analyzes the performance by measuring system error and cost-effect variation and reports the issues to be resolved for better performance. The absence of numeric results for transaction latency, transaction throughput, block creation time, consensus algorithm efficiency, and data storage efficiency in the paper hinders the ability to quantify and assess the performance of regulatory technology and blockchain solutions. Efficiency gains, cost reduction, and customer satisfaction, identify bottlenecks, compare different solutions, and make informed decisions are harder to make for improving regulatory reporting and KYC requirements in the financial industry.

IoT-based smart devices utilize prepaid cards or mobile devices as a payment medium [26]. The system complexity's availability identifies the problems and challenges in the payment medium for the system. In most cases, Blockchain-based smart contracts help remove third parties from completing payment procedures. This feature increases privacy over the internet in payment mediums. However, the system does not offer off-chain capabilities, resulting in the system only being able to execute the payment procedure with an internet connection and an external connection. The system is not user-centric, meaning it is not dependent on the user, and the development process is no longer reliant on the user. Anonymity allows the user to keep their information anonymous in the network, whereas the absence of pseudonymity exposes users' information. The Blockchain-based transaction process is nearly impossible to alter or change, ensuring privacy and trustworthiness. As a result, the system provides confidentiality. The hardware application might hamper security; however, a conscious mechanism must be implemented to maintain security. The absence of accountability does not consider who is responsible for any occurrence in the system. Non-repudiation maintains undeniable evidence of verification of the micropayment system, and robustness deals with unwanted exceptions in micro-transactions. The paper [26] lacks numeric results for transaction latency, transaction throughput, block creation time, consensus algorithm, and data storage efficiency rate. This absence of specific data limits our understanding of the system's speed and feasibility. The lack of transaction throughput data makes it challenging to assess data transfer efficiency over time. Additionally, without block creation time, we cannot determine the time taken to generate a block. The absence of an efficient consensus method hinders quick transaction validation and overall network efficiency. Moreover, the paper does not provide numeric values for data storage efficiency, which impacts data retrieval and access speed while also affecting costs. The absence of these numerical metrics limits a comprehensive evaluation of the system's performance.

Integrating Blockchain into an existing system can be time-consuming and complex [27]. System complexity ensures the assessment of challenges and threads in integrating Blockchain technology. Controlling data in a system and maintaining limited access to data are essential for security. Data sharing and access control features maintain accessibility based on predefined permissions, enhancing security. Smart contracts help reduce unwanted third parties and build data more securely between users and banks. Blockchain maintains user privacy and confidentiality when sharing information initially provided by the user. A Blockchain-based framework may have an off-chain feature to share information with a limited number of individuals externally from the Blockchain network. However, in this situation, banks may face threats to privacy. Blockchain provides secure transactions over the internet in payment by ensuring user or validator information remains anonymous. In banking, authorities often keep their information private, relying on anonymity. Pseudonymity partially enables anonymity at specific stages to maintain system security. The Blockchain-based banking system can be user-centric or non-user-centric, depending on the banking procedure. It may provide a demo for users to understand the underlying processes. Authenticity ensures users' information is protected and updated in the Blockchain network. The system does not prefer data deletion and keeps records with timestamps.

Confidentiality is maintained according to a bank's rules and regulations. Accountability is also maintained in the system regarding data sharing with third parties, who sometimes play the role of guarantor. Data can undergo an investigation process with the data auditing feature. The document on integrating Blockchain in banking also provides non-repudiation to collect, provide, verify, and maintain undeniable evidence about user transactions and behavior. Moreover, the document demonstrates robustness to deal with unwanted occurrences and resolve issues.

The system in [27]utilizes the PoS consensus mechanism, offering benefits like energy efficiency, environmental friendliness, decentralization, and security compared to PoW. PoS reduces the carbon footprint and promotes decentralization by not favoring players with expensive mining gear. The block creation time plays a crucial role in the system's cost, energy efficiency, and scalability. Optimal block formation time leads to faster transaction confirmation, higher throughput, and resilience to forks, minimizing delays and potential chain divergences. Blockchain systems may encounter challenges related to transaction delays, high throughput, and data storage efficiency. Instant confirmation raises the risk of double-spending attacks, and a lack of transaction throughput limits scalability, resulting in costly and delayed transactions. Ineffective data storage can lead to inflated blockchain sizes and synchronization delays, impacting network users.

Blockchain implementation in KYC explores various features in the context of KYC verification. The system complexity of [28] is medium for implementation on a private blockchain. The data sharing and access control feature ensures a secure data sharing process and protection. Two different types of smart contract design help the system share verified information through the public key of the 'Home Bank.' The Home Bank verified data storage process provides the advantage of an Off-Chain facility, and the lightweight solution allows for storing validated data smoothly without compromising real data privacy.

The system does not refer to any user-centric design for providing conceptual information about blockchain integration in the system [28]. The theoretical concept of the authors' proposal does not mention pseudonymity for delivering fundamental concepts. However, blockchain technology offers the advantage of executing transactions anonymously, leaving a connectable link against transactions. On the other hand, a financial institution gets anonymous compensation with the feature of anonymity.

Transactions within blockchain maintain undeniable evidence, and any insertion of information in the chain is impossible due to the feature of immutability. This feature helps a system to be trusted. Blockchain provides security and ensures user privacy with a pair of keys. Confidentiality is maintained through the key pair's privacy, preventing third parties from revealing personal information. Blockchain helps to identify individuals' authenticity by verifying their identity. The accountability of a blockchain system allows it to perform better by investigating flaws in various areas. The feature of blockchain provides the advantage of information availability in the blockchain, depending on the blockchain type and its execution to verify the information. The system does not have scalability for the theoretical application; however, blockchain requires scalability to measure system performance.

Transparency adds value to the system by maintaining transaction records in the peer-to-peer network, enabling users to track those records. The consensus mechanism depends on the project requirement and application of how the system would approve a newly validated request; therefore, the consensus mechanism is not present in the article [28]. Data auditing is a crucial part of finding flaws and improving performance by addressing issues for national regulation. Non-repudiation in the system works as evidence against the sender's information and confirmation of the deliverance of that sent message. Robustness ensures the proper functioning of nodes inside the blockchain network. Without proper numeric results, it is challenging to evaluate and optimize the system's performance because the transaction latency does not provide a proper value to make the system difficult to assess the network's ability of real-time transaction performance. On the other hand, how many transactions are being handled simultaneously can not evaluate for the absent data of transaction throughput. The system hampers the transaction confirmation process along with network efficiency for having no value of block creation time. The security and effectiveness of the consensus protocol employed are harder to evaluate without information on consensus algorithm efficiency. Without data storage efficiency, it is complicated to optimize and estimate scalability.

In medical health applications [29], the system complexity has a sensitive role. Medical health applications have a numeral of branches. Technical difficulties in this sector are vital issues. Having the feature in the system helps reduce issues in specific branches. Smart-contract removes third parties from medical documents and provides data security for a person. Besides, access control and data security benefit users who want to share their medical history. The off-chain feature has the advantage of sharing data through a third party as a guarantee. Off-chain is absent in the system; however, having a Smart Contract feels like something other than an off-chain necessity. The user-centric system also has lightweight solutions that help the system not compromise data. Pseudonymity hides user identity for privacy and anonymity and exchanges data anonymously among parties in the network using a secure algorithm that is not needed in the system. Immutability in the system keeps data unalterable without a top portion's action in the network. Blockchain keeps data transparent, and the user has authenticity over the network. Non-Repudiation keeps transaction undeniable evidence between users about the transactions and behavior. The robustness facility handles exceptions and the functioning of nodes. The lack of transaction latency data hinders optimizing real-time performance and responsiveness, potentially impacting transaction continuity. Additionally, the absence of transaction throughput figures makes it challenging to assess the system's capacity to handle high transaction volumes, leading to potential bottlenecks and performance issues. The unknown mining time for consecutive blocks complicates evaluating the efficiency of the consensus mechanism and transaction confirmation time. Moreover, the system's storage capacity is not mentioned, making it difficult to assess scalability constraints, cost-effectiveness, and storage allocation efficiency. This lack of information raises concerns about potential inefficiencies and overutilization of storage resources.

In recent years, users' data has been flooding from various sources. KYC is the primary process to identify these flooding data. Regarding Big Data Analysis, the KYC verification system is costly and risky without blockchain technology [30]. Besides, integrating blockchain into a system is a complicated process because of erasing users' previous data from the system and inserting verified data against users' locations. Data sharing and access control are significant issues for the system considering the system's structure and purposes of use. The Smart Contract design can eliminate the third parties for identity verification against users' information by defining a set of rules, which feature is not considered for the discussion. The off-chain feature can collect data manually and helps in the processing phase.

Generalizing multiple types of identification methods into one can provide the system to verify users faster with the help of an off-chain feature. A nation of developing countries with a large number of people might have multiple verification methods such as birth certificates, driving licenses, passports, and national identity cards.

The lightweight solution can help the system in an environment of no-compromising data share, which is not explained in the system. It is hard for a big populated country to bring all nations together under the same system. Only a user-centric design can encourage nations to do so. This feature's benefit should consider in the context of Big Data Analysis. The authors did not cover the study of pseudonymity, anonymity, and authenticity in KYC using big data analytics. Pseudonymity should consider from the end of the authors to verify users' identity without revealing complete information. Standardization of addresses of users can be excellent cooperation for the verification process and national database. Anonymity can give the government more flexibility and control over its national identity without revealing any information. KYC without blockchain cannot make the system immutable for not keeping transaction records. Additionally, having no nonce in the authors' discussion does not give KYC immutability. KYC itself can give privacy by ensuring consumers' privacy laws. The measurement of Big Data Analysis and its relevance; authenticity can be identified. The study on KYC from the perspective of Big Data Analysis gives the system accountability for performing better by comparing, correlating, and comparing provided present and permanent addresses on different sets of identity verification cards. KYC does not guarantee confidentiality because consumers do not know how and where their data will be used. Public information on social media makes them available. In this case, taking unavailable information from consumers can solve the current problem.

Scalability provides an onboarding solution for KYC by giving authentic verification, notifying threads, and helping in thread reduction. Transparency is highly maintained in KYC by giving security to personal data. The KYC process does not need a consensus mechanism for varying user information appropriately. Data auditing is a significant part of KYC. A regular audit helps identify internal issues and gives ideas on how to solve them [30]. Non-Repudation gives the advantage of non-deniable evidence transactions of consumers with digital signatures. The robustness of KYC ensures verification accuracy and identifies the profiles' risks. The concept of KYC in the context of Big Data Analysis study helps authentication, verification, and reducing threads in business. The article [30] lacks numerical values for transaction latency, transaction throughput, block creation time, consensus algorithm efficiency, and data storage efficiency. This absence hinders assessing the real-time transaction processing speed, scalability, and overall performance of the system. Additionally, it limits our understanding of transaction confirmation time and record storage efficiency within the blockchain. The absence of data storage efficiency values makes it difficult to optimize the system's storage capacity, leading to potential inefficiencies and increased costs.

