IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 18 March 2024, accepted 21 April 2024, date of publication 1 May 2024, date of current version 14 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3395918

SURVEY

The Role of Blockchain in Finance Beyond Cryptocurrency: Trust, Data Management, and Automation

HANFANG CHEN[1,2], NIANKUN WEI[1], LEYAO WANG[1], WAEL FAWZY MOHAMED MOBARAK[3,4], MARWAN ALI ALBAHAR[5], AND ZAFFAR AHMED SHAIKH[6], (Member, IEEE)

[1]School of Economics and Management, Hubei University of Technology, Wuhan 430068, China
[2]Postdoctoral Research Station, School of Public Finance and Public Administration, Jiangxi University of Finance and Economics, Nanchang, Jiangxi 330013, China
[3]Civil Engineering Department, College of Engineering, University of Business and Technology, Jeddah 21448, Saudi Arabia
[4]Engineering Mathematics Department, Alexandria University, Alexandria 21544, Egypt
[5]Computer Science Department, Umm Al-Qura University, Mecca 16786, Saudi Arabia
[6]Department of Computer Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi, Sindh 75660, Pakistan

Corresponding author: Leyao Wang (1052577419@qq.com)

This research is funded by the Foundation of Hubei University of Technology: Research on the impact mechanism of macro tax burden changes driving innovation and development in the real economy, and their co-track spillover effects (BSQD2020083); Humanities and Social Sciences Youth Foundation, Ministry of Education: Research on the measurement of spatial effects of transfer payments on improving the economic resilience of poverty-stricken areas and sustainable mechanisms (21YJC790008); the 69th batch of grants from China Postdoctoral Science Foundation: Research on the spatial effect of transfer payments on improving the economic resilience of poverty-stricken areas (2021M691348).

ABSTRACT Blockchain has been a vibrant technology in the past decade, with a wide variety of applications across different industrial sectors. The concept of blockchain has been widely recognized as an enabler for cryptocurrency-based decentralized payments, with two major decentralized payment systems such as Bitcoin and Ethereum. However, the global acceptance of blockchain as a cryptocurrency sums up significant challenges that hinder the fast adaptation of cryptocurrency as a payment service enabler. In this survey, we explore the advantages of blockchain and its technical capabilities beyond cryptocurrency. We focus on the technical potential to ensure trust, data governance, and automation of the financial application domain utilizing the fundamental security features of blockchain, including consensus, digital signatures, and transparency. The significant subcomponents of trust, data management, and automation in banking and financial systems are also identified and discussed, including how blockchain and smart contracts can achieve the anticipated features of each subcomponent through their technical capabilities. In addition, we shed light on the position of blockchain-based applications in key application sectors of the banking and financing domain with a mapping of technical features with the application domains. Thereafter, the applicability of blockchain-based applications is evaluated with relevant regulatory definitions. Finally, we discuss open research challenges and potential future works with the blockchain in the domain of financial systems.

INDEX TERMS Automation, Bitcoin, blockchain, cryptocurrency, data governance, decentralized payments, Ethereum, finance, financial application domain, survey, transparency, trust.

I. INTRODUCTION

The financial industry is transforming towards an Information Technology (IT)-enabled evolution with significant technological advancement to align with global economic dynamics. The rapidly changing economic landscape with extensive requirements of diversified capabilities of financial applications, emerges significant technological challenges. In addition, the regulatory requirements that enforce standards of personal data management, trust, and traceability of financial events incur additional effort for the innovators of financial systems to design the systems to align with the standardization requirements. In recent years, the emergence of blockchain technology has revolutionized the financial landscape with its initial association with cryptocurrencies. Cryptocurrency is an alternative to fiat currency that enables

The associate editor coordinating the review of this manuscript and approving it for publication was Thanh Ngoc Dinh.

TABLE 1. Summary of important acronyms.

Acronym	Definition
AML	Anti Money Laundering
API	Application Programming Interface
EFT	Electronic Fund Transfer
GDPR	General Data Protection Regulation
IT	Information Technology
KYC	Know Your Customer
ML	Machine Learning
FL	Federated Learning
IoT	Internet of Things
MiTM	Man in The Middle
PoS	Proof of Stake
PoW	Proof of Work
SMS	Short Message Service
XAI	Explainable Artificial Intelligence

consumers to transfer payments without the intervention of intermediaries [1]. Bitcoin [2] is the world's first and most well-known cryptocurrency, enabling peer-to-peer payment transactions without the intervention of trusted third parties such as payment associations operated for Fiat currencies. The system enables payments without a third party and the transactions committed to the network are subject to verification by dedicated nodes called miners, using cryptographic techniques. Buterin et al. [3] extended the blockchain towards the distinguishing concept of smart contracts, emphasizing the unique capability of operation as a decentralized program on the blockchain network. The program is immutable and cryptographically verified immutability to ensure the trust and integrity of the program. As in Bitcoin, smart contracts execute in a peer-to-peer mode without the contribution of a centralized third party and service availability without any centralized dependency. The autonomous execution conditions define the logical conditions to execute a sequence of events comparable to the paper contracts.

Blockchain, which is empowered with decentralized and distributed ledger technology, gained prominence through its unique capabilities in ensuring the integrity of transactions using the cryptographically interlinked distributed ledger including cryptocurrency networks. However, the potential of blockchain extends far beyond the boundaries in the context of securing financial ecosystems as an enabler for cryptocurrency. As financial institutions face significant challenges related to trust, data management, and automation, blockchain offers promising solutions by utilizing its unique capabilities of decentralization to eliminate important challenges that emerge in the financial ecosystems. This survey identifies substantial challenges in different and interrelated contexts in the financial ecosystems and explores the capabilities of blockchain to alleviate these challenges.

Trust is a fundamental requirement of any financial system. Trust in finance depends on top moral foundations [4], which attract consumers, enterprises, and regulatory authorities to rely on the economic systems for financial transactions. Transparency in the automated decision-making process is important to ensure consumer trust in financial systems [5]. Overall, trust establishment is challenging with the complicated evolution of classical banking systems with the digital transformation of banking with mobile and electronic banking [6]. The attack surfaces are complex with the existence of heterogeneous electronic banking applications.

Secured consumer data management is important in the information era, which is characterized by large amounts of sensitive information consumer information [7]. Regulatory compliance to the data management [8] has been strictly enforced by the statutory authorities for the financial ecosystems by introducing data protection regulations such as GDPR [9]. Even though the statutory organizations urge secure data management policies, including regulations such as GDPR compliance [10], there exists a significant set of practical challenges that make the enforcement harder.

Automating the processes in financial ecosystems is significantly important in the context of finance to cope with the scale of consumer demand anticipated in the future. Automation streamlines the different processes of financial ecosystems, including credit decision-making, customer onboarding, and fund transfers, with reduced costs and improved efficiency compared with the human-intervened approaches. Especially, the evolution of automation techniques facilitates the ecosystems with real-time decision-making [11], thereby increasing efficiency. In the context of the financial industry, automation optimizes key tasks such as transaction processing [12], risk management [13], compliance, and financial reporting [14]. In addition to the banking sector, automated stock trading algorithms execute the buying and selling of stock transactions in milliseconds, leveraging automated data analytics and intelligent decision-making techniques to identify profitable opportunities and minimize risks of losses incurred by human errors. Similarly, automated loan processing systems analyze vast amounts of data for computational modeling of the individual's financial behavioral features to assess consumer creditworthiness and make lending decisions quickly and accurately [15] with zero paperwork. Automation plays a pivotal role in regulatory compliance, where financial institutions rely on automated systems for surveillence [16] and ensure adherence to regulatory requirements. In this paper, we explore the role of blockchain in the financial application context, with a comprehensive overview of the technical capabilities of blockchain to advance trust, secured data management, and automation to provide an extended value for consumers. In addition, this survey aims to contribute valuable insights to the scientific community, including researchers and practitioners who navigate the evolving landscape of blockchain in the financial domain.

Abou and George [17] explained blockchain-based applications in different contexts, including finance. The authors mainly highlighted the capabilities of blockchain to improve transaction processing, sustainable banking, enhanced financial transaction security, and automated financial transactions. Monrat et al. [18] explained the significant applications of blockchain in different application domains. The authors

highlighted the potential of blockchain to improve the trade finance and stock exchange with advanced security. Zhang et al. [19] introduce a blockchain-based project financing instrument for infrastructure projects in China. The authors highlighted the strengths of blockchain, including information irreversibility to improve the project financing systems. Almesha and Alhogail [20] examined the state-of-the-art evaluation models and frameworks to identify the adaptation requirements of blockchain for different applications such as finance, insurance, logistics, government, education, and healthcare. In the financial domain, the authors highlighted the potential of Blockchain 2.0, smart contracts can enable the security of a wide range of financial applications such as smart property trading, securities trading, supply chain finance, anti-fraud systems, banking instruments, credit systems, and mutual insurance using the autonomous execution capabilities with data provenance. Zhang et al. [21] highlighted the potential of blockchain to automatically identify customer credit conditions in loan application processing, restructure the financial market collaborators as a cooperative system with strengthened communication, as an enabler for improved cross-border payments, and as a digital asset registry. The authors have highlighted the significant challenges of financial regulation and global collaboration due to complexity. Nguyen [22] explained the role of blockchain as a financial tool for the sustainable development of the global economy from an analytical perspective. The author has highlighted that the new technology can bring massive benefits to the consumers of the current banking system and society. However, the author elaborated on the significant challenges of blockchain as a financial enabler, such as the lack of adaptation of the legal and policy systems, with observational insights on the global integration delay of Bitcoin for the past years. Schar [23] proposed a multi-layer framework for the analysis of various blockchain-based decentralized financial applications, including token standards, decentralized exchanges, and debt markets. The author has emphasized that the decentralized financial markets are still niche with interesting features such as efficiency, transparency, and composability. However, the author elaborated on the associated risks of blockchain in finance, including the risk of illicit activities, dependencies, and scalability limitations. Yu et al. [24] explain blockchain's potential capabilities in financial accounting. The authors highlighted the inherent features of blockchain, including transparency and traceability, to resist the prevalent frauds of state-of-the-art financial accounting systems. Patel et al. [25] presented a bibliometric and content analysis on blockchain technology for the banking and financial application domains. The authors explained the role of blockchain in interesting financial applications such as cryptocurrency, tokenization, and crowdfunding. Furthermore, the authors reflected significant insights on financial regulation and sustainability. Chang et al. [26] investigated blockchain adoption cases in financial services. The authors explained the key technical features of blockchain, elaborating on the key challenges such as scalability, energy consumption, and privacy issues. The authors also highlighted the key ethical issues in blockchain, including privacy, regulation challenges, and cybercrime risk, which can emerge with blockchain integration. Sriman and Kumar [27] explained the significance of cryptocurrency with a review of theoretical and practical implications. Tian et al. [28] analyzed the significance of security tokens to provide transaction efficiency and transparency with concrete examples of energy asset security tokens. The authors also highlighted that the potential of tokenization was not fully realized due to the technical infrastructure, regulatory uncertainties, volatilities in the token market, and lack of intervention of the state sector. Identifying the importance of blockchain for trust, data management, and automation for the sector of banking and finance, we propose,

1) A review and reflections on the technical features of blockchain and how they are applicable to trust, automation, and data management.
2) Brief review on the state of art cryptocurrency.
3) A comprehensive review on the trust components in finance
4) A comprehensive review on the secured data management in finance
5) A comprehensive review of the potential automation applications of blockchain
6) A proposal of novel two-layered blockchain architecture that enables blockchain as a decentralized service to facilitate trust, data management, and automation for financial stakeholders
7) Key insights and open challenges with integration architecture and the applicable regulatory bodies

Table 2 reflects a summary of our contribution beyond the state of the art. The rest of the paper is organized as follows: Section II presents the technical background of blockchain, focusing on its current position and technical capabilities. Section III describes the components of trust in finance. Section IV emphasizes the role of blockchain for secured data management. Section III emphasizes the potential automation components of the blockchain that can be applied to improve financial applications. Section VI illustrates the significant applications of blockchain in the domain of finance. Section VII proposes a novel integration architecture for the blockchain with a multilayered approach to improve trust, data management, and automation in finance with a focus on regulatory compliance. Section VIII concludes the paper. Table 1 includes important acronyms used in the paper.

II. BACKGROUND OF BLOCKCHAIN

This survey emphasizes the significant properties of blockchain and smart contracts, which have the strong potential to improve financial applications by improving trust, data management, and automation. In this section,

TABLE 2. Previous surveys on blockchain-based smart contracts.

Ref	Description	Comparison with our contribution
[17]	**Blockchain applications–usage in different domain**: A comprehensive survey that emphasizes the significance of blockchain from a general perspective, including finance.	Our survey is a more focused study on the context of finance while highlighting the technical strengths of blockchain for trust, data management, and automation. We also point out the position of technical capabilities with the definitions of regulatory frameworks.
[18]	**A survey of blockchain from the perspectives of applications, challenges, and opportunities**: The role of blockchain has been discussed without a specific focus on the context of finance.	Our work specifically identifies the components of trust, data management, and automation. It highlights the potential of the technical capabilities of blockchain to achieve the features of these components in a more focused financial domain.
[19]	**Framework for a blockchain-based infrastructure project financing system**: Reflects the insights of blockchain applicability for project financing.	Our scope is not limited to project financing, and we explored different potential applications in a wider perspective. We also considered how the technical capabilities of blockchain support the regulatory frameworks.
[20]	**Blockchain for businesses: a scoping review of suitability evaluation frameworks**: A comprehensive survey that discovers the applicability of blockchain in business applications.	In contrast, we discuss the technical features in detail to ensure trust, data management, and automation with a specific focus on the financial applications, including the supportive regulatory definitions.
[21]	**The challenges and countermeasures of blockchain in finance and economics**: Automated credit decisions and several applications of blockchain have been discussed. The technical strengths were not discussed.	We reflected on the applications of blockchain for different categories, including the position of regulatory definitions, and also discussed the potential of blockchain to improve future research domains that apply to banking and finance.
[22]	**Blockchain-a financial technology for future sustainable development** : Reflects the role of blockchain in global sustainability.	We decomposed We discussed mostly on the applications of blockchain in the present and future to envision the community towards a direction that leverages the blockchain for a wide range of future financial applications.
[29]	**Blockchain: A Survey on Functions, Applications and Open Issues**: Presents an analysis of blockchain and its applications along with different open issues.	Our work specifically focuses on finance, from the application of a novel architecture to improving trust, data management, and automation.
[30]	**Blockchain and Its Applications – A Detailed Survey** : A high-level discussion on blockchain and its applicability in different contexts.	Rather than discussing in a more high-level perspective, we discuss the applicability of blockchain in detail for financial applications.

we discuss the properties of blockchain with a technical focus on the underlying principles.

A. TECHNOLOGICAL FOCUS ON BLOCKCHAIN

Blockchain transaction workflow exists with five generic steps, regardless of the blockchain platform and consensus mechanism. As indicated in Figure 1, the following events can be identified.

1) **Blockchain network receives the new event**: This is the initial point of a blockchain transaction that receives the transaction from external services. In financial applications, this can be either a request to verify the credentials, transfer a particular asset, or even a new customer registration event received from the banking system. External Application Programming Interfaces(API) of the blockchain network generally integrate with the external services.
2) **The event is converted into a transaction**: In this step, the event will be converted into the generic form, which will make it understandable to the blockchain network. Specifically, the blockchain network predefines the form of a transaction, the mandatory elements to be included, and so on. This transaction will be included as blocks in chronological order.
3) **The node performs the action that fulfills the condition** The consensus requires a particular condition to be achieved to authorize the new blocks of transactions to be included in the blockchain ledger. In Bitcoin [2], this is Proof of Work, which requires the generation of a hash value with four leading zeros, while in Ethereum [31], the condition is the Proof of Stake.
4) **The node mines new block:**Once the condition is fulfilled, the new node mines the block that consists of new transactions. In this scenario, the new block is disseminated within the network.
5) **The new block is verified:** Once the condition is fulfilled, the new node mines the block that consists of new transactions. If the blockchain nodes can verify, the new block is eligible for addition to the new ledger.

As indicated in Figure 2, blockchain has three main components distributed ledger, mining and consensus mechanism, and smart contracts. The three main components are described below.

1) DISTRIBUTED LEDGER

The distributed ledger is a decentralized database that exists consistently across multiple peers of the network. It ensures availability by transforming the instances from one