Casper, proposed in [31], aims to enhance the speed and security of client credential verification procedures. It leverages blockchain technology to create a decentralized and secure platform for securely storing and verifying consumer credentials. The verification process is automated through smart contracts, ensuring data integrity and reducing the risk of unauthorized access or tampering. With a reputation-based consensus approach, Casper incentivizes participants to validate consumer credentials accurately, enhancing overall efficiency. The Casper system encourages network users to contribute processing power, enhancing effectiveness and overall security by detecting and excluding malicious nodes. Transaction throughput remains relatively consistent, ensuring predictability, reliability, and a positive user experience. Query transaction throughput exceeds invoke transactions, making Casper suitable for various use cases, including finance, supply chain, and IoT sectors. The system's quick search processes reduce computing overhead, making it a valuable choice for blockchain implementation. However, block generation time increases with additional peers.

Numeric data on transaction latency, throughput, block creation time, consensus algorithm efficiency, and data storage improves clarity, evidence-based decision-making, and system performance optimization. The Casper platform's transaction throughput is measured, allowing for a precise and quantitative assessment of its performance and scalability. The evaluation shows that each platform peer achieved a significant throughput, indicating the system's capacity to handle concurrent operations. Numeric results help identify bottlenecks and improvement areas, such as transaction scalability evaluation showing linear query transaction growth after specific nodes but saturation due to ledger write operations. Numeric values enable comparison, benchmarking, performance target setting, and data-driven decision-making to optimize systems' efficiency and effectiveness.

The article [32]explores different performance and functionality metrics for blockchains, specifically in the context of a decentralized energy datahub. It addresses the complexities of creating and executing such a datahub, focusing on secure data-sharing techniques, data-sharing policies, permissions, and encryption protocols to ensure privacy and data protection. Additionally, the role of smart contracts within the energy datahub ecosystem is examined, highlighting their ability to automate rules and enable safe communication among stakeholders. The article discusses approaches to enhance scalability and performance, including exploring off-chain data storage or computing techniques while maintaining system integrity and security. The concept of a ''lightweight solution'' is likely used to refer to resource optimization strategies. The paper adopts a

user-centric perspective, emphasizing intuitive interfaces and user empowerment to promote stakeholder involvement. It may explore methods for preserving participant identities and traceability while ensuring data immutability on the blockchain. Availability, authentication, accountability, and confidentiality safeguards are considered to ensure continuous access to the system and protect sensitive information. Scalability strategies such as sharding, sidechains, or off-chain scaling are likely discussed to accommodate an expanding participant base and increasing data quantities within the energy datahub ecosystem.

The proposed system utilizes blockchain to enable transparency in the energy sector, making transactions public and auditable. However, consensus mechanisms like PoW, PoS, or Practical Byzantine Fault Tolerance could be explored. Techniques for data audits to ensure integrity, spot irregularities, and guarantee accurate data on the blockchain may be covered, along with non-repudiation mechanisms like digital signatures. The paper may also address countermeasures for system failures and attacks, ensuring the energy datahub's robustness and resilience. To optimize the DenHub model, concrete values for transaction latency, throughput, block creation time, consensus algorithm efficiency, and data storage efficiency are crucial. Numeric metrics enable accurate performance measurement, informed decision-making, and scalability enhancements for the system.

The proposed system in [33] has a medium-to-high complexity, integrating blockchain technology and cryptographic techniques. It enables verified financial institutions to securely access and share customer KYC data, reducing duplication and enhancing compliance outcomes. Smart contracts automate certain KYC process steps, reducing manual intervention and potential errors. On-chain immutability ensures data authenticity and enhances trust. Privacy measures safeguard customer identities, and authenticity verifies data by authorized financial institutions, fostering confidence. Transparency allows all stakeholders to access and verify KYC data, promoting trust and accountability. Consensus mechanisms ensure agreement on data validity, eliminating the need for central authorities. However, the absence of an off-chain solution in e-KYC can limit data management flexibility for sensitive client information, compromising privacy and data protection requirements. A lightweight solution is necessary for reduced computational requirements and faster processing times. A user-centric design facilitates the safe exchange of personal data, but complete anonymity may hinder regulatory compliance and increase fraud risks. Explicit accountability measures are needed to address concerns about the validity and reliability of KYC data on the blockchain.

Inadequate confidentiality safeguards may risk third-party access to private customer information, compromising the credibility of the e-KYC system and endangering user privacy. Availability and scalability are essential to efficiently handle high volumes of KYC verification requests, avoiding processing delays and customer frustration. Data auditing and non-repudiation mechanisms are necessary for data authenticity verification and regulatory compliance. Robustness is crucial to withstand potential attacks and ensure data security. However, the article lacks information on transaction latency, throughput, block formation time, consensus method performance, or data storage performance. This may result in longer wait times and slower response times for customers and banks during KYC transaction processing. Insufficient transaction throughput can hinder system scalability due to network congestion. The article focuses on setting up and engaging with the blockchain for KYC applications rather than discussing the efficiency of the local blockchain network's consensus technique. To ensure smooth operations and address performance concerns, practical consensus algorithms and data storage systems are vital for a blockchain-based KYC system.

The blockchain system in [34] may have drawbacks or restrictions if a user-centric, lightweight solution is absent. Weaknesses can arise from system complexity, data sharing and access control issues, lack of lightweight solutions, poor user experiences, pseudonymity and anonymity concerns, immutability challenges, accountability, confidentiality, availability, data auditing, and non-repudiation. Without appropriate data sharing and access control, sensitive client data may be exposed to unauthorized parties, impacting system effectiveness and security. Additionally, inadequate confidentiality safeguards can jeopardize the system's integrity. Insufficient availability measures can affect the system's reliability, leading to downtime or service interruptions. Non-repudiation methods may complicate establishing transaction authenticity and hinder dispute resolution. Data auditing is essential for maintaining data integrity on the blockchain.

The system gains advantages from the presence of smart contracts, off-chain processes, privacy measures, authenticity verification, scalability, transparency, consensus mechanisms, and robustness. Smart contracts enable fair and transparent bidding procedures without intermediaries. Off-chain processes, including encryption and computations, lighten the blockchain network's processing load, increasing scalability. Fully homomorphic encryption (FHE) ensures privacy in processing sensitive data securely without exposing the plaintext, enhancing authenticity verification. By reducing computing burden and maximizing resource efficiency, off-chain processing and smart contracts contribute to increased scalability. Transparency is achieved through blockchain technology, recording all transactions and data on an unchangeable public ledger. Consensus algorithms ensure network participants' agreement, enhancing security and dependability. Decentralization through blockchain technology and cryptographic methods improves data integrity and resistance to attacks. Faster transaction confirmation and improved user experience are enabled by reduced transaction latency, facilitating quicker KYC authentication and Vickrey auction completion. Faster block creation leads to quicker verification and transaction processing, boosting system responsiveness and overall performance. However,

low transaction throughput can result in slow processing, delay time, and network congestion, affecting user experience and efficiency. Ineffective consensus algorithms may lead to longer confirmation times, increased resource usage, and decreased system performance. Data storage efficiency is essential for controlling and storing data on the blockchain to avoid unnecessary bloat and increase storage costs and retrieval times. Addressing these challenges is crucial to enhance the system's overall efficiency and effectiveness.

The secure data exchange and the address-search method feature raise the system complexity at least medium to high. [35] CODE enforces FATF compliance criteria that require VASPs. VASPs share personal information limiting unnecessary information exposure during virtual asset transfers. The secure P2P communication of Corda ensures that. Corda network securely maintains transaction-related data. CODE's organized design, smart contract, and data maintenance enforce only travel rules. Data exchanged between VASPs is assumed to be accurate and unaltered. The smart contract ensures rules and data sharing between VASPs to confirm the availability of necessary data before executing a transaction. VASP with blockchain technology, ensures immutability and makes CODE a scalable and strong travel solution. CODE's smart contract automates travel rule compliance, data sharing policies between VASPs, and expediting operations. Non-repudiation makes travel data permanent and tamperproof, holding VASPs accountable. The lightweight data storage and communication architecture helps CODE being effective and benefits network size. Data redundancy improves availability and fault tolerance, while consensus algorithms maintain data integrity and dependability by avoiding duplicate spending and contradictory information. These attributes make CODE more dependable. Although CODE guarantees data integrity but may have an impact on scalability. The absence of off-chain may hamper higher processing and storage needs. Although CODE guarantees data integrity but may have an impact on scalability. The absence of off-chain may hamper higher processing and storage needs; compliance concerns may occur for the absence of user-centric design. FATF requires identity verification ahead of pseudonymity and anonymity; data could reveal users' identities. There's a need to balance identity verification and user privacy.

Transparency for outsiders has not maintained that impact visibility of travel rule data share while CODE prioritizes transparency among VASPs for compliance with travel regulations. That may raise system integrity. For the appropriate sharing of travel rule data and regulatory compliance, data auditing is essential. Without strong capabilities, the CODE system may have trouble confirming correctness and completeness, which might result in information exchange faults or disparities. Even while Corda's blockchain technology provides some resilience, it isn't further strengthened, which might make it more vulnerable to security breaches or other interruptions and jeopardize the integrity of travel rule data. CODE performance has not been evaluated yet. It is complex to analyze its performance. The absence of performance results does not give a proper sense of scalability and further enhances CODEs capabilities and overall user experience.

B. EXISTING WORKS WITHOUT KYC

The verification of documents is a sensitive issue for ensuring authentication. Countries need help with verifying original certificates [36]. The system complexity of document verification is highly observed for ensuring the identity of users. Companies find suitable employees by analyzing the skill set of the applicant's CV. The process is lengthy and time-consuming. In this situation, Blockchain-based controlled access users are a solution. Data sharing and access control features give necessary data access to specific companies and concerns. The existing prototype implements micro-credentials in Blockchain that offer the smart contract facility to remove middle media. The absence of an off-chain facility does not allow external verification over the internet. Besides, the lightweight solution's absence does not cover complete security and protection of users' information. Certificates are the identity of users' skills which is the advantage of sharing information in a network. User-centric advantage gives the user the facility of real-time experience of inserting information. The feature controls the user on what information the user wants to share or not. The absence of Pseudonymity does indicate any issue in the system due to the agenda of the system. Anonymity offers the advantage of certificate verification of users without revealing validator information. Immutability ensures users' certificates validity authentication by the 51 percent stake of the network. Using the hyper ledger framework of Blockchain gives accountability in the system by identifying the duplicate information availability in the network. The system gives the public key of certificates to all users in the network, and the cryptographic private key ensures security in the system. The system provides scalability with the features of a hyper ledger framework by supporting increasing information blocks in the network. The feature notifies immediately every time of any changes with a customized access level.

The article highlights the advantages and characteristics of the Hyperledger Fabric blockchain framework for academic certificate verification without providing specific numeric values for Transaction Latency, Transaction Throughput, Block Creation Time, Consensus Algorithm Efficiency, or Data Storage Efficiency [36]. The absence of these concrete values hinders the evaluation and optimization of the proposed framework, potentially leading to inefficiencies and difficulties in setting performance targets. Specific numeric data is crucial for measuring the system's behavior, performance accuracy, and effectiveness, identifying potential bottlenecks, and making data-driven decisions. Without concrete values, it becomes challenging to assess data storage effectiveness and scalability within the system, hindering informed decisions on optimal storage mechanisms.