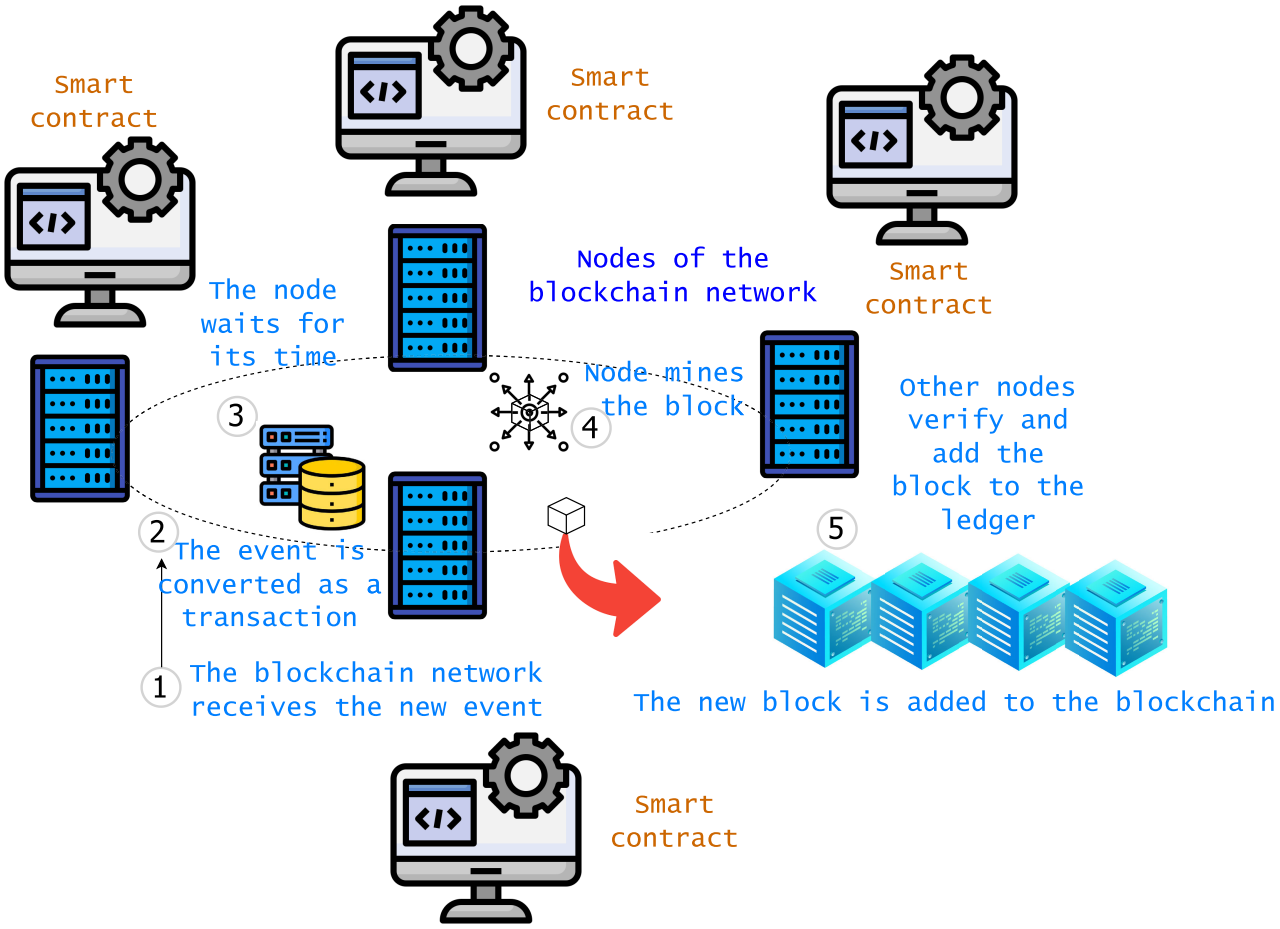


FIGURE 1. Blockchain workflow.

single instance to another. In a distributed ledger, no single entity controls the server. The distributed ledger provides transparency for all participants. The distributed ledger is cryptographically integrity preserved, and forging the records of the distributed ledger is computationally hard, thereby guaranteeing an improved level of security. The distributed ledger plays a distinguishing role in establishing trust in the stored data.

Depending on the blockchain platform and its properties, the distributed ledger has been implemented. It is important to note that a blockchain is a form of distributed ledger that interconnects bunches of transactions in the form of blocks with cryptographic links. Each transaction and each block is cryptographically linked in chronological order. This data structure can be implemented on different technical platforms. For example, Hypedrledger Fabric [32] uses the CouchDB database to implement the blockchain ledger as a NoSQL record. In Mystiko blockchain [33], the Cassandra database has been utilized to implement the distributed ledger with eventual consistency.

2) MINING AND CONSENSUS MECHANISM

The consensus mechanism is a fundamental trust-building service in the blockchain ecosystem. It decides the utmost condition of block mining, which is collaboratively verifiable and provable among the members of the blockchain network. The consensus condition can be defined depending on the requirements of the blockchain network stakeholders. The consensus mechanism is the most important part of the blockchain, making its function "collaborative." The Consensus mechanism includes the transaction approval process upon corporate decision.

Depending on the properties of the blockchain platform, the consensus mechanisms vary. For example, Bitcoin [2] uses Proof of Work consensus while Ethereum [31] uses Proof of Stake consensus. In addition, the blockchain platforms use different consensus mechanisms such as Hyperledger Fabric [34] that utilize voting-based consensus.

3) SMART CONTRACT

A smart contract is an immutable, consistent software program that operates on each member blockchain node. The smart contract ensures that the program operates on the decentralized node itself, which reduces latency compared with the cloud. Smart contracts can be dynamically deployed and operate consistently over the network.

The smart contracts can be different depending on the requirement. For example, Ethereum uses Solidity as the

programming language of smart contracts. Furthermore, Hyperledger Fabric provides flexibility in NodeJS, Java, and Go programming languages.

B. CURRENT POSITION OF BLOCKCHAIN'S TECHNOLOGICAL CAPABILITIES IN FINANCE

The concept of blockchain emerged with the invention of Bitcoin by Satoshi Nakamoto in 2008, who published the whitepaper entitled ''Bitcoin: A Peer-to-Peer Electronic Cash System'' [2]. This whitepaper proposed a digital currency system that operates on the distributed ledger. The key distinguishing feature of Bitcoin is its decentralized operational capability when compared with the centralized financial ecosystems. However, the first conceptual presentation of smart contracts by Nick Szabo dates back to 1994 [35]. In 2013, Vitalik Buterin [3] introduced the concept of Ethereum. Ethereum has extended its capabilities beyond the Bitcoin blockchain with the emergence of smart contracts that enable the development of decentralized applications, which are also known as dApps. The smart contracts provided a consistent platform for the developers to deploy computational logic in the form of computer programs. In addition, Ripple XRP [36] was introduced in 2012 as an alternative to enable cross-border payments such as international remittance. Cardano was invented by Charles Hokinson, who is a co-founder of Ethereum, and the native cryptocurrency is ADA. Cardano provides a layered approach that extends the interoperability and scalability capabilities of similar blockchain platforms in the market. Finally, Polkadot [37] is one of the most distinguishing technologies that enables connectivity of all blockchain platforms in the financial market. Table 3 lists the technical details of leading blockchain platforms for cryptocurrency, including distributed ledger techniques, consensus mechanisms, and smart contracts. Table 4 gives a summary of blockchain platforms in cryptocurrency, including native cryptocurrency names, benefits, and limitations.

C. TECHNICAL OVERVIEW OF BLOCKCHAIN IN TRUST, DATA MANAGEMENT, AND AUTOMATION

Blockchain is a widely used technology in many other domains to establish trust, data management, and automation. Since this survey focuses on the establishment of trust, data management, and automation using blockchain in the financial domain, we have identified that it is important to explore the state of the art in trust establishment, data management, and automation in the other domains.

Blockchain has been used in trust establishment in a wide variety of domains including IoT and healthcare. Shin [38] explains the role of blockchain that develops trust with the decentralized architecture of the distributed ledger. Hammi et al. [39] proposed a decentralized trust mechanism named ''bubbles of trust''. The proposed architecture leverages the identification and authentication of IoT devices while preserving the integrity and availability of data using blockchain. Lockl et al. [40] proposed a blockchain-based IoT sensor data monitoring and logging system that ensures transparency while eliminating the single point of failure to extend trust. Yu et al. [41] proposed ''IoTChain'', by demonstrating the applicability of blockchain by eliminating a trusted third party. The authors highlighted openness and robustness to the denial of services as the important features for trust building in the proposed architecture. Tang et al. [42] proposed an IoT passport, which is a blockchain-based trust framework. In this work, the authors highlighted smart contract-based identity management as a trust enabler. Lin and Liao [43] emphasized the trust establishment of LoRaWAN IoT by leveraging tamper-proof data structures that correspond to IoT. Shala et al. [44] reviewed various trust models for IoT environments by proposing a multi-layer adaptive and trust-based weighting system.

We also identified the significance of blockchain for data management in different domains. Yaqoob et al. [45] discussed the strong potential of blockchain to manage healthcare data with decentralization, transparency, accessibility with enhanced auditability and trust. The authors also emphasized the advantages of blockchain that provide immutability and a tamper-proof environment for healthcare data storage. Chen et al. [46] proposed a personal data management system using blockchain with prototype implementation results. Tian et al. [47] proposed a blockchain-based medical data management service with the incorporation of encryption on ledger data. The experimental evaluation reflected the improvement of privacy, integrity, and availability of medical data. Cheng et al. [48] proposed a novel blockchain architecture to improve public sector data management. The authors have discussed key examples of recent applications of blockchain in the public sector, including Sweden and Estonia. Zaabar et al. [49] proposed Healthblock, which is a decentralized healthcare data-sharing service utilizing blockchain. Truong et al. [50] proposed a GDPR-compliant personal data management solution using blockchain. The authors facilitated a decentralized mechanism for potential service providers and data owners to ensure data provenance and transparency by leveraging the distinguishing features of blockchain technology. The platform enables data owners to enforce data usage consent, which is one of the most important requirements of GDPR from the perspective of user data with audit trails. Kakarlapudi and Mahmoud [51] the potential of blockchain for private data management for sectors such as healthcare. The authors evaluated the prototype using Hyperledger Caliper.

Blockchain is widely used for automation in different sectors. Kassen et al. [52] highlighted the potential of blockchain as a decentralized system for public information processing and management. The authors highlighted the capability of automation in e-healthcare, e-migration, e-city, and e-military with discussions on regulatory issues. Chelladurai and Pandian [53] a novel blockchain-based health record automation system. The authors proposed

TABLE 3. Technical summary of leading blockchain platforms.

Blockchain platform	Distributed ledger	Consensus mechanism	Smart contracts
Bitcoin [2]	Bitcoin uses blockchain-based database	Bitcoin uses Proof of Work consensus mechanism. Proof of Work includes	Smart contracts are not used.
Ethereum [31]	Blockchain-based database is used.	Proof of Work	Solidity programming language is used for programming smart contracts.
RippleXRP	XRP	Ripple Protocol Consensus Algorithm (RPCA) is used in XRP.	Smart contracts are used to facilitate payments.
Cardano	ADA	A Proof of Stake Consensus protocol called Ourberos.	Cardano supports on-chain and off-chain smart contracts.
Polkadot	DOT coin	GRANDPA and BABE (Blind Assignment for Blockchain Extension).	However, para chains which are layer 1 blockchains on Polkadot, are equipped with the functionality to support smart contracts.

TABLE 4. Summary of blockchain platforms in cryptocurrency applications.