The hiring process is hectic and critical for a company. As a result, CVs have a vital role in the job market. In most cases,

recruiters have to invest separately in the verification process. [37] has shown that the obstacle of verifying documents is time-consuming and a hassle. The paper's authors have proposed a consortium blockchain to ensure the system's complexity. The authors have also proposed using hyper ledger fabric for their use case diagram. The feature provides access control over their shared data. The system proposal for smart contracts architecture has the compatibility to reduce cost and decrease data loss attacks. Besides, a hyper-ledger fabric network will allow the system to verify the applications manually through the verifier organization. The lightweight solution ensures data sharing without sacrificing information security.

The architecture of the proposed method [37] provides a friendly and easily operatable interface for users. As a result, users get an organized interface to operate with low energy waste. On the other hand, verifiers' justified information will help recruiters find applicants' identities in terms of the requisition process. Anonymity does not need in the system because the verifier information is highly required for sterling verification. Using a blockchain mechanism in the system confirms the immutability of transactions. Immutability helps the system to maintain transparency of applicants' data transactions. A person's identity and academic information are confidential. Blockchain technology maintains the high security of these credentials. The confirmation of privacy and security develops the authenticity of the system over the blockchain-based CV verification system. Having no accountability in the system can reduce participation. In this situation, productivity might decrease, and turnover can go higher. The assurance of transparency and immutability of the system helps maintain the confidentiality of users' given information in CVs. The system shares the applicant's information in the peer-to-peer network, which makes data available in the network. Authentic Recruiters can access and verify the given data from the network. The growing list of records against applicants' CVs can easily be supported by scalability. The consensus protocol helps the proposed system prevent unauthorized verification of CVs using its mechanism, except for verifier interaction. The main advantage of feature data auditing is the reliability of the system. It provides a non-parallel transaction record. As a result, the transactions' authenticity and validity can be verified. The non-Repudiation feature ensures a secure and quickly updatable data storage mode. For its advantage, the feature provides the system with authenticity, integrity, and evidence of the origin of data. The maintenance of the hyper ledger network and its proper functioning for the feature Robustness.

The proposed Hyperledger Fabric-based consortium blockchain for academic certificate verification [37] lacks quantitative data for 'Transaction Latency,' 'Transaction Throughput,' 'Block Creation Time,' 'Consensus Algorithm Efficiency,' and 'Data Storage Efficiency,' which presents significant drawbacks. The absence of transaction latency data hinders assessing real-time processing capabilities, while the lack of transaction throughput values raises uncertainty about the system's ability to handle verification efficiently. Additionally, the inaccessibility of block creation time data hampers analyzing block generation efficiency and its impact on transaction speed and scalability. The potency of the chosen consensus algorithm cannot be assured without numeric measurements of transaction validity. Moreover, the lack of numerical values for data storage efficiency prevents identifying optimal storage strategies and potential challenges. This deficiency in performance metrics limits informative discussions, optimization, and scalability of the academic certificate verification process.

Technological development is increasing day by day. Currently, many projects are being executed to reduce global warming. Everything is getting digitized simultaneously to cope with the industrial revolution. Recent work shows that digital invoice reduces exchange costs by up to €6.7 in terms of exchange. Concerning global and economic developments [38] proposed digital invoice and VAT payment management using blockchain technology. The proposed system has a high system complexity for full infrastructure development. For the project's development, every sector must be developed from the root. In the proposed system, data sharing and access control feature gives the advantages to whom data access can be shared. The value-added tax and vat approval can maintain by the smart contract. Every person's initial data of VAT has to insert into the blockchain manually that ensure the off-chain feature. The lightweight feature helps the system maintain VAT information against the population without sacrificing their data. The system is also designed with a user-friendly interface that helps users use the system in a cooperative environment. Pseudonymity helps the proposed system provide a verifier and the users' transaction information partially visible to the network. As a result, the user can see who is verifying their VAT-related information.

The system's anonymity feature absence cannot ensure online attacks from unknown, harassment, and false information in the blockchain network because of the low privacy of transaction information [38]. The transactions in the network are unchangeable except for external attacks that ensure the immutability feature. VAT information against every ID is highly confidential. The privacy feature maintains that and allows the system to be highly secure. Transparency against every transaction can help build reliability among users. Authentication of the system is established by maintaining Ethereum-based smart contracts. Having no accountability in the system might decrease the system's performance. The system should have accountability to maintain system performance, and verifiers should be more involved. The scalability feature increases transparency and maintains non-parallel transactions in the network. The availability of information in the blockchain network assures users accessibility of their VAT information easily. The consensus mechanism helps the system verify and includes updated information in the chain that does not apply to the proposed system. The system will update automatically at that time

when users make payments. The data auditing feature helps the system helps to grow assurance among users. The non-Repudiation feature gives the system the main advantage of authenticity, integrity, and root of data. Besides, the feature also rejects the non-verified data from the insertion. The robustness of the system provides healthy and proper functioning to execute properly.

The absence of concrete values for transaction latency, transaction throughput, block creation time, consensus algorithm efficiency, and data storage introduces several disadvantages. These metrics are crucial for evaluating a blockchain system's performance and scalability. Accurate values enable effective measurement of the system's efficiency and effectiveness. Transaction latency measures the time for a transaction to be confirmed and added to the blockchain, impacting overall speed and effectiveness. Transaction throughput indicates the system's processing capability with the number of transactions processed per unit of time. Block creation time affects the blockchain's speed and fairness. Data storage efficiency influences resource utilization and cost. Having specific values for these metrics allows for better performance optimization, identifying bottlenecks, and making informed decisions for scalability and resource allocation, thus preventing inefficiencies and suboptimal resource utilization.

Educational documents are confidential and sensitive to a person. In recent days, researchers have been working on securing education documents [2]. The securing process of an educational document is costly and time-consuming. Besides that, the system has to be implemented from the root, which indicates the high system complexity. Education documents should be available in the proposed system's private blockchain. The shared education document must ensure the availability feature and makes it accessible to all in the system network. The private blockchain-based secure system eliminates third parties from verifying the authenticity of educational documents. Ethereum is used for building Smart Contact design. The system does not have the off-chain feature. However, specific admins confirm the first injection of verified data in the blockchain, which provides the authenticity feature of the system. The lightweight solution feature provides security for users' educational data without sacrificing data. The system's user-centric design makes the system more compatible and user-friendly. Users can verify the authenticity quickly and cheaply through the network. Pseudonymity does not belong to the system. However, the feature provides indirect information about verifiers that do not need in the system.

The availability of immutability gives the system the advantage of notification of sudden changes in the chain. The feature helps to track down the changing root. Privacy of each individual's data is highly maintained, which gives the system an extra advantage. Having the accountability feature boosts the performance of participation of the validator. As a result, participation helps the verification process be more updated and less time-consuming. Scalability supports the system by giving transparency about non-parallel transactions of documents. The PoA consensus mechanism is used in the system to identify the known validator of the educational documents more efficiently. Data auditing gives the proposed system the advantage of relying upon the users against the security of users' educational documents. Robustness ensures healthiness against attacks and proper functioning of the system's execution. Non-Repudiation gives the proposed system the advantages of origin of the distribution location of educational documents and their authenticity. Non-Repudiation also ensures the integrity of the educational documents.

Evaluating the performance of a multimode private Ethereum blockchain setup and a private IPFS network offers valuable insights into various system aspects [2]. In the Ethereum blockchain, transaction latency is influenced by the difficulty level, leading to longer processing times that enhance security and prevent fraud. The efficiency of the blockchain system is impacted by the network size and load, resulting in higher transaction latency due to increased node propagation time in larger networks. Private IPFS networks experience longer retrieval times due to file fragmentation and distribution, affecting upload and retrieval latencies. Transaction throughput is a critical metric for assessing a blockchain system's efficiency and scalability, measuring the number of transactions processed within a given time frame. Higher throughput indicates greater transaction volume, providing benefits like scalability, faster confirmation times, improved user experience, and lower transaction costs. High transaction throughput demonstrates robustness and resilience in handling surges in transaction volumes and contributes to the widespread adoption of blockchain technology.

However, the test results depict that the performance impact of various factors on transaction latency, transaction throughput, and consensus algorithm efficiency. PoA outperforms PoW in terms of transaction latency, as it requires less computational power and time. The text provides numerical values for transaction latency but lacks quantitative data for block creation time and data storage efficiency in the IPFS network. The use of IPFS for distributed peer-to-peer file storage is highlighted, with potential higher retrieval latency than upload latency due to network fragmentation and distribution. Numeric results help stakeholders compare system configurations, assess transaction latency and throughput, and identify suitable configurations for specific use cases. It aids in resource allocation decisions and enables targeted optimizations. Numeric data is crucial for validating hypotheses, conducting in-depth analysis, and making informed decisions on upgrades and new technology adoption. Additionally, numeric results enhance reproducibility and transparency in the study.

The power Grid is currently an area of concern [39]. System complexity ensures secure systematic ways by establishing compatible relations among elements at Pacific Northwest National Lab (PNNL). The smart-contract facility offers faster speed, scale, and security among energy resources in

the system. The application of limited data sharing access and control helps the system from third-party threads and information leakage. Besides, the execution process without compromising user information gives the Blockchain-based system extra benefit with multiple-layer security in the power grid. User-centric features help building-up a mindset of users and vendors to participate in cryptographic signing. The outcome shows a positive impact on trusting a system.

The absence of anonymity and pseudonymity do not hamper the system due to the behoof of complete grid exchange information. It does not require an external facility for power grid transactions at Pacific Northwest National Lab (PNNL), which makes off-chain unnecessary for the system. Blockchain technology integration ensures the security of electricity infrastructure. The integration increases the reliability of authentication and encryption. Immutability property stores all electric energy distribution and buildings-to-grid connections information with the timestamp. The authentic validator, PNNL's buildings-to-grid cybersecurity test-bed, requires fifty-one percent to alter transactions. However, the removed data transaction also stores in the system. The application of Blockchain in the power grid maintains transparency that makes the system trustworthy, and the availability of a consensus mechanism helps the system verify the authentic provider of the power grid system. Confidentiality provides the transaction between providers are users of the power grid. Smart-contract feature use in the power grid omits the necessity of a third party to be a guarantee. The allowance of data auditing in Grid Modernization supports multiple transactions based on predefined rules. Non- Repudiation collects, maintains, provides, and verifies the undeniable evidence between distributed energy providers and customers. Additionally, robustness handles exceptions and functioning of nodes of Grid Modernization path and Cyber Resiliency.

The absence of numerical values for transaction latency, transaction throughput, block creation time, consensus algorithm efficiency, and data storage efficiency in the proposed system leads to various disadvantages. Without these values, it becomes challenging to accurately measure the system's performance and scalability. The uncertainty in transaction latency affects real-time data operations and verification times, hindering responsiveness. Specific information about transaction throughput is crucial for understanding the system's capacity to handle a high volume of transactions concurrently, ensuring scalability and efficiency. The lack of block creation time data makes it difficult to assess the average time to create a new block in the blockchain, impacting overall transaction speed and system responsiveness. Evaluating the efficiency of the consensus algorithm becomes challenging without relevant metrics, which affects the system's resilience against attacks and its ability to maintain consensus. Furthermore, the absence of data storage efficiency results hampers understanding of the effects of optimization and resource utilization in the blockchain network.