Blockchain platform	Native cryptocurrency	Advantages	Limitations
Bitcoin [2]	Bitcoin	No requirement of third party	Transaction approval time is higher
Ethereum [31]	Ether	Can use the operators to launch distributed applications, dApps	Public nature of the ledger incurs security threats for the data.
RippleXRP	XRP	Enables faster settlements. Accepted by a few financial institutions, and	The domination of validators is not aligned with the original concept of decentralization in blockchain
Cardano	ADA	Enables faster settlements. Accepted by a few financial institutions	The domination of validators is not aligned with the original concept of decentralization in blockchain. Polkadot
DOT coin	Provides cross-cryptocurrency support	Still not being accepted by the regulatory bodies.	

to operate smart contracts for patient registration and data sharing with an experimental evaluation. Hamledari and Fischer [54] proposed a novel smart contract-based automation architecture for construction process automation. Chen et al. [55] proposed a novel control transfer mechanism by leveraging smart contracts to automate the control of terminals. Kohen et al. [56] proposed a smart contract-based automation technique for securities trading automation.

III. TRUST COMPONENTS IN FINANCE

Trust in finance is relevant for individuals or entities' confidence and reliance on the credibility, integrity, and transparency of financial systems, institutions, and counterparties. Trust is important in the context of finance as the stakeholders exchange expensive monetary commodities. The modern world has more complex financial exchange scenarios than simple retail purchases from a random vendor on the street. In this section, we investigate the important building blocks of trust in a financial context and how blockchain and smart contracts can be incorporated to strengthen the identified trust elements.

A. FAULT TOLERANCE

The persistent operational capability while the adversaries are present, which is also known as fault tolerance, is one of the most crucial features anticipated in the financial ecosystems. The persistent and reliable operation is important for the stakeholders to construct trust [57]. In the complicated landscape of financial ecosystems, faults that affect the functionality of the financial systems can affect the availability of the system. The origins of such faults can be due to technical issues, cyber-attacks [58], or other unforeseen technical issues, which pose the financial systems with substantial risk that eventually eradicates trust. The significance of fault tolerance lies in its capacity to ensure the persistent continuity of financial operations, mitigating the potential impact of disruptions to the system stakeholders. A fault-tolerant system can recover from faulty scenarios, minimizing downtime [59] and preventing data inconsistencies, thereby minimizing the real impact of the faulty scenarios on external services. For the financial sector, trust is fundamental, and the ability to maintain uninterrupted service is important for preserving confidence among stakeholders, which is important to establish trust.

Blockchain-integrated financial systems are robust to the faulty node presence with their uniquely owned decentralized architecture and consensus mechanisms that ensure the system's resilience to failures. In blockchain-integrated financial systems, each transaction is subject to be verified in the collaborative consensus mechanism and eventually

added to the ledger upon approval of the multiple nodes. This is quite a different and secure approach, and it does not rely on a single centralized authority. Especially, the consensus mechanisms are Byzantine fault tolerant [60], which tolerate the presence of faulty/malicious nodes and maintain the consistent and non-malicious functions of the network while adversaries are present. This decentralized functional architecture of blockchain reduces the risk of a single point of failure that compromises the availability of the service. The network can persistently operate even if some nodes are maliciously attempting to manipulate the transactions. In addition, the existence of services as instances of multiple nodes ensures robustness to the DoS attacks [61].

It is important to identify the insights of fault tolerance using a realistic example. Especially when a permissioned blockchain network is integrated into a consortium of financial entities to enable cross-border payments, which is a potential example in the industry of supply chain [62], [63]. The blockchain is used to track, verify, and execute the relevant steps by the pre-defined process, which has been encoded as smart contracts. If a node responsible for verifying a particular shipment fails due to an adversarial impact or technical issue, other nodes in the network can take over the validation of the transaction, ensuring that the supply chain process persists without disruption. This type of fault tolerance feature is very important for maintaining the efficiency and reliability of supply chain financing functions to operate without any practical challenges. The fault tolerance ensures that the network remains functional and transactions can still be processed securely and efficiently even though adversaries are present, thereby establishing trust.

B. REGULATORY COMPLIANCE

Regulatory compliance is important within the financial ecosystems to ensure economic stability, integrity, and trust in the industry. Financial institutions operate within a complex set of regulations and standards established by governmental bodies and regulatory authorities within the national, international, and regional scopes. Compliance with these regulations is an important component of governance and eventual trust establishment. That is an essential requirement for fulfilling the confidence of investors, protecting consumers, and maintaining the overall consistency of the financial system.

The inherent transparency and consensus-driven trust are the key capabilities of the blockchain to establish trust by strengthening regulatory compliance rather than operating as a consumer unreachable black box. Anti-Money Laundering (AML) [64] regulations are one of the most sensitive regulatory mandates that force financial institutions to monitor and report suspicious transactions to regulatory authorities. EU Anti-Money Laundering Directives are well-known examples that have been implemented to eliminate money laundering and terrorist financing activities [65]. In addition, Financial Crimes Enforcement Network [66], which is a bureau of the U.S. Department of the Treasury, regulates financial transactions to defend from money laundering and other financial crimes committed within the US territory. Blockchain can be integrated as an external service that facilitates AML compliance by adapting the inherent transparent and immutable ledger of transactions while maintaining consumer due diligence [67]. Each transaction recorded on the blockchain contains a cryptographic hash that links it to previous transactions, forming a continuous chain of blocks. This ensures that once a transaction is recorded in the ledger, the record cannot be tampered with or removed which can be maintained as a consistent audit trail for regulators to trace the flow of monetary commodities and identify suspicious activities.

Furthermore, blockchain-based smart contracts are the ideal candidates to streamline the process of sharing sensitive identity information while maintaining personal data privacy. Specifically, regulatory agencies often force financial institutions to exchange customer information for compliance purposes, such as conducting KYC checks. Blockchain-based identity verification systems can securely verify, store, and share customer information across multiple institutions using cryptographic privacy preservation techniques, ensuring that only authorized parties can access the data while in storage and transfer. In addition, the decentralized and consistent ledger ensures data availability across the multiple instances deployed in the collaborative organizations, thereby eliminating rigorous and repetitive consumer onboarding processes. This simplifies the compliance process and also minimizes the risk of data breaches and unauthorized access.

Smart contracts operate as self-executing, transparent, and consistent programs according to the predefined rules encoded on the blockchain that correspond to the compliance procedures for regulatory alignment in real-time smart contracts can enforce the boundaries of international transactions, block payments to suspicious organizations, verify the source of origin of the funds, and automatically flag and report suspicious fund transfers based on predefined regulatory criteria. Automating compliance processes with smart contracts eliminates human errors or biased mispractices by the suspicious to ensure consistent enforcement of regulatory governance across the financial ecosystem.

C. TRUSTED AUTHORIZATION SERVICES

Financial authorization is a key feature of financial ecosystems that function at different scales and across different entities. Therefore, trusted financial authorization services are important to ensure the security of transactions, thereby establishing trust among consumers, enterprises, and state authorities regarding the financial ecosystem. Trusted authorization services facilitate the financial ecosystems with a secured mechanism for verifying the identity, authentication, and payment authorization of individuals or entities engaging in financial activities, thereby mitigating the risk of

TABLE 5. Summary of the trust components of the banking and finance and the applicability of blockchain.

Trust component	Challenge	How blockchain solves the challenge	Key research articles
Fault tolerance	Existence of adversarial participants in the financial ecosystems that affect the integrity and availability of data.	Blockchain provides consensus-driven fault tolerance to preserve service availability and smart contract-driven integrity.	[57], [58], [59], [60], [61], [62], [63]
Regulatory compliance	Enforcing regulatory compliance is challenging due to the implementation difficulties, including the integrity of non-transparent transactions.	The smart contracts ensure unbiased and consistent transaction execution with integrity preservation with the distributed ledger.	[64], [65], [66], [67]
Trusted services	Trust establishment of the services are challenging when the service consumer cannot rely on the integrity of services.	The transparent architecture of smart contracts ensures consumers' transparency by convincing them the service is not malicious.	[68], [69], [70], [71]
Transparency of financial indicators	Financial indicators that must be transparent are subject to potential manipulations and eradicate trust.	Blockchain can be used to indicate the financial indicators and construct trust transparently.	[72], [73], [23], [74]

fraud, prevention of unauthorized access [68], and identity theft [69]. Considering a well-known example, financial institutions utilize trusted third-party authorization services to authenticate customers in real-time during online banking transactions, which comprises transaction routing in different components, including web gateways, SMS servers, and third-party authentication services for financial authorization. Trusted authorization services defend the financial systems as gatekeepers, granting access to the financial services only to authorized parties while safeguarding against malicious actors and unauthorized activities that attempt to break the security.

Blockchain is a prominent technology that facilitates trusted financial authorization by leveraging the inherent decentralized and cryptographic features that advance security, transparency, and reliability that will eventually cultivate trust. Blockchain's decentralized nature replaces the requirement of trust for a central authority to authenticate transactions and authorize access to payment services, reducing the risk of single points of failure. In addition, the PoS-based and Electronic Fund Transfer(EFT) transactions are prone to different risks such as impersonation [70] and Man in the Middle (MiTM) attacks [71].

In particular, smart contracts, which are self-executing and transparent programs with predefined authorization rules, automate and enforce authorization processes with the consensus-driven trust establishment. Smart contracts specify the exact conditions for transaction authorization, such as verifying the identity of participants and checking the customers' account balances while enforcing compliance with regulatory definitions. In addition, blockchain provides an immutable ledger of transaction traces that eliminates the risk of fraudulent activities. For example, in a blockchain-based crowdfunding platform [75], smart contracts automatically authorize the disbursement of funds to project creators once predefined funding goals are met, thereby eliminating the need for intermediaries and enhancing trust in the authorization process.

The key features of blockchain-based smart contracts support trusted authorization in financial systems to ensure reliability and trust in authorization processes.

D. TRANSPARENCY

Transparency is one of the most important expectations in the financial ecosystem, playing a significant role in establishing and sustaining trust among important stakeholders, including customers, regulatory authorities, and financial institutions. In a different scenario where complex transactions are committed, the openness and clarity afforded by a transparent financial system are essential to developing trust. Possible examples are the importation of restricted commodities for commercial purposes, such as certain chemicals that are also usable for terrorist activities. In such scenarios, transparent payments are important considerations in customs clearing procedures. In addition, public investors, regulators, and government bodies strongly rely on accessible and accurate financial information to execute data-driven and well-informed decisions for future investments in the organizational entities. For instance, transparent financial accounting [76] and related reports [73] ensure that companies disclose their financial performance, allowing public investors to assess risks and opportunities to proceed or deny potential investments. Manipulated financial performance indicators expose investors to a massive risk. Therefore, it is one of the most prominent requirements that require transparency [77] to defeat misleading reflections of the financial health insights of the organizations that encourage public investments.

From the perspective of transparency, blockchain has immense potential to improve the financial ecosystems with extended trust. The distributed and transparent ledger especially ensures the recorded events are not modifiable/forgeable to the adversaries, thereby improving trust. Supply chain financing [72] In this article, we identified the significance of transparency, which is not limited to deterring fraudulent activities and unethical behaviors. In addition, transparency cultivates an environment where participants can have confidence in the fairness, reliability, and ethical values of the financial system. Transparency thus emerges as a foundational element for constructing trust in ended trust.

In addition, the transparent service deployment potential that utilizes smart contracts [23] ensures the consumers that the services operate consistently over the decentralized

nodes, thereby eliminating the concerns on trust to the consumers. In addition, smart contracts ensure the flow of financial instruments is transparent, thereby eliminating the potential of corruption [74] and other fraudulent practices.

Table 5 summarizes the trust components in finance while highlighting the technical capabilities of blockchain to cope with identified challenges.

IV. SECURED DATA MANAGEMENT IN FINANCE

The world has transformed towards the information era in the previous decade [78]. Therefore, the data is one of the most important commodities in almost all application contexts. It is important to manage the data lifecycle data management in finance refers to the framework and practices that ensure the proper management, quality, security, and compliance of financial data within an organization. It involves establishing policies, processes, and controls to manage data throughout its lifecycle. This helps maintain data accuracy, integrity, and confidentiality, ensuring that financial information is reliable and can be trusted for decision-making, regulatory compliance, and reporting purposes. Effective data management in finance also involves defining roles and responsibilities, establishing data stewardship, and implementing technologies to support data management. Stewert and Juvenes [79] reflected that data security and consumer trust strongly affect the adoption of fintech systems in Germany. Bose et al. [80] highlighted the significance of data security and trust with a comprehensive comparison of cloud computing and banking applications. Moiso and Minerva [81] presented a user-centric model that enables the data owners to control the gathering, management, and data. The authors proposed a new personal data ecosystem centered around individual data, with a comparable model that a commercial bank manages money, emphasizing challenges and opportunities. Soloway [82] and Covington highlighted the significance of privacy control in the context of financial data sharing.

A. PERSONAL DATA PROTECTION

Personal data protection is an important action in data management within the financial ecosystems. The sensitive personal data includes personal information, bank account details, credit card numbers, and social security numbers. The protection of this data is not limited to legal and ethical obligations with extended requirements for preserving individuals' privacy and preventing identity theft and fraud. For instance, robust data protection measures, such as encryption of the data at rest, data access controls, and secure authentication protocols, are essential to safeguarding sensitive financial information from unauthorized access or breaches. Compliance with stringent data protection regulations, such as GDPR in Europe or the Gramm-Leach-Bliley Act (GLBA) in the United States, highlights the importance of prioritizing personal data protection within the financial industry.

Blockchain and smart contracts are the widely used technologies to enforce personal data protection [83]. Personal data protection includes ensured data availability and personal data access control, which empowers the personal data owner to manage the access of data and guarantee that there is no unauthorized party accessing the data without the consent of the data owner. Especially, the identity data protection using blockchain [84] ensures the robustness against identity thefts in the context of financial ecosystems. In addition, blockchain stores the data in a decentralized form, which exists in the form of multiple instances across each node. When compared with the centralized database-integrated architecture of the banking systems that store the data in the form of single instances, blockchain-based identity data storage is more robust to the attacks that affect the data availability as the blockchain stores data in multiple instances. In addition, the blockchain includes data with inherent integrity preservation. Overall, data integrity and availability are ensured.

B. TRANSACTION DATA PRIVACY

Data privacy [85] holds significant importance in the financial ecosystem for the establishment of trust. In the context of financial processes such as real-time authorizations, individuals and institutions share extremely sensitive personal and financial information. The assurance among the stakeholders that this sensitive data is handled with utmost privacy is essential for maintaining trust in the financial systems. For instance, banking transactions, investment-related information, and personal credit histories contain a significant set of private information that is not supposed to be publicly disclosed. If this private information is compromised, this can lead to significant security threats, such as identity thefts [86], fraudulent activities [87], or unauthorized access to the systems that will affect the data security of the financial ecosystems. In addition, regulatory compliance [88] and adherence to the personal data protection standards become a primary requirement for financial institutions to secure client confidentiality. Therefore, personal data privacy is one of the main expectations in financial systems.

Blockchain has a wide range of technical capabilities to ensure transaction data privacy beyond the state of art financial ecosystems. Especially, Bitcoin [2] provides pseudo-anonymity, which eliminates the disclosure of consumer information with personal details. This ensures the transaction data privacy on payment authorizations without revealing the consumer details that could be used by a curious adversary, either an insider or an external party, to derive insights into the payment details. The Ring signature scheme [89] used in Monero is another one of the most prominent examples in finance that ensures anonymity in transactions. Furthermore, the zCash [90] utilizes BulletProof [91], with shorter and more efficient proofs to approve the transactions without revealing the actual balances of the consumer. Secure multi-party computation [92] provides on-chain decentralized privacy preservation on the transaction authorization

process. The smart contracts that operate as decentralized services for multiparty computation ensure scalability rather than converging the services towards centralized server instances that create a performance bottleneck. These technologies are adaptable to enhance the privacy of financial systems to ensure transaction data privacy beyond the state of the art.

C. TRANSACTION DATA INTEGRITY

Data integrity is an important requirement in financial ecosystems, which plays an indispensable role in data management. In the context of finance, accurate and unaltered data is a mandatory requirement in informed decision-making, financial risk assessment, and alignment with regulatory requirements. It is important to preserve the integrity of financial data, such as the indicators that reflect the insights on the financial performance of the organizations. In addition, transaction data, time information, and payer-payee information are required in scenarios that require deriving evidence for forensic investigations and dispute resolutions. It is important to prevent data manipulations to maintain consistency of the data management systems in the financial sector [93].

Blockchain provides a distributed ledger that stores data in the form of block transactions in chronological order. Each block is connected with a cryptographic link that ensures the blocks and underlying data cannot be manipulated. In banking applications, it is important to preserve the integrity of the data that is associated with the account details and user identity information [94]. In addition, integrity preservation of the transaction data is one of the most important requirements in banking and financial systems [95]. Unlocking the potentials of integrity preservation, and manipulating the data [96] has been formulated as a computationally hard problem in the blockchain. That ensures the blockchain data cannot be manipulated due to the computational expansiveness. In contrast, centralized data storage, such as widely used centralized databases, does not specifically monitor the data storage integrity unless deployed as a separate service. Furthermore, the financial data can be manipulated by a malicious insider who deliberately forges the data on behalf of an adversary, which will lead to manipulated outcomes from the insights. In contrast, integrating the blockchain systems into financial system data management ensures the data is not being forged.

D. DATA ACCESS CONTROL

Data access control is an important requirement in the financial ecosystems. The access control mechanisms distinguish the authorized personnel and services to access the data for either accessing or modifications as defined by the organizational requirements. Accessing the data by unauthorized personnel or services makes the data breaches thereby compromising privacy. It is important to identify, prevent, and respond to unauthorized data access to preserve confidentiality, integrity, and availability. Limitation of data access to entities those who are with legitimate credentials and authorization prevents insider threats and external attacks while adhering to the regulatory compliances and data protection's legal boundaries of data access. Since the banking systems cope with sensitive financial data. Therefore a robust data access control mechanism is essential for financial ecosystems.

In the access control process of financial ecosystems, blockchain has strong capabilities to deliver efficient access control mechanisms using inherent decentralization. The smart contract-based identity management and access control mechanisms [97] provide transparent and immutable access control rules and policies with immutability and consistency. In addition, data access transactions are subject to be approved among the members through consensus mechanisms, thereby the adversarial impacts that deliberately modify the access rights are technically impossible with smart contract-driven access control mechanisms. In addition, data sharing enables enterprises to share access to the data to derive important insights such as credit information [98] in financial applications. Blockchain-based smart contracts enable dynamic data sharing with consistently available data-sharing rules.

E. DATA AVAILABILITY AND RECOVERY

Availability is an important aspect of preliminary security services. Especially, data availability ensures that the data can be accessed in real-time when the services are required to access and proceed with appropriate processing. Especially, when the banking and financial entities rely on data-driven internal decision-making, the availability of data is important. Corrupted or unavailable data hinders the decision-making process. In addition, market analysis and public insights, such as the financial performance of the organizations, must be available for the investors to derive insights into investment decisions. Furthermore, data availability is mandatory for regulatory compliance and auditing procedures. In case the data is lost due to technical failures, appropriate data recovery services must be available.