The Blockchain-Based Hyperledger Fabric Network system complexity for KYC Optimization [16] has multiple sectors. Financial institutions must maintain the system complexity for transactional procedures for various purposes. Financial institutions focus on technical difficulties and challenges by identifying system complexity. Financial institutions use Smart Contracts for securely executing transactions without relying on third parties. Besides, data sharing and access control advantages with limited data shares and user control. As a result, users partially access data with the concern. Sometimes off-chain helps transactions execute externally securely in terms of money laundering. Financial statements are highly confidential. In this case, a lightweight solution provides a transaction facility without compromising privacy. Although all information is not user-centric in the financial category, they have limited accessibility to see a demo of the execution process from the user end. Anonymity offers transactions in the network hiding user information, and Pseudonymity offers a state to maintain users' information private in the whole network. Regarding KYC optimization, Immutability helps keep data unalterable so that financial statements have authenticity over the network. Besides, significant changes in financial statements require a 51 percent stake in the whole network. The system provides privacy over the system with safer and faster bank transactions. Financial insertion in a node requires authenticity and has to be proven through the validators. Having the facility of accountability, customers of a bank have the right of accountability to the bank. Confidentiality of user data is required. In this case, a bank must maintain confidentiality to achieve a few services, such as vehicle insurance. Blockchain-based KYC optimization makes data available to the network, but the person with access to visible data can only see the data. Blockchain strictly maintains this. The Scalability of financial institutions must require real-time updates over the network and support the system with increased nodes that contain information in the network. The unavailability of Conscious may occur unreliability of the system. Its absence makes the system questionable. Its availability ensures the conscious mechanism in the network and helps achieve trust. The presence of non-repudiation collects, maintains, provides, and verifies the undeniable evidence about financial transactions and behavior between users. On the other hand, robustness handles exceptional transactions and unwanted occurrences in the network. The advantage of having transaction latency within the Hyperledger Fabric is that it provides a relatively quick registration process with low latency for data access. However, the system does not provide specific information about block creation time, consensus algorithm efficiency, and data storage efficiency. The duration for generating a block is still being determined, and it is unclear if the system measures the time between mining consecutive blocks. The evaluation should include an assessment of the consensus algorithm's efficiency in reaching consensus quickly and securely. While Docker, Composer, and Oracle VirtualBox are mentioned,

there needs to be a specific mention of evaluating data storage efficiency. The system should analyze the efficiency of data storage on the blockchain network to provide a comprehensive evaluation of its performance.

Blockchain-based mobile charger billing system [40] has the system complexity of whom to share data and whom to not. System complexity gives the best requirements analysis for executing the system and which angle might give the best result. The system is facilitated with data sharing and access control over the system. The system is user decentralized, with access to a group of people that ensure security. Additionally, the system removes the third party, reducing the unnecessary verification cost between users and the billing procedure. Off-chain facilities offer external transaction facilities to a group of people without compromising any privacy that is absent in the system. As a result, the system information is available and public to the network. In the billing system, where the vehicle is charged is hardly identifiable. The presence of the feature is challenging and has technical difficulties. Pseudonymity is vital in this situation. Anonymity offers the billing transactions anonymous. Additionally, immutability requires data unalterable. Blockchain technology is more secure and safe. The system gives the advantages of it. The billing transaction is transparent, which makes the system trustworthy. Authenticity gives trustworthiness and reliability to the billing system.

Absent accountability removes the questionable medium that has control over the user's private key. The system does not maintain confidentiality due to not necessity of a third party. The integration of Blockchain technology provides availability and scalability in the system. Availability ensures data after verification in the network. Scalability supports the increasing number of nodes with transactional data in the network. The non-existence of consciousness occurs the lackings of trust in the system. The situation might create complications in the system, believing the currency belongs to the system. In some cases, data auditing can have a manual process by the validator to ensure the system information is valid; or invalid. The absence of it does not support the high-value transactions in the system. The presence of non-repudiation and robustness investigates the evidence of transaction data and behavior between users and handles exceptions among numerous recharge transactions.

The proposed solution [40] focuses on the proposed system architecture and functionalities related to mobile chargers, billing, and lightweight blockchain data management. However, more specific quantitative data is needed on key performance metrics for mobile charges in the proposed lightweight blockchain system. Transaction latency, transaction throughput, block creation time, consensus algorithm efficiency, and data storage efficiency are crucial for measuring the system's efficiency and effectiveness. The absence of these quantitative data points may hamper the ability to assess the system's responsiveness, scalability, and efficiency. It becomes challenging to identify potential bottlenecks, optimize transaction processing times, and manage storage costs effectively. Furthermore, the lack of this data creates difficulty in evaluating the algorithm's security and effectiveness and making informed decisions concerning the system's feasibility and practicality.

The current educational certificates have built-in security features to identify originality. Besides that, several attachments are there, along with educational certificates, depending on requirements. The certificate verification system follows a hierarchy. In this sector, the accredited certification authority belongs at the top, whose sign refers to the authenticity of a certificate holder. On the other hand, it requires considerable effort to ensure the security of Digital Certificates and certificate registration because a standard digital signature must be used in verification [41]. As a result, the complexity of the system is high. The system offers individual features to share certificates to verify. It also offers data-sharing features to specific audiences and controls access over the system. The advantage of two different types of smart contract design gives the system an immediate outcome of verification. Moreover, this system allows a third-party 'Certification Authority' to verify certificates through its smart contract design. The system allows learners' certificate verification applications from their end to reduce the manual insertion of previous certificates that have already been issued. This process does not require off-chain verification. The simplified blockchain algorithm' Lightweight Solution' ensures reliability on the system without sacrificing data security, such as certifiers' identity information and certificate holders' additional information.

The simplified algorithm also maintains verified information. The user-centric design provides a web interface where learners can easily understand what and how to apply for verification. The advantage of pseudonymity is that it allows communication between learners which is not required in the blockchain-based education certificate verification system because of no necessity of having the feature. Learners must have the right to know the accredited certification authority that is verifying their certificates. The anonymity feature gives the advantage of reducing the system's accountability by keeping the privacy of employers to learners working behind the scenes. Any transaction record in a blockchain-based system is unchangeable, which gives the system the advantage of reliability. Privacy preservation is the primary concern of blockchain and digital certificates as well. The system with blockchain ensures the privacy of certificates; however, it costs a massive amount of work. Authenticity allows learners to store their educational certificates in the peer-to-peer network. Besides that, the expiry period of the certificates can quickly identify the authenticity of the verified certificates.

Accountability is a vital part of the system where learning certificates and their performance are evaluated throughout the process. The analytical result is used to help perform better, giving security and authenticity [41].

Confidentiality gives the advantage of sharing learners' information within the institution and organization in the chain unless sharing the certificate. In terms of verification from the blockchain network, the availability of learners' information gives the advantage of the identification process faster and low cost. There is a high risk of maintaining regulation and securing processes for the current context. Besides that, efforts in registry securing are questionable. In the present context, the system's scalability is needed to inspect the global verification process. Redundancy of certificate allocation and distribution channels along with accreditation authority signature gives the system the advantage of transparency. However, certificate expiration periods and storing cryptographically signed certificate processes are not on the spot. The system does not mention the consensus mechanism for securing a network from external attacks for validating certificates; however, the validation process should be considered. Performance of the system boosts for continuous monitoring of certificates validatory period. Keeping track of certificate verification transactions gives the advantage of non-deniable evidence from learners' applications to the compilation of verified certificates from accreditation authorities. The robustness of the system needs to be executed correctly in the system. The process of verification is complicated and can have external threats. Besides that, forged authentication of certificates for the maximum number of nodes can hamper the system from proper functioning. The article discusses the Blockchain for Education platform but lacks specific performance metrics. Transaction latency, throughput, block creation time, consensus algorithm efficiency, and data storage efficiency data are essential for system evaluation and scalability planning. The absence of these metrics hampers performance assessment, optimization, and real-world implementation readiness. Including key metrics enhances transparency and reliability.

Recently, multimedia has been unauthorized audio and music files, images, and video/movies and releases issues before productions release [42]. As a result, multimedia has vital system complexity to protect against unauthorized release and ensure authenticity. Multimedia has to rely on third-party for promotion and publicity; however, third-party involve hampers and steal data. The Smart Contract application reduces third-party engagement and keeps data secure. On the other hand, the absence of third parties helps to get benefit distributors, producers, and artists. The reliance on third parties is a part of publicity and promotion. As a result, the user has to focus on data sharing and access control. The limited and authorized data sharing and access control facilities with the authentic user and third party. Confidentiality is a sensitive part of multimedia. Confidentiality in the system includes private information of distributors, producers, and artists. Maintaining confidentiality helps the accountability of the system.

Blockchain application in multimedia makes it transparent over copywriting. The system provides authenticity-verifying distributors, producers, and artists through the network. This way helps the system control user data keeping it user-centric. This facility ensures data privacy and control without compromising authenticity to third parties. The off-chain facility is not available in the system for no necessity of sharing information outside of the Blockchain. As the system has a lightweight solution, the system does not require any compromise with data; however, the system depends on third-party verification. Users in multimedia do not require any hides for their identity. Therefore pseudonymity is not necessary for the system. Anonymity represents any transaction without revealing user information. Anonymity is highly used in financial transactions that do not need to use in multimedia. Non-repudiation advantage ensures undeniable evidence of producers, artists, and distributors that validate the necessary content of multimedia, and Immutability ensures all records regarding productions and their release.

In terms of changing transactions or altering information, maximum stacks allowance in the system. Conscious is a part of a Blockchain-based framework. Consciousness adds value to distributors, producers, and artists' profiles as currency, not in the system. The robustness handles the exceptions of the system and the publicity information of nodes within the network. The scalability of the system ensures the increasing number of nodes of information that is not available. The absence of scalability in the system can not support the increasing number of nodes and transactions in the network. Data Auditing validates multimedia information. As multimedia is a proposed scope of Blockchain, data auditing is highly required for the system. Data auditing can also be verified manually.

The article [42] lacks specific numeric values for transaction latency, transaction throughput, block creation time, consensus algorithm efficiency, and data storage efficiency. Further analysis and measurement are needed to obtain these metrics, which could impact the system's functionality, security, and user experience. Transaction latency and transaction throughput are crucial metrics for evaluating the speed of multimedia data transactions on the blockchain. High latency can cause data access and retrieval delays, affecting multimedia applications' responsiveness. There needs to be more transaction throughput to avoid a backlog of pending transactions, leading to congestion and reduced user satisfaction. Block creation time, the interval between consecutive block additions, can also be challenging in estimating transaction finalization and security. Long block creation time can cause slower data storage and retrieval processes, impacting the system's real-time capabilities. The consensus algorithm is crucial for blockchain security and integrity, ensuring network participants agree on transaction validity and order. However, it is easier to assess the reliability and withstand potential attacks by measuring its efficiency. Inefficient data storage practices compromise multimedia privacy, user trust, and system performance, causing higher costs, slower access, and potential scalability issues. This

hinders the system's ability to handle large multimedia data volumes effectively.

The paper [43] introduces NovidChain, a blockchain-based platform designed to address privacy concerns and enhance the security and efficiency of COVID-19 test and vaccine certificates. The system utilizes cryptographic techniques, smart contracts, and a distributed ledger to prioritize privacy preservation and enable selective sharing of health data. NovidChain adopts a user-centric approach, empowering individuals to control their data while ensuring privacy. Smart contracts automate certificate verification and management operations. The platform ensures immutability, authenticity, and accountability through blockchain technology, preventing unauthorized modifications to health records and enabling traceable transactions. While scalability is acknowledged as a challenge, potential solutions like off-chain data storage are considered. Transparency is achieved through the distributed ledger, allowing participants to validate transaction integrity. The paper does not explicitly define consensus but mentions data auditing and non-repudiation facilitated by the blockchain's transparent and immutable nature.

The evaluation assesses the NovidChain platform in comparison to academic works like SecureABC, CATCApp, and the commercial solution ImmuPass. It focuses on key security properties, financial cost, and scalability using performance metrics. The findings reveal that NovidChain, CATCApp, and ImmuPass satisfy crucial security properties like forge resistance, tamper-proof certificates, binding between the certificate and the holder, uniqueness of certificates per user, peer-indistinguishability protecting user information, and revocation mechanisms. However, SecureABC is considered less secure in this context. NovidChain stands out with its improved transaction latency for issuing and verifying COVID-19 credentials. It demonstrates an impressive average transaction latency and efficient block generation capacity, making it well-equipped to handle a substantial number of users per block. The platform's average block production time is noteworthy, highlighting its efficiency in processing transactions. Additionally, by leveraging exclusively IPFS hashes, NovidChain achieves enhanced data storage efficiency, leading to significant cost savings compared to direct data storage on the Ethereum Blockchain.

The transaction latency of NavidChain ensures a quick response at the time of accessing and verifying COVID-19 credentials, which confirms data retrieval and verification almost instantly with the user experience and reduces delays in critical situations. The high throughput capacity allows NovidChain to handle a large number of transactions concurrently, accommodating a substantial number of users and healthcare providers. The higher the transaction throughput, the more efficient the system is at processing multiple operations simultaneously. NovidChain's high throughput capacity enables the concurrent handling of large transactions, accommodating numerous users and healthcare providers, resulting in increased efficiency in processing multiple operations. Blockchain's frequent updates and regular data addition enable quick block creation, resulting in an efficient system with faster formation times, enabling faster transaction inclusion and validation. NovidChain greatly lowers the cost of data storage by using IPFS storage to store COVID-19 credentials off-chain and hashes on-chain. The system becomes more effective and cost-effective because of this method's reduction in the size of on-chain data. NovidChain ensures quick transaction latency, facilitating instant data retrieval and verification for COVID-19 credentials. Its high throughput capacity enables efficient concurrent handling of multiple transactions, accommodating numerous users and healthcare providers. The system's fast block creation allows for quicker transaction inclusion and validation. Utilizing IPFS storage reduces data storage costs, making NovidChain more effective and cost-efficient by minimizing on-chain data size.

The research in [44] proposes a PoTx-based traceability system for the agricultural supply chain using blockchain technology. It aims to address data exchange, access management, and supply chain accountability issues. The article should provide detailed insights into the challenges associated with implementing the PoTx traceability system, including infrastructure setup, network configuration, and blockchain integration. It should describe the mechanisms for controlled data sharing, privacy protection, and access control within the system, including authentication, permissions, and protocol techniques. The incorporation of smart contracts is a crucial part of the traceability system, and the paper should elaborate on their functionalities and logic, showing how they enforce rules, automate verification, and enable self-executing agreements. Any off-chain elements or procedures used in the traceability system should also be explained, highlighting their role in improving performance and scalability. The user-centric nature of the traceability system must be emphasized, considering the requirements and perspectives of different stakeholders. User-friendly interfaces, simple interactions, and accessibility features should be included to enhance usability and adoption.

Focusing on user-centric design highlights the system's potential for widespread participation and acceptance. The paper should elaborate on privacy-preserving measures, such as pseudonymity and anonymization, to enable traceability and accountability while safeguarding private information within the supply chain. To ensure a secure and reliable environment, the system must guarantee data immutability, privacy, authenticity, and confidentiality. Mechanisms for accountability, availability, and robustness, including auditability, fault tolerance, redundancy, and disaster recovery, need to be thoroughly discussed to demonstrate the system's resilience and ability to withstand potential attacks or failures. Scalability is a critical aspect that should be extensively covered in the article, considering growing network sizes and transaction volumes. The chosen consensus method's impact on scalability and transparency should be

examined to ensure efficient data audits within the supply chain.

The system's capacity to achieve non-repudiation, preventing denial of involvement in transactions or data manipulation, should be highlighted using cryptographic proofs like digital signatures. The study should emphasize how each criterion is applied and handled in the proposed PoTx-based traceability system for the agricultural supply chain. By addressing system complexity, data sharing, smart contracts, off-chain solutions, user-centric design, privacy, authenticity, scalability, transparency, consensus, data auditing, non-repudiation, accountability, and robustness, the paper lays a solid foundation for understanding the technical and operational efficacy of the proposed traceability system.

The article discusses implementing an agriculture product traceability system using blockchain technology, emphasizing the advantages of the Proof of Transaction (PoTx) consensus algorithm over traditional ones like PoW and PBFT. However, it lacks specific data on important performance metrics, such as transaction latency, throughput, and block creation time. The absence of these metrics makes it challenging to assess the system's processing speed, leading to uncertainty about real-time product movements and data accuracy. Delayed transactions can compromise traceability and supply chain response, potentially causing product recalls or quality control issues. Additionally, the system's handling of high transaction volumes is unknown without transaction throughput metrics. Sufficient throughput is crucial to avoid backlogs and delays in tracking product movements during peak periods. Block creation time is essential for maintaining an up-to-date and tamper-resistant ledger. Unpredictable block creation times can affect data integrity and efficiency, leading to discrepancies in product traceability records. Monitoring and optimizing these metrics are crucial for ensuring efficiency, reliability, and seamless supply chain management in agriculture product traceability systems.

The article [45] presents a framework for blockchain-based multi-level marketing (MLM) networks that prioritize privacy and security. Through the use of encryption, pseudonymity, and selective disclosure, the framework protects participant information, transaction data, and confidential company details. Blockchain's transparency and decentralization are leveraged to maintain openness and accountability while safeguarding sensitive data. Smart contracts automate and enforce MLM regulations, ensuring participant confidence and fairness. Scalability concerns are addressed through methods like sharding and off-chain solutions. The article provides a comprehensive approach to enhancing privacy in blockchain-based MLM platforms. To further enhance understanding, the study should detail the specific functions and logic built into smart contracts, demonstrating their role in regulating the MLM system. Additionally, the integration of off-chain components and their contributions to performance, scalability, and privacy optimization should be explained. The article highlights the lightweight nature of the framework and any resource optimization strategies implemented to improve productivity. By addressing these aspects, the research showcases its knowledge of resource optimization requirements in MLM systems and offers a streamlined solution.

The article focuses on user-centric design, prioritizing user demands and preferences to improve adoption and usability. It emphasizes pseudonymity and anonymity methods for privacy in the MLM system, ensuring participant privacy while maintaining accountability and traceability. The paper highlights immutability, privacy, authenticity, and confidentiality, detailing encryption methods and cryptographic protocols for data protection. Procedures for availability, robustness, and accountability are discussed, covering fault tolerance, redundancy, auditability, and disaster recovery. The framework demonstrates scalability solutions to handle growing network sizes and transaction volumes.

Data auditing strategies and consensus methods are explained to maintain transparency and integrity. The system's non-repudiation capacity is highlighted, ensuring participants cannot deny transactions or alter records. The cryptographic procedures for transaction integrity and non-repudiation are outlined. The article provides a comprehensive analysis of each parameter within the privacy-preserving MLM framework, covering system complexity, data sharing, access control, smart contracts, off-chain solutions, lightweight design, user-centricity, privacy, authenticity, accountability, confidentiality, availability, scalability, transparency, consensus, data auditing, non-repudiation, and robustness. This establishes a strong technical foundation for implementing the framework in blockchain-based MLM platforms.

The article [45] describes the process of rewarding active users in the MLM system using Enc and Signcrypt algorithms. The CID (company id) transaction latency represents the time taken for the company to process and complete reward payments for active users. Finalizing rewards on IDi or UIDx sites requires executing the Unsigncrypt algorithm for ADU (Active Direct Users) times. The IDi side of rewards is fast, while users with UIDx must execute the Unsigncrypt algorithm for ADU times, taking a specific period of time on the UIDx side. Transaction throughput for finalizing rewards on IDi or UIDx depends on the execution of the Unsigncrypt algorithm by ADU users, enabling them to receive rewards from lower layers. Each user can execute the algorithm to claim rewards. The given information emphasizes the importance of throughput as the number of transactions (rewards finalized) processed within a specific timeframe in the BB-MLM framework. However, details about block creation time and the specific consensus algorithm used are not provided, hindering a comprehensive evaluation of the system's performance.

Additionally, the framework utilizes cryptographic schemes like IBE, IBSC, and IB-PRE, which may impact data storage requirements and efficiency. To fully assess the system's scalability, security, and overall efficiency, more

information on block creation time, consensus algorithm efficiency, and data storage efficiency is required. These metrics are crucial for understanding how the BB-MLM framework performs in real-world scenarios and ensuring its effectiveness and reliability. Providing specific data on these aspects would enhance the evaluation and understanding of the system's technical capabilities.

The article [46] provides a technical overview of blockchain-based identity management for the IoT, emphasizing the challenges of implementing the SmartDID system in a complex IoT environment. It highlights the importance of access control techniques and secure data exchange to protect identity-related information. Smart contracts play a crucial role in the SmartDID system, ensuring accurate and transparent identity processes within the blockchain network. The article details the creation and use of smart contracts and their significance in identity management. Off-chain solutions are explored to improve scalability and efficiency while maintaining the accuracy of identity data stored on the blockchain.

The paper describes the ''lightweight solution'' strategy used in SmartDID to minimize resource needs and maximize system effectiveness in resource-constrained IoT environments. User-centric design empowers individuals to manage their identities and provide attribute information selectively. Cryptographic methods like zero-knowledge proofs or selective disclosure mechanisms are employed to maintain user privacy while using IoT applications. Privacy, anonymity, and immutability are addressed through cryptographic protocols and privacy-preserving techniques in SmartDID.

The paper also covers responsibility, authenticity, and secrecy aspects, discussing the use of cryptographic techniques and digital signatures to ensure integrity and veracity of identity-related transactions and safeguard private data. Availability and scalability are considered, with redundancy, fault-tolerant methods, sharding, or off-chain scaling strategies as potential solutions. The paper emphasizes transparency and auditable records of identity-related transactions achieved through blockchain technology. Consensus mechanisms like PoW or PoS are discussed in terms of obtaining agreement and validating transactions within the blockchain network.

Robustness, non-repudiation, and data auditing strategies are considered to ensure the correctness, integrity, and security of identity data. Performance metrics of SmartDID are analyzed, including block generation time and transaction processing time, as well as the time for creating Decentralized Identifiers (DIDs) and verifying credentials. Data storage efficiency is not explicitly mentioned, but SmartDID's performance metrics suggest better efficiency compared to other systems.