Blockchain provides a distributed ledger that redundantly stores the data in multiple instances consistently over the members' nodes [99]. The data redundancy in the blockchain is different from the centralized storage services as the blockchain ledger exists in multiple instances rather than a single instance and corresponding disaster recovery nodes in centralized approaches [100]. In addition, blockchain can be customized to enable transparent audit trails when compared with centralized systems. That eliminates the risk of being attacked and the eventual unavailability of data. In addition, a possible data loss that could happen due to hardware failure of a particular ledger instance's server can be easily recovered by replicating the ledger instance from another node as the nodes are consistently holding the distributed ledger across the members. Therefore, blockchain brings up significant advantages of data recovery [101].

TABLE 6. Summary of the data management components of the banking and finance.

Data management component	Challenge	How blockchain solves the challenge	Key surveys and review articles
Personal data protection	It is challenging to preserve the confidentiality, integrity, and availability of personal data from adversaries, including malicious insiders that intend to identity thefts.	Distributed ledger preserves the integrity of the data with cryptographic integrity preservation while ensuring consistent availability across multiple nodes.	[83], [84]
Transaction data privacy	Exposing transaction data, including fund source, destination, and amount lead to a significant security risk.	The smart contracts with appropriate privacy-preservation techniques ensure the transaction data privacy.	[85], [90], [91], [92]
Transaction data integrity	Preserving transaction data integrity is a significant challenge with centralized databases as they can be modified even without the awareness of the data owners.	Cryptographical integrity preserved distributed ledger makes the integrity manipulation a significantly hard computational problem.	[93], [94], [95], [96]
Data access control	Dynamic and transparent access control are challenging due to the computational overheads of access control mechanisms and centralization.	Access control can be performed with smart contracts.	[97], [98]
Data availability and recovery	Data availability due to technical or adversarial attacks.	Recovery is possible with the distributed ledger.	[99], [100], [101]

Table 6 summarizes the data management components in finance while highlighting the technical capabilities of blockchain to cope with identified challenges.

V. AUTOMATION

In this section, we reviewed how the automation features of blockchain can benefit different applications in financial applications. Efficient and real-time operations as well as cost reduction are key anticipations of the automation.

A. AUTOMATED SETTLEMENTS

Automated settlements play a crucial role in the financial ecosystem by streamlining transaction processes, reducing operational costs, and minimizing settlement risks. In traditional finance, settlements often involve manual intervention, multiple intermediaries, and lengthy reconciliation procedures, leading to delays and increased operational inefficiencies. Automating settlements through technology eliminates the need for manual intervention, enabling transactions to be executed and settled automatically based on predefined conditions or smart contracts. This accelerates transaction processing and reduces the risk of errors and discrepancies, enhancing overall efficiency and transparency in financial operations. For example, in securities trading, automated settlements ensure that trades are settled promptly without the need for manual confirmation, reducing settlement times and mitigating counterparty risks. Similarly, in payment processing, automated settlements enable near real-time transfer of funds between parties, improving cash flow management and liquidity. Overall, the adoption of automated settlements in the financial ecosystem offers significant benefits in terms of speed, accuracy, and cost savings, paving the way for a more efficient and resilient financial infrastructure.

Blockchain-based smart contracts, which are integrated into the blockchain [102], provide significant advantages in automating the settlements with improved transparency. Blockchain-based settlement systems [103] ensure automation with improved efficiency for large-scale applications. The consensus-based settlement process improves the security with robustness for the adversarial attempts that deliberately deviate the settlement process from the anticipated workflow. In addition, automated settlements also ensure peer-to-peer operations rather than relying on a centralized payment system. Settlements with blockchain leave immutable traces that ensure non-repudiation during the settlement process.

B. AUTOMATED AUDIT TRAILS

Automated cross-border transactions play a pivotal role in the modern financial ecosystem by facilitating seamless and efficient international payments, trade, and investment. Traditional cross-border transactions are often plagued by complexities, including multiple intermediaries, lengthy settlement times, and high transaction fees. Automating cross-border transactions streamlines the process by leveraging technology to execute and settle transactions swiftly, securely, and cost-effectively. This enhances liquidity management, reduces currency conversion costs, and mitigates settlement risks, thereby enabling businesses to expand their global reach and capitalize on international opportunities. For instance, automated cross-border payments enable e-commerce merchants to accept payments from customers worldwide without the hassle of dealing with multiple currencies and payment processors. Similarly, multinational corporations can efficiently manage their supply chains, payroll, and treasury operations across different countries thanks to automated cross-border transaction capabilities. Overall, the adoption of automated cross-border transactions revolutionizes the way businesses conduct international financial transactions, driving global economic growth and fostering financial inclusion.

Blockchain provides automated audit trails with improved trust and security [104]. Specifically, the conditional definition of the audit actions eliminates the additional operational overhead of manual audit procedures [105]. In addition, automated auditing with smart contracts ensures non-repudiation with the cryptographic integrity-preserved ledger [106]. The most important feature is that the audit reports generated

from the blockchain-based auditing systems are automated, independent, and transparent when compared with the traditional audit methodologies that rely on third parties. Blockchain-based smart contracts ensure the audit procedure is free from human errors [107].

C. AUTOMATED DECISION MAKING

The consumer volume of banking systems is increasing as the world's population grows and more people express interest in onboarding with a bank account. When consumer volume is higher in financial ecosystems, automated decision-making is required to reduce processing time and improve customer response. In the context of finance and banking, autonomous decision-making is widely used in applications such as credit score evaluation in loan processing and credit card issuance. This is important to deliver real-time or near-real-time credit decisions to consumers and eventually improve consumer satisfaction. In addition, applications such as automated decision-making systems for the stock exchange also require automation.

Blockchain-based decision-making ensures transparency and fairness in the process [108], with a strong potential for automated credit scoring [109]. Transparency improves confidence in the acceptance of a particular decision rather than operating as a black-box-type automated system. The immutable ledger record ensures the non-repudiation of decision-making with added audit trails on the ledger.

D. AUTOMATED ACCESS MANAGEMENT

Automated access management is important to facilitate dynamic access control of services. Banking and financial systems exchange sensitive information. In addition, the volume of data and the number of consumers are increasing. Therefore, the automation of data access management is essential to deliver real-time data access management requirements rather than manually managing the access to the data.

Blockchain-based smart contracts ensure autonomous access management of data, including transaction data, user credentials, and so on [110]. The smart contracts can be used to encode the computational logic to manage access [111]. Smart contract-based access management ensures transparency, traceability, and auditability in access management functions of banking applications [97].

Table 7 summarizes the automation components in finance while highlighting the technical capabilities of blockchain to cope with identified challenges.

VI. POSITION OF BLOCKCHAIN-BASED STATE OF THE ART IN TRUST, DATA MANAGEMENT, AND AUTOMATION

In this section, we reflect on the key state of the art for trust establishment, data management, and automation in financial ecosystems. As shown in Figure 3, we evaluated the applications of blockchain and smart contracts in finance and other domains, such as the Internet of Things (IoT), to identify potential strengths to improve the financial domain's applicability in trust, data management, and automation.

1) KNOW YOUR CUSTOMER FOR TRUST ESTABLISHMENT

Customers without clear identification details are restricted in almost all banks in the world. Preliminary information corresponding to a customer, such as names, residential addresses, and contact numbers, is the preliminary information that has been recorded by the banks in a formal customer screening process. If spurious activities committed by the customers or any dispute, either financial or legal, have been identified, this information is important for surveillance and further investigations. Therefore, all banks in every territory must adhere to their own Know Your Customer (KYC) process. In general, KYC processes include paperwork which has proceeded to the storage of digital records. However, the existing KYC procedures have significant challenges in terms of security and practicality. It is challenging to maintain the integrity of the centralized databases as insider attacks will lead to the forgery of customer data included in the databases. In addition, people can conceal customers' identities for criminal activities such as money laundering and illicit trading due to non-standardized consumer verification that only relies on customer data. Furthermore, the customers do not have stronger authority to control the data sharing, which enables the banks to share the data with third parties. From a practical perspective, the KYC process is not a favorable experience for consumers if there are repetitive steps included in the consumer onboarding process. The instanced and independent KYC processes are cumbersome experiences for customers.

In the blockchain-based approach, the incorporation of customer information into smart contracts eliminates awkward manual data entry operations with improved trust. Specifically, the blockchain-based approach ensures data availability, integrity, and data sharing of the KYC data. In addition, malicious manipulations of the data can be traced through the potential transparent audit trails that can be integrated into the distributed ledger. In addition, customers can manage the boundaries of the ownership of data so that banks can control access to data and eliminate misuse of data, which leads to identity theft. The smart contracts can be extended to request permission that specifically defines the scope of data access using transparent policies incorporated through the smart contracts. Distributed data storage eliminates the potential risks of a single point of failure and data loss. The decentralized ledger that incorporates blockchain for data storage ensures the availability of the data and the KYC service with its distributed service architecture. The smart contract-based KYC system can be integrated as a global platform for KYC for banks, with expected improved customer satisfaction.

Ye and Liang [112] emphasized the potential advantages of smart contract transformation for advancing the capabilities of the banking industry. The authors suggested

TABLE 7. Summary of automation components.