The proposed system [47] utilizes smart contracts to automate and secure the execution of predefined rules and conditions, enabling patient registration, update permissions, data sharing permissions, and viewership permissions. These contracts promote trust, transparency, and enforceability without the need for intermediaries, resulting in reduced administrative overhead and accurate healthcare transactions.

To enhance efficiency, cost-effectiveness, and scalability, the system employs IPFS storage for off-chain storage of COVID-19 credentials, effectively reducing on-chain data size. This approach enables the blockchain to handle larger volumes of data without compromising performance. The system demonstrates its scalability by accommodating various patient groups of different sizes. Through strategies like off-chain storage and efficient block creation, it ensures smooth performance even with increased data volumes and growing numbers of patients and healthcare providers.

Blockchain technology indeed offers several benefits for keeping medical information due to its immutability, data sharing, access control, privacy protection, and transparency features. These aspects ensure that sensitive health data is securely stored, only accessible by authorized individuals, and transactions are validated and authenticated, increasing trust and accuracy in healthcare data. However, the lack of specific information and numeric values in the assessment of system complexity, lightweight solution, user-centric design, pseudonymity, anonymity, privacy, confidentiality, availability, consensus mechanism, and data auditing makes it challenging to comprehensively evaluate the system's performance and effectiveness.

Without knowledge of the system's complexity, it is difficult to assess its manageability and understand its inner workings. The absence of details on a lightweight solution suggests that resource optimization and efficiency may not be prioritized, potentially leading to increased resource usage and decreased performance. A user-centric approach is crucial for user adoption and satisfaction. Without information on how the system caters to user preferences and needs, there could be reduced user uptake and suboptimal user experiences. Pseudonymity and anonymity are important for protecting users' identities and promoting privacy. The lack of information on these characteristics might limit users' ability to remain anonymous and raise privacy concerns. Privacy and confidentiality protections are critical for safeguarding patient information and ensuring data availability. The absence of specific details on these aspects might compromise patient data and healthcare services. Ethics play a crucial role in healthcare systems, and data auditing is essential for maintaining data integrity, traceability, and regulatory compliance. Without data auditing, it can be challenging to identify and rectify data issues, leading to potential biases and inequitable treatment for patients and stakeholders.

Transaction latency is a critical factor as it directly impacts the speed of processing, user experience, and real-time decision-making in healthcare systems. Specific numeric values on transaction latency, such as average transaction processing time or confirmation time, would provide valuable insights into the system's efficiency and responsiveness. Data storage effectiveness, especially with the implementation of off-chain storage technologies like IPFS, is essential for

TABLE 1. Comparison of literature review.

Performance Analysis																											
		Parameters																									
Existing Work	Reference Articles	System Complexity	Data Sharing and access control	Smart Contract	Off-Chain	Light Weight Solution	User Centric	Pseudonymity	Anonymity	Immutability	Privacy	Authenticity	Accountability	Confidentiality	Availability	Scalability	Transparency	Conscious Base	Data Auditing	Non-Repudiation	Robustness	Transaction Latency	Transaction Throughput	Block Creation Time	Consensus Algorithm Efficiency	Data Storage Efficiency
With KYC	[24]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	×	×	×	×	×
	[15]	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	×	×	×	×	×
	[25]	✓	✓	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	×	×	×	×	×
	[26]	✓	✓	✓	×	×	×	×	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×
	[27]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	×	×
	[16]	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	×	×	×	×	×
	[28]	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	✓	✓	✓	×	✓	×	✓	✓	✓	×	×	×	×	×
	[29]	✓	✓	✓	×	✓	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	×	×	×	×	×
	[30]	✓	✓	×	✓	×	×	×	×	✓	✓	✓	✓	×	✓	✓	✓	×	×	✓	✓	×	×	×	×	×
	[31]	✓	✓	✓	×	✓	✓	×	✓	✓	✓	✓	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×
	[32]	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×
	[33]	✓	✓	✓	×	×	×	×	×	×	✓	✓	×	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×
	[34]	×	×	×	✓	×	×	×	×	×	✓	✓	×	×	×	-	×	✓	-	×	✓	-	×	×	×	×	×
	[35]	✓	✓	✓	×	✓	×	×	×	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×	✓	×	×	-	×	×	×
Without KYC	[36]	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	×	×	×	×	×
	[37]	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×
	[38]	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓	-	✓	✓	✓	×	×	×	×	×
	[2]	✓	✓	✓	×	✓	✓	×	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×
	[39]	✓	✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×
	[40]	✓	✓	✓	×	✓	✓	×	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×	✓	✓	×	×	×	×	×	×
	[41]	✓	✓	✓	×	✓	✓	×	✓	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	×	×	×	×	×	×
	[42]	✓	✓	✓	×	×	✓	×	×	✓	✓	✓	×	✓	✓	×	✓	✓	✓	✓	×	×	×	×	×	×	×
	[43]	✓	✓	✓	×	×	✓	✓	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	×	×	×	✓	×	×	×
	[44]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	[45]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	[46]	✓	✓	✓	✓	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	-	×
	[47]	✓	✓	✓	✓	×	×	×	×	✓	✓	×	✓	✓	×	×	✓	✓	✓	×	✓	-	✓	×	×	×	✓	✓

efficient scaling and cost reduction in healthcare systems. Providing specific information on data storage efficiency, such as the reduction in on-chain data size achieved by using off-chain storage, would allow for a better understanding of the system's scalability and cost-effectiveness. Furthermore, numeric values on data retrieval times from off-chain storage and the impact on overall system performance would be valuable for assessing the system's ability to quickly update and retrieve medical records.

VI. OPEN RESEARCH AREAS

Integrating Blockchain into existing systems can be complex, yet it offers significant advantages, especially in Know Your Customer (KYC) processes within the banking sector. Traditional KYC procedures are often time-consuming, costly, and paperwork-intensive. In contrast, Blockchain-based KYC brings decentralization, enhanced security, and efficiency. While existing solutions have illuminated various aspects of incorporating Blockchain into KYC, there still remains areas that requires further exploration. Therefore, this section aims to identify and discuss a range of open research areas and design challenges related to Blockchain in KYC.

A. CONSENSUS MECHANISM AND SCALABILITY

- Designing a decentralized blockchain is more complex than designing a similar centralized system. Moreover, a mechanism for approving data depends on the consensus algorithm. The consensus algorithm may follow PoW, PoS, Delegated Proof of Stake (DPoS), or Byzantine Fault Tolerance (BFT). Mining in the blockchain is a simultaneous process of the PoW

algorithm, and multiple miners attempt simultaneously to solve the same puzzle. Therefore, much work is executed for the same result.

Use Cases for Consensus Algorithms

- Litecoin is akin to Bitcoin's PoW mechanism for quicker confirmation times and lower fees. PoS application in DeFi platforms and NFTs is akin to Ethereum 2.0's might uphold higher TPS. DPoS-based EOS.IO's dApp might boost transparency and reliability in the social media ecosystem. PBFT of Hyperledger brings integrity to the trade finance process.
- PPoS-based Algorand blockchain applications like SOV meets fast and reliable digital currency. Cardano's Ouroboros PoS allows parallel processing to speed up the environmental impact of cryptocurrencies like Bitcoin. MoneyGram is akin to Ripple's XRP Ledger - Consensus Protocol for cross-border payments and quick currency exchange settlements.

- Scalability improvement can enhance the performance of PoW. PoS depends on full node acceptance among the total nodes of a network. This consensus mechanism can be vulnerable to attacks by malicious actors. Security should be improved to ensure the efficiency of PoS. DPoS is a consensus algorithm with majority control over the network. Decentralization improvement can increase security and stability. BFT can be inefficient in its current performance, such as slow updates and loading compatibility. By improving efficiency, the performance issue can be solved.

B. STORAGE AND REGULATION

Regulation and storage are two related concepts with big significance for many different sectors. Regulations give directions and standards for carrying out storage activities, whereas storage entails the administration and preservation of assets. These laws guarantee lawful actions, compliance, safety, and security. For enterprises to reduce risks, protect integrity, and uphold ethical norms, storage requirements must be followed. By adhering to regulatory regulations, organizations can promote confidence, safeguard priceless assets, and support a secure and long-lasting working environment.

- The integration of IPFS with blockchain technology presents a robust solution for KYC data storage within a decentralized and peer-to-peer (P2P) network. This synergistic approach thrives within a private IPFS network, leveraging the emerging technology of IPFS document storage. However, it's essential to recognize that the efficiency of data transfer within IPFS depends on network conditions, stability, and data transfer speed, raising concerns about its scalability. Furthermore, the decentralized nature of IPFS, while advantageous, introduces security risks, such as the potential for malicious data injection. As IPFS is still in its early stages of development, it grapples with technical complexities surrounding maintenance, access control, monitoring, and data auditing, all of which require ongoing attention and refinement.
- The secure e-KYC landscape has evolved through a combination of symmetric and public key encryption, ensuring the protection of customer identity documents in the cloud and sensitive transaction data within the blockchain [73]. This approach utilizes lightweight cryptographic protocols for IPFS and integrates smart contracts for consent collection. It is worthwhile to mention that such fusion offers promising prospects for enhancing blockchain-based KYC systems, including user-initiated data updates and dynamic access control. Examining the scheme's performance under high e-KYC registration and verification volumes and exploring methods for enabling batch verification of e-KYC transactions within the blockchain are important open research areas. Additionally, further exploration is required into implementing searchable encryption features to advance privacy-preserving e-KYC systems. These research avenues offer the potential to significantly enhance the security and efficiency of identity verification processes through the synergies between IPFS and blockchain-based e-KYC developments.
- Regulators are pivotal in the world of Blockchain, overseeing its development, deployment, and ensuring security, data integrity, and privacy compliance. They establish the legal and regulatory framework, issue licenses, and closely monitor operations, particularly in the financial sector. Their role is critical in upholding safety, security, and reliability standards. Regulators enforce legal compliance, investigate validators, and set rules for consumer-facing blockchain applications, fostering trust and confidence in the technology's adoption across industries. Their responsibilities encompass jurisdiction-specific roles, case-driven variations, and diverse blockchain types, all aimed at safeguarding consumer interests and maintaining the technology's integrity. Few open regulation challenges are as follows,
  - The convergence of cutting-edge technologies represents a paradigm shift in how we approach identity verification and customer authentication in various sectors, particularly within the financial industry. The integration of blockchain's security and transparency features, the adaptability of humanoid robots, and the power of deep neural networks have collectively opened up unprecedented possibilities [74]. Moreover, the fusion of these technologies empowers us to reimagine the very essence of Know Your Customer (KYC) processes. This innovative approach empowers customers with control over their KYC identity while maintaining privacy and security in inter-bank ecosystems. A fundamental challenge inherent to this approach lies in meeting the current banking standards, which require an impeccable 100% customer satisfaction

rate, compelling the need for continuous human supervision of the automated system. Furthermore, it's essential to highlight the formidable challenges that regulators face when attempting to craft comprehensive regulations within the swiftly evolving domain of blockchain technology. This underscores the critical importance of adopting a balanced approach that harmonizes the imperative of innovation while safeguarding consumer interests in the dynamic and intricate landscape.

- Furthermore, the implementation of regulations by regulators in the context of international standard blockchain encounters several formidable challenges. These challenges arise from the intricate technical nature of blockchain systems, the difficulties related to ensuring interoperability with established system infrastructure, and the essential requirement of upholding uniform and cohesive regulations across diverse countries and jurisdictions. The hurdles and complexities faced by regulators when crafting regulations for blockchain technology underscore the imperative of adopting a balanced approach that carefully weighs the advantages of innovation and growth against the paramount need for ensuring consumer protection and safety.

C. BLOCKCHAIN PLATFORMS

- Ethereum; As a leading platform for smart contracts, Ethereum is a purpose-built ecosystem which uses the Solidity programming language] [72]. Its robust network effect, supported by active communities, leads to a rich ecosystem of tools and libraries. Decentralization is ensured through PoW, transitioning to PoS with Ethereum 2.0 for better scalability and energy efficiency. Ethereum remains popular due to its acceptance, durability, and cutting-edge ecosystem. The EVM and Solidity are vital for smart contracts, enabling flexible function creation and execution of arbitrary code. Token standards like ERC-20 and ERC-721 enhance compatibility and promote a robust token economy. Ethereum's open community governance fosters continuous improvement.
  - A decentralized and open-source blockchain platform is Ethereum. Ethereum enables the deployment and creation of decentralized Applications (dApps) that provide a decentralized virtual machine (EVM) to execute scripts by a global network of public nodes with Smart Contract features. The public ledger contains history and cannot be deleted from the network. Besides, the Ethereum network uses PoW for validation, where miners solve mathematical puzzles to validate block transactions, and miners earn rewards in the form of Ether. The environment has the potential for supply chain management. The Ethereum environment can be vulnerable to hacks and malicious attacks that can hamper sensitive data. Its implementation strongly impacts limited transactions per second, slow confirmation, and higher transaction costs.
  - On the other hand, a certain level of technical expertise is needed to implement Ethereum, which can be difficult to adopt and may not be compatible with other blockchain systems. As a result, it limits interaction between other technologies and faces regulatory uncertainty in many countries. The PoW mechanism consumes a lot of energy, leading to concerns about sustainability. Addressing these challenges and refining the Ethereum platform can help facilitate its adoption and integration with existing systems while maintaining security, privacy, and efficiency.
- Corda: FATF contributes to the finance industries' fight against crime in their AML/CFT framework, which incorporates cross-border threats. FATF's member countries are manually evaluated with a Grey and Black list. The implementation and advancement of VASP on a blockchain-based finance platform can be improved by setting rules for better performance through ICOs or token sales. Integration of VASP in FATF can automate the system as well.
- Hyperledger Fabric: HyperLedger Fabric is getting popular for protecting digital keys and sensitive data. It plays a vital role in the financial industry, especially in the customer verification procedure. However, its implementation depends on specific programming languages. The hyperledger fabric network can be modified with cross-chain interoperability protocols focusing on the consumer's criteria, which can enable customer identification to detect illegal activities.

VII. CONCLUSION

This survey article conducts an in-depth exploration of the application of Blockchain technology within the banking sector for Know Your Customer (KYC) processes. It comprehensively examines the adoption of blockchain in KYC and evaluates various recently developed blockchain-integrated KYC systems. Moreover, this article introduces a set of performance metrics aimed at evaluating the effectiveness of these blockchain solutions in the context of KYC processes within the banking industry. These metrics encompass crucial aspects such as data integrity, privacy, security, and scalability. While existing research has illuminated various facets of blockchain-based KYC, there are still some areas that necessitate further exploration. Therefore, this article also identifies the open research areas in the integration of blockchain for KYC, with a primary emphasis on consensus mechanisms, scalability, storage solutions, regulatory considerations, and the enhancement of blockchain platforms. These research directions are intended to address challenges, strengthen security and efficiency, and drive the evolution of KYC processes within the banking sector.

ACKNOWLEDGMENT

The authors would like to thank UTAR for giving the opportunity to publish articles apart from workload hours allocated at the University.

REFERENCES

[1] P. Ruce, "Anti-money laundering: The challenges of know your customer legislation for private bankers and the hidden benefits for relationship management (the bright side of knowing your customer)," *Banking LJ*, vol. 128, p. 548, 2011.

[2] P. Haveri, U. B. Rashmi, D. G. Narayan, K. Nagaratna, and K. Shivaraj, "EduBlock: Securing educational documents using blockchain technology," in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2020, pp. 1–7, doi: 10.1109/ICCCNT49239.2020.9225265.

[3] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[4] F. Glaser, "Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis," Tech. Rep., 2017.

[5] D. Martens, A. T. Van Serooskerken, and M. Steenhagen, "Exploring the potential of blockchain for KYC," HSTalks, London, U.K., Tech. Rep., 2017.

[6] B. Nguyen and D. Nguyen, "Improving KYC process by machine learning," Vietnam-Korea Univ. Inf., Tech. Rep., 2021.

[7] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, pp. 1–34, May 2020, doi: 10.1145/3316481.

[8] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity," *Inf. Manage.*, vol. 59, no. 7, Nov. 2022, Art. no. 103553, doi: 10.1016/j.im.2021.103553.

[9] H. Hassani, X. Huang, and E. Silva, "Banking with blockchain-ed big data," *J. Manage. Anal.*, vol. 5, no. 4, pp. 256–275, Oct. 2018.

[10] J. Thavanathan, "Process innovation with blockchain in banking—A case study of how blockchain can change the KYC process in banks," NTNU, Tech. Rep., 2017.

[11] M. Hannan, A. Shahriar, S. Ferdous, M. J. M. Chowdhury, and M. S. Rahman, "A systematic literature review of blockchain-based e-KYC systems," *Computing*, vol. 105, pp. 1–30, Apr. 2023, doi: 10.1007/s00607-023-01176-8.

[12] D. Malhotra, P. Saini, and A. K. Singh, "How blockchain can automate KYC: Systematic review," *Wireless Pers. Commun.*, vol. 122, no. 2, pp. 1987–2021, Jan. 2022, doi: 10.1007/s11277-021-08977-0.

[13] N. H. Arrifin and U. Subramanian, "Blockchain in banking," in *Proc. Int. Conf. Inf. Technol. Syst. Innov. (ICITSI)*, Nov. 2022, pp. 58–63, doi: 10.1109/ICITSI56531.2022.9970827.

[14] R. Weerawarna, S. Miah, and X. Shao, "Emerging advances of blockchain technology in finance: A content analysis," *Pers. Ubiquitous Comput.*, vol. 27, pp. 1–14, Feb. 2023, doi: 10.1007/s00779-023-01712-5.

[15] J. P. Moyano and O. Ross, "KYC optimization using distributed ledger technology," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 411–423, Dec. 2017, doi: 10.1007/s12599-017-0504-2.

[16] N. Ullah, K. A. Al-Dhlan, and W. M. Al-Rahmi, "KYC optimization by blockchain based hyperledger fabric network," in *Proc. 4th Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE)*, Mar. 2021, pp. 1294–1299, doi: 10.1109/AEMCSE51986.2021.00264.

[17] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain: A centralized tutorial," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–39, Jan. 2021, doi: 10.1145/3366370.

[18] P. Yadav and R. Chandak, "Transforming the know your customer (KYC) process using blockchain," in *Proc. Int. Conf. Adv. Comput., Commun. Control (ICAC)*, Dec. 2019, pp. 1–5, doi: 10.1109/ICAC347590.2019.9036811.

[19] A. Biryukov, D. Khovratovich, and S. Tikhomirov, "Privacy-preserving KYC on Ethereum," in *Proc. 1st ERCIM Blockchain Workshop*, 2018, doi: 10.18420/blockchain2018_09.

[20] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019, doi: 10.1109/ACCESS.2019.2903554.

[21] S.-W. Noh, Y. Park, C. Sur, S.-U. Shin, and K.-H. Rhee, "Blockchain-based user-centric records management system," *Int. J. Control Autom.*, vol. 10, no. 11, pp. 133–144, Nov. 2017, doi: 10.14257/ijca.2017.10.11.12.

[22] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: A state of the art review," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–5, Dec. 2020, doi: 10.1186/s13638-020-01665-w.

[23] A. Al Omar, A. Jamil, A. Khandakar, A. Uzzal, R. Bosri, N. Mansoor, and M. Rahman, "A transparent and privacy-preserving healthcare platform with novel smart contract for smart cities," *IEEE Access*, vol. 9, pp. 90738–90749, 2021, doi: 10.1109/ACCESS.2021.3089601.

[24] A. Al Mamun, S. R. Hasan, M. S. Bhuiyan, M. S. Kaiser, and M. A. Yousuf, "Secure and transparent KYC for banking system using IPFS and blockchain technology," in *Proc. IEEE Region Symp. (TENSYMP)*, Jun. 2020, pp. 348–351, doi: 10.1109/TENSYMP50017.2020.9230987.

[25] Y. Lootsma, "Blockchain as the newest regtech application—The opportunity to reduce the burden of KYC for financial institutions," Banking Financial Services Policy Rep., vol. 36, 2017, pp. 16–21.

[26] A. Xu, M. Li, X. Huang, N. Xue, J. Zhang, and Q. Sheng, "A blockchain based micro payment system for smart devices," *Signature*, vol. 256, p. 115, 2016.

[27] L. Cocco, A. Pinna, and M. Marchesi, "Banking on blockchain: Costs savings thanks to the blockchain technology," *Future Internet*, vol. 9, no. 3, p. 25, Jun. 2017, doi: 10.3390/fi9030025.

[28] B. Rankhambe and H. Khanuja, "Hassle-free and secure e-KYC system using distributed ledger technology," *Int. J. Next-Gener. Comput.*, vol. 12, no. 2, pp. 74–90, Apr. 2021, doi: 10.47164/ijngc.v12i2.209.

[29] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5, doi: 10.1109/PIMRC.2017.8292361.

[30] A. Soni and R. Duggal, "Reducing risk in KYC (know your customer) for large Indian banks using big data analytics," *Int. J. Comput. Appl.*, vol. 97, no. 9, pp. 1–5, 2014, doi: 10.5120/17039-734710.5120/17039-7347.

[31] E. Bandara, S. Shetty, R. Mukkamala, X. Liang, P. Foytik, N. Ranasinghe, and K. De Zoysa, "Casper: A blockchain-based system for efficient and secure customer credential verification," *J. Banking Financial Technol.*, vol. 6, no. 1, pp. 43–62, Jun. 2022, doi: 10.1007/s42786-021-00036-3.

[32] S. Küfeoğlu, E. Açıkgöz, Y. E. Taşcı, T. Y. Arslan, J. Priesmann, and A. Praktiknjo, "Designing the business ecosystem of a decentralised energy datahub," *Energies*, vol. 15, no. 2, p. 650, Jan. 2022, doi: 10.3390/en15020650.

[33] K. Chandraprabha, "Blockchain-based implementation on electronic know your customer (e-KYC)," in *Intelligent Communication Technologies And Virtual Mobile Networks*, 2023, pp. 281–297, doi: 10.1007/978-981-99-1767-9_22.

[34] B. Dhiman and R. Bose S, "A reliable, secure and efficient decentralised conditional of KYC verification system: A blockchain approach," in *Proc. Int. Conf. Edge Comput. Appl. (ICECAA)*, Oct. 2022, pp. 564–570, doi: 10.1109/ICECAA55415.2022.9936486.