Automation component	Challenge	How blockchain solves the challenge	Key surveys and review articles
Automated settlements	Challenges of settlement delays and scalability limitations of centralized systems with a lack of transparency	Smart contract-based transparent systems ensure real-time peer-to-peer settlements.	[102], [103]
Automated audit trails	Automated audit trails eliminate overheads of manual operations of auditing and reduce the overheads.	The role of smart contracts is analyzed and distinguished by the application domains.	[104], [105], [106], [107]
Automated decision making	Automation in decision making is required when transaction volume is high and it is important to convince the criteria for an automated decision to the consumers to ensure acceptance.	Smart contract provides in-built transparency in conditional criteria formulation for decision-making with transparent and immutable records on the ledger.	[108], [109]
Automated access management	Dynamic access management are required when the variety of functions increases in the banking systems, which are robust to the manipulations from adversaries.	Smart contracts ensure robustness to the manipulations of smart contracts.	[110], [111], [97]

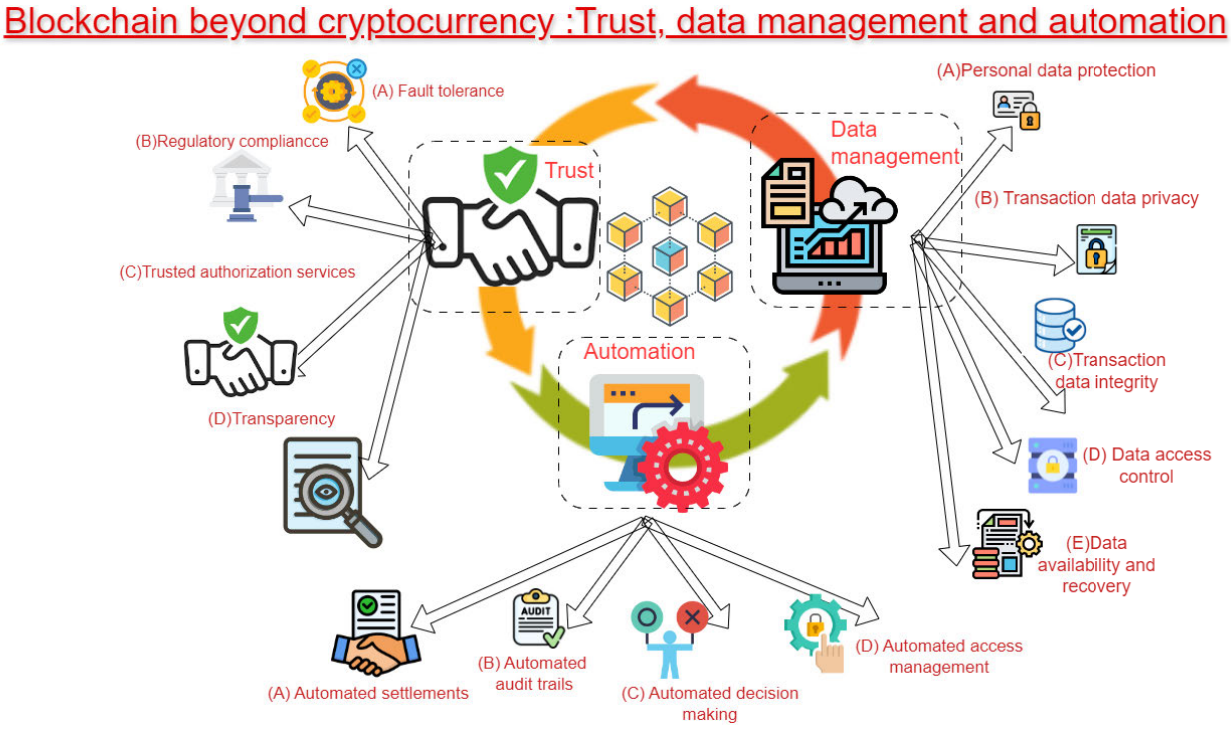


FIGURE 2. Summary of the contribution of blockchain beyond cryptocurrency.

the significance of data encryption for financial institutions to keep a summarized form of data before being shared with the public ledger of blockchain, This process fulfills the trust components by improving the capability to encryption with secured data management. Moyano and Ross [113] proposed a novel blockchain-based system to facilitate the KYC process. The key advancement of the proposed work is the reduction of costs and enhancement of consumer experience, as well as the elimination of repetitive processes on customer onboarding by leveraging the Ethereum blockchain. The authors also emphasized the potential to incorporate permissioned blockchains such as R3 Corda for the system to improve the integration. Alex et al. [114] proposed a privacy-preserving KYC scheme on Ethereum, which leverages customer onboarding with compliance with the regulatory requirements. The system defined two smart contracts, namely KycProvider and KyceToken, which maintain access-related information and function as standard ECR - 20 tokens for the KYC checks.

2) ESCROW SERVICE

Escrow is a widely used electronic payment service for online international trading platforms. Escrow acts as the mediator that governs the fund transfer process that corresponds to the international transaction. International trade transactions are complicated when compared with retail transactions where the consumer and seller are present in proximity. In contrast, the buyers and sellers are physically located in different geographical regions. Therefore, the requirement for a strong intermediary has emerged to authorize the payment transfer upon a certain condition, such as the receipt of goods by the consumer. In centralized escrow services,

it is challenging to cope with an extensive transaction throughput anticipated in production-grade ecosystems when it exists as a single-instanced cloud-based service. In addition, the settlement is not real-time with significant practical challenges in the dispute resolution process. In contrast, the smart contract-based Escrow services enable real-time traceability of the transactions with an in-built audit trail with blockchain integration. Smart contracts ensure real-time peer-to-peer transaction flow, with improved scalability when compared with the state of art centralized systems.

Peters [115] discussed blockchain technology, smart contracts, and their application in global money remittance. The author discussed the potential of blockchain-based multi-signature escrow services leveraging the capabilities of smart contracts. The author has pointed out the significance of smart contracts from the perspective of trust. From the perspective of automation, smart contract-based Escrow executes autonomously and proceeds on the fund transfer between the buyer and seller when the condition has been reached. Bogner et al. [116] emphasized the potential of Ethereum-based decentralized applications for sharing tangible objects in everyday use. The solution implemented associating a web application and a mobile application that is capable of reading a QR code displayed on the objects. The system utilizes an escrow service to hold the associated fees as per the requirement.

3) INSURANCE

Insurance is one of the most essential services that has evolved with various features in the past decades. The people insure different assets such as business properties, conveyance objects, enterprises, and their own lives. Three main components can be identified in the insurance: the insurer, the organization that provides the insurance, and the policy, which is compiled as a paper document. The main drawbacks of the insurance policies compiled in the paper document are the risk of being forged and the possibility of human errors. In addition to that, insurance frauds are accountable for more than 40 billion dollars a year, according to the statistical data published by the Federal Bureau of Investigations. The technical capabilities of blockchain and smart contracts in the insurance industry will be ideal for trust, secured data management, and automation. For example, smart contracts can be utilized to establish insurance policy terms and conditions in a transparent and immutable manner to establish trust. In this function, no human intervention is required to initiate the claim, as claim processing can be handled automatically without human intervention. This process is beneficial in eliminating costs and unnecessary risks, such as manipulative claims of insurance. In addition, the integration of an immutable ledger provides more straightforward, automated, and transparent audit records.

From the literature, we identified that Hans et al. [117] emphasized the strong potential of blockchain-based smart contracts in the context of insurance to speed up claim processing with reduced costs. However, the authors also highlighted that the limitations of several aspects still need to be improved in the smart contracts before integration into the insurance industry. B3i application [118] is another one of the most significant and versatile innovations that targetted the insurance industry in collaboration with fifteen giants in the sector. The smart contract-based systems improve the insure and re-insure value chain as well as improve customer experience in the KYC process. Reference [119] illustrated the improvements in the insurance industry using blockchain-based smart contracts. The authors highlighted the key benefits of the proposed architecture, including enhanced customer satisfaction through a unified KYC process, fraud detection since each claim transaction requires verification by the number of parties to be approved, automation of claim processing, and innovative product integration capabilities such as micro insurance. Guo et al. [120] proposed a distinguishing innovation named WISChain, which was intended for web identity security improvement. WISChain caters to two insurance service models to defend the applications web identity security and commercial website security. WISChain enables autonomous claims when uploading evidence to the blockchain. Bird [121] proposed a novel insurance scheme for the agricultural industry that supports crop insurance for farmers in Ghana. In this application, smart contracts have been defined to compensate policyholders for certain conditions such as drought or rainfall, utilizing high-resolution satellite images to identify weather conditions and eliminate fraudulent claims. Thanks to the smart contracts, the falsified claims can be identified and eliminated in this proposed architecture. In [122], a novel scheme that utilizes blockchain which is named Etherisc has been proposed. Etherisc comprises decentralized smart contracts to facilitate the insurance system with two types of tokens for economic incentivization and to represent risks, respectively. The authors utilized Ethereum smart contracts to establish a standardized set of rules to define how stakeholders should function in the system. Vo et al. [123] presented a permissioned blockchain-based solution for data provenance in car insurance. In this application, the system was implemented using the Hyperledger Fabric blockchain platform. The smart contracts were invoked to capture events such as weather events, location variations of the car, and so on.