[35] C. Lee, C. Kang, W. Choi, M. Cha, J. Woo, and J. W.-K. Hong, "CODE: Blockchain-based travel rule compliance system," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Aug. 2022, pp. 222–229, doi: 10.1109/Blockchain55522.2022.00038.

[36] O. Saleh, O. Ghazali, and M. Rana, "Blockchain based framework for educational certificates verification," *J. Crit. Rev.*, vol. 7, pp. 79–84, 2020.

[37] V. Marella and A. Vijayan, "Document verification using blockchain for trusted CV information," in *Proc. AMCIS*, 2020.

[38] V.-C. Nguyen, H.-L. Pham, T.-H. Tran, H.-T. Huynh, and Y. Nakashima, "Digitizing invoice and managing VAT payment using blockchain smart contract," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 74–77, doi: 10.1109/BLOC.2019.8751256.

[39] M. Mylrea and S. N. G. Gourisetti, "Blockchain: A path to grid modernization and cyber resiliency," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–5, doi: 10.1109/NAPS.2017.8107313.

[40] N. H. Kim, S. M. Kang, and C. S. Hong, "Mobile charger billing system using lightweight blockchain," in *Proc. 19th Asia–Pacific Netw. Oper. Manage. Symp. (APNOMS)*, Sep. 2017, pp. 374–377, doi: 10.1109/APNOMS.2017.8094151.

[41] W. Grther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres, and F. Wendland, "Blockchain for education: lifelong learning passport," in *Proc. 1st ERCIM Blockchain Workshop*, 2018, doi: 10.18420/blockchain2018_07.

[42] A. Vishwa and F. K. Hussain, "A blockchain based approach for multimedia privacy protection and provenance," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2018, pp. 1941–1945, doi: 10.1109/SSCI.2018.8628636.

[43] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates," *Softw., Pract. Exper.*, vol. 52, no. 4, pp. 841–867, Apr. 2022, doi: 10.1002/spe.2983.

[44] P. Saranya and R. Maheswari, "Proof of transaction (PoTx) based traceability system for an agriculture supply chain," *IEEE Access*, vol. 11, pp. 10623–10638, 2023, doi: 10.1109/ACCESS.2023.3240772.

[45] S. B. Far, M. R. Asaar, and A. Haghbin, "A privacy-preserving framework for blockchain-based multi-level marketing," *Comput. Ind. Eng.*, vol. 177, Mar. 2023, Art. no. 109095, doi: 10.1016/j.cie.2023.109095.

[46] J. Yin, Y. Xiao, Q. Pei, Y. Ju, L. Liu, M. Xiao, and C. Wu, "SmartDID: A novel privacy-preserving identity based on blockchain for IoT," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 6718–6732, doi: 10.1109/JIOT.2022.3145089.

[47] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *J. Ambient Intell. Humanized Comput.*, vol. 13, pp. 1–11, 2022, doi: 10.1007/s12652-021-03163-3.

[48] S. S. Kamble, A. Gunasekaran, and R. Sharma, "Modeling the blockchain enabled traceability in agriculture supply chain," *Int. J. Inf. Manage.*, vol. 52, Jun. 2020, Art. no. 101967, doi: 10.1016/j.ijinfomgt.2019.05.023.

[49] B. Tyma, R. Dhillon, P. Sivabalan, and B. Wieder, "Understanding accountability in blockchain systems," *Accounting, Auditing Accountability J.*, vol. 35, no. 7, pp. 1625–1655, Aug. 2022, doi: 10.1108/AAAJ-07-2020-4713.

[50] R. Mulgan, "Comparing accountability in the public and private sectors," *Austral. J. Public Admin.*, vol. 59, no. 1, pp. 87–97, Mar. 2000, doi: 10.1111/1467-8500.00142.

[51] R. L. Lewis, D. A. Brown, and N. C. Sutton, "Control and empowerment as an organising paradox: Implications for management control systems," *Accounting, Auditing Accountability J.*, vol. 32, no. 2, pp. 483–507, Feb. 2019, doi: 10.1108/AAAJ-11-2017-3223.

[52] D. Rus, D. van Knippenberg, and B. Wisse, "Leader power and self-serving behavior: The moderating role of accountability," *Leadership Quart.*, vol. 23, no. 1, pp. 13–26, Feb. 2012, doi: 10.1016/j.leaqua.2011.11.002.

[53] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K.-R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101966, doi: 10.1016/j.cose.2020.101966.

[54] F. Hofmann, S. Wurster, E. Ron, and M. Bohmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," in *Proc. ITU Kaleidoscope, Challenges Data-Driven Soc. (ITU K)*, Nov. 2017, p. 18, doi: 10.23919/ITU-WT.2017.8247004.

[55] J. Casti, "On system complexity: Identification, measurement, and management," in *Complexity, Language, and Life: Mathematical Approaches*, 1986, pp. 146–173, doi: 10.1007/978-3-642-70953-1_6.

[56] A. E. Ferdinand, "A theory of system complexity," *Int. J. Gen. Syst.*, vol. 1, no. 1, pp. 19–33, Jan. 1974, doi: 10.1080/03081077408960745.

[57] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, and B. Gipp, "On-chain vs. off-chain storage for supply- and blockchain integration," *It-Inf. Technol.*, vol. 60, nos. 5–6, pp. 283–291, Dec. 2018, doi: 10.1515/itit-2018-0019.

[58] J. Chen, "Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks," *ACM SIGBED Rev.*, vol. 15, no. 5, pp. 22–28, Nov. 2018, doi: 10.1145/3292384.3292388.

[59] S. Benouar and A. Benslimane, "Robust blockchain for IoT security," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013580.

[60] L. Tian, "Robust and effective consensus approaches for blockchain systems," Univ. Tasmania, Tech. Rep., 2021, doi: 10.25959/23250257.v1.

[61] J. Yadav and R. Shevkar, "Performance-based analysis of blockchain scalability metric," *Tehnički Glasnik*, vol. 15, no. 1, pp. 133–142, Mar. 2021, doi: 10.31803/tg-20210205103310.

[62] P. Jogalekar and M. Woodside, "Evaluating the scalability of distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 6, pp. 589–603, Jun. 2000, doi: 10.1109/71.862209.

[63] B. Seok, J. Park, and J. H. Park, "A lightweight hash-based blockchain architecture for industrial IoT," *Appl. Sci.*, vol. 9, no. 18, p. 3740, Sep. 2019, doi: 10.3390/app9183740.

[64] L. Wan, D. Eyers, and H. Zhang, "Evaluating the impact of network latency on the safety of blockchain transactions," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 194–201, doi: 10.1109/Blockchain.2019.00033.

[65] C. Li, P. Li, D. Zhou, Z. Yang, M. Wu, G. Yang, W. Xu, F. Long, and A. Yao, "A decentralized blockchain with high throughput and fast confirmation," in *Proc. USENIX Annu. Tech. Conf. (USENIXATC)*, 2020, pp. 515–528.

[66] F. Hashim, K. Shuaib, and N. Zaki, "Sharding for scalable blockchain networks," *Social Netw. Comput. Sci.*, vol. 4, no. 1, Oct. 2022, doi: 10.1007/s42979-022-01435-z.

[67] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, "SimBlock: A blockchain network simulator," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2019, pp. 325–329, doi: 10.1109/INFCOMW.2019.8845253.

[68] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Syst. Appl.*, vol. 154, Sep. 2020, Art. no. 113385, doi: 10.1016/j.eswa.2020.113385.

[69] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Appl. Sci.*, vol. 10, no. 6, p. 2011, Mar. 2020, doi: 10.3390/app10062011.

[70] M. Alizadeh, K. Andersson, and O. Schelén, "Efficient decentralized data storage based on public blockchain and IPFS," in *Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE)*, Dec. 2020, pp. 1–8, doi: 10.1109/CSDE50874.2020.9411599.

[71] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. Al Azad, and N. Mansoor, "Verifi-chain: A credentials verifier using blockchain and IPFS," 2023, *arXiv:2307.05797*, doi: 10.48550/arXiv.2307.05797.

[72] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Ethereum smart contract analysis tools: A systematic review," *IEEE Access*, vol. 10, pp. 57037–57062, 2022, doi: 10.1109/ACCESS.2022.3169902.

[73] S. Fugkeaw, "Enabling trust and privacy-preserving e-KYC system using blockchain," *IEEE Access*, vol. 10, pp. 49028–49039, 2022, doi: 10.1109/ACCESS.2022.3172973.

[74] M. Hajiabbasi, E. Akhtarkavan, and B. Majidi, "Cyber-physical customer management for Internet of robotic things-enabled banking," *IEEE Access*, vol. 11, pp. 34062–34079, 2023, doi: 10.1109/ACCESS.2023.3263859.

NAFEES MANSOOR (Senior Member, IEEE) received the B.Sc. degree (cum laude) in computer science and the M.Sc. degree in telecommunication engineering from Independent University, Bangladesh (IUB), and the Ph.D. degree from Universiti Teknologi Malaysia (UTM), in 2016, with a focus on communication systems and networks. He is currently an Associate Professor with the Department of Computer Science and Engineering, University of Liberal Arts Bangladesh (ULAB), where he is also a Coordinator of the Faculty Research Office. His research interests include ad hoc networks, information security, and digital twin. He was a recipient of the best paper awards at the ICAICT 2016, RISP-NCCP 2015, ICEEE 2014, and MJJIS 2013. He was also a recipient of the JACTIM Research Proposal Award, in 2012. He is serving as an Associate Editor for IEEE Access journal.

KANIZ FATEMA ANTORA (Member, IEEE) is currently pursuing the B.Sc. degree in computer science and engineering (CSE) with the University of Liberal Arts Bangladesh (ULAB). She is also with ULAB as an on-campus mentor teaching math and a Teaching Assistant with the Department of CSE, ULAB. Her research interests include blockchain technology and computational geometry. She had contributed to IEEE ULAB Student Branch as the Chairperson (2022–2023).

PRIYATA DEB is currently pursuing the degree with the Computer Science and Engineering Department, University of Liberal Arts Bangladesh. Her research interest includes blockchain technology.

TAREK AHAMMED ARMAN is currently pursuing the degree with the Computer Science and Engineering Department, University of Liberal Arts Bangladesh. His research interest includes blockchain technology.

AZIZAH ABDUL MANAF has published her works in numerous high-indexed journals and conference proceedings and to this date has achieved a very high number of citations. Her research interests include image processing and pattern recognition and information security specifically in watermarking and steganography. Her past and current research has been fully sponsored mostly by the government and industries related to her specialty.

MAHDI ZAREEI (Senior Member, IEEE) received the M.Sc. degree in a computer network from the University of Science, Malaysia, in 2011, and the Ph.D. degree from the Communication Systems and Networks Research Group, Malaysia-Japan International Institute of Technology, University of Technology, Malaysia, in 2016. In 2017, he joined the School of Engineering and Sciences, Tecnologico de Monterrey, as a Postdoctoral Fellow, where he has been a Research Professor, since 2019. His research interests include wireless sensor and ad hoc networks, information security, applied machine learning, and natural language processing. He is a member of the Mexican National Researchers System (level I). He is also serving as an Associate Editor for IEEE Access, *PLOS One*, and *Ad Hoc and Sensor Wireless Networks* journals.