4) LENDING AND BORROWING

Lending, borrowing, and loans are significant economic activities of a civilized nation that are important in economic development. The economic development sophisticated human needs and lending also diversified along different avenues. Peer-to-peer lending, which was a famous activity in the past was transformed into flexible syndicated products presented by major financial institutions. Banks act as the trusted third parties. The banks are the only authorized repository of money for lending and dominate the lending market. The current mortgage and loan processing often spans about 60 days. This arduous process includes

ascertaining loan applicants' credit scoring, underwriters' profile verification, and so on. In addition to that, the loans were subject to processing fees and a few other surcharges imposed by the banks. Some hidden charges surprise the customers too. Borrowers sometimes escape and refuse to pay back the loan. The smart contracts circumvent the existing issues and promise a trust-based ecosystem that streamlines the application and payment with automatic execution.

Salt Lending [124] is the world's one of the largest lending platforms, with a market capital of USD 126 million. The borrowers automatically send collateral to Salt's multi-signature wallet according to enforced conditions. EthLend [125] is an Ethereum-based lending platform. Important attributes, such as loan terms, fund transferring conditions, and collateral, are handled by smart contracts with ERC-20 tokens. Everex [126] is a Singapore-based lending and remittance service. Everex provides a transparent platform for unbanked customers in Southeast Asian countries. It uses ERC-20 tokens which can be pegged with fiat currencies. Debitium [127] is one of the Ethereum-based crowdfunding platforms. It facilitates cross-border deals and connects borrowers and investors.

5) AUTOMATED AUDITING PROCEDURES

Auditing procedures are one of the most important requirements in the organizations. Auditing ensures the reliability and accuracy of the financial statements that reflect the financial performance of the organization. In addition, auditing procedures are important to the fraudulent activities of the organizations and eventually safeguard the assets of the organization. In general, the regulatory requirements recommend that auditing has to be performed by trusted independent third-party organizations. The auditing procedure is a formal and tedious human-intervented process that is expensive to organizations. In addition, the derived auditing insights are subject to human errors as well. In contrast, smart contract-based audit procedures ensure autonomous auditing and traceability procedures with a significant reduction of human intervention. In addition, smart contracts guarantee with autonomous execution of smart contracts in real-time. The inherent distributed and transparent nature of the smart contracts ensures the regulatory authorities can transparently view the audit insights without the risk of malicious manipulations.

Zou et al. [128] highlighted the significance of smart contract-based audit schemes that resist the manipulations of audit records. This work reflects the strengths of blockchain in ensuring integrity while bringing up the advantages of automation. Rozario et al. [129] explained the strength of smart contracts to automate auditing procedures. Still, significant opportunities exist in the context of auditing procedures to be leveraged by smart contracts.

6) AUTOMATED STOCK TRADING SERVICE

Stock trading is one of the highly dynamic and real-time trading processes that consists of multiple real-time operations, including trading platform management, investments, brokering, financial indicator identifications, and so on. The stock markets are in the millions of dollars of Volume within a wide range of individual investors to multi-millionaire conglomerates. Each stock exchange transaction is committed with the active contribution of different parties, such as brokers, investors, and stock sellers. Significant limitations can be identified in the manual stock exchange functions, including human errors and efficiency limitations. In addition, trusted third-party-based systems emerge performance bottlenecks. In contrast, the blockchain-based approaches eliminate the centralized processing architecture by incorporating smart contracts. The blockchain-based stock exchange emerges as a decentralized platform for stock trading that enables peer-to-peer transactions for all parties without relying on a trusted third party. The automated smart contracts ensure the conditional execution of stock trading transactions without human errors and improve transparency.

Yermack [130] emphasized the significant advantages of blockchain-based smart contracts with an elaboration on the benefits of financial asset trading. The author highlighted the key advantages of automation and the advantages of tracking asset ownership to improve liquidity and transparency. The author has also shed some light on the ongoing initiatives of the USA and Australia for blockchain-enabled stock trading. Reference [131] is a whitepaper that presents TITA, which is an Ethereum-based system for commodity trading in manufacturers and consumers. The system elaborates with a crypto-token to enable purchases and transfers while incentivizing stakeholders as a gesture of appreciation. In this work, the smart contracts transfer assets or establish escrow conditions as required. In Australia, [132] is a well-known application of permissioned blockchain-based smart contracts to enable stock trading in Australia. The proposed system enables automated clearing and settlement by smart contracts while supporting post-trade activities with the invention of a unique Digital Asset Modeling Language (DAML) and run privately on a defined set of nodes. References [133] and [134] in Hong Kong followed the Australian Stock Exchange implementation which was discussed above.

Table 8 summarizes the significant blockchain-based applications in finance and its relevance to the identified components in trust, data management, and automation. The different applications have more bias towards each trust, data management, and automation. However, blockchain operates as a global enabler with its distinguishing technical capabilities to facilitate more robust and efficient ecosystems for finance with advanced trust, data management, and finance with a envision toward profitability.

VII. WAY FORWARD TOWARDS BLOCKCHAIN-BASED TRUST, DATA MANAGEMENT, AND AUTOMATION IN FINANCIAL APPLICATIONS

This section reflects insights into blockchain-based trust, data management, and automation for financial applications.

TABLE 8. Summary of blockchain-based applications in finance and the position of blockchain's capabilities.

Application	Key related works	Trust				Data management					Automation			
		Fault tolerance	Regulatory compliance	Trusted authorization services	Transparency	Personal data protection	Transaction data privacy	Data integrity	Data access control	Data availability and recovery	Automated settlements	Automated audit trails	Automated decision making	Automated access management
Know Your Customer	[112], [113], [114]		✓	✓	✓	✓		✓	✓	✓				✓
Escrow service	[115], [116]	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Insurance	[117], [118], [119], [120], [121], [122], [123]		✓	✓	✓	✓			✓	✓	✓	✓	✓	
Lending and borrowing	[124], [125], [126], [127]	✓	✓	✓						✓	✓	✓	✓	
Automated auditing	[128], [129]	✓	✓	✓	✓							✓	✓	
Automated stock exchange	[130], [131], [132], [133], [134]	✓	✓	✓	✓		✓	✓		✓		✓	✓	

We propose a novel blockchain integration architecture and highlight the strengths of blockchain-based financial applications in these areas.

A. POSSIBLE INTEGRATION ARCHITECTURE

Since blockchain adoption in cryptocurrency is challenging, it is important to identify the possible integration architecture for the proposed services. In this article, we investigated the potential integration architecture of the blockchain in the financial application context. In this application, we proposed the integration of a multi-level hierarchical blockchain that enables international collaboration.

Possible approaches have been defined as follows. In this work, we propose a possible integration architecture for blockchain as a decentralized service for financial applications as indicated in Figure 3. The main Components of the proposed architecture are as follows.

In this proposed service architecture, we propose a multi-layered architecture for trust establishment, data management, and automation. We also propose a two-layered blockchain integration architecture for deploying the services. Finally, we propose to incorporate a consortium-type blockchain deployment setup. The key objective of the consortium-type blockchain instead of the public blockchain is limiting information access to a selected set of consumers and organizations instead of making the data available on a public ledger. The main components of the proposed architecture are as follows.

1) NATIONAL BLOCKCHAIN SERVICE LAYER (LAYER 1)

We propose to incorporate a national blockchain service that consists of a consortium of national banks and other financial institutions, such as the local tax authority. The key objective of this architecture is to enable seamless access for data sharing and secured data management. The blockchain service is connected to the blockchain network that comprises central banks of layer 2.

2) INTERNATIONAL BLOCKCHAIN SERVICE LAYER (LAYER 2)

As proposed in our work, the Layer 2 blockchain consortium incorporates the national central banks as members of the consortium. This architecture improves cross-border collaboration for international transactions and information sharing.

3) NATIONAL LEVEL INFORMATION SHARING SERVICES

National-level information-sharing services include collaboration between national authorities such as local tax offices, banks, and other regulatory authorities. In this proposed architecture, smart contracts can be utilized to dynamically manage access and eventually establish trust with automation.

4) INTERNATIONAL LEVEL INFORMATION SHARING SERVICES

International-level information-sharing services are important to enable cross-border trust establishment, data management, and automation. This is important to people

TABLE 9. Position of blockchain-based applications and regulatory bodies.

Regulation	Section	Description	Distributed ledger				Conseneus			Smart contracts					
			Detailed payment logs	Transparency on personal data processing	Tracking the access of data	Data sharing requirements	Global access control policy	Identification and authentication of users	Identification of suspicious activities	Automation in the compliance audit	Secure coding architecture	Automated data access management	Automated incident response	Automated data sharing response	Efficient data confidentiality enforcement
GDPR	Article 5	Principles relating to the processing of personal data		✓	✓	✓		✓	✓		✓				
	Article 6	Lawfulness of processing	✓	✓		✓	✓	✓	✓		✓		✓		✓
	Article 9	Processing of special categories of personal data		✓		✓	✓				✓	✓		✓	
	Article 25	Data protection by design and by default		✓	✓	✓	✓		✓	✓	✓	✓	✓		✓
	Article 32	Security of processing	✓	✓		✓		✓	✓			✓	✓	✓	
	Article 35	Data protection impact assessment (DPIA)		✓	✓	✓	✓	✓	✓				✓		✓
	Article 37	Designation of the data protection officer (DPO)		✓	✓	✓	✓	✓			✓	✓			
PCI-DSS	Requirement 3	Protect stored cardholder data	✓	✓	✓	✓	✓								
	Requirement 7	Restrict access to cardholder data by business need-to-know	✓	✓	✓		✓			✓	✓		✓		✓
	Requirement 8	Identify and authenticate access to system components	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓
	Requirement 10	Track and monitor all access to network resources and cardholder data	✓	✓	✓	✓	✓	✓							
	Requirement 12	Maintain a policy that addresses information security for all personnel	✓	✓	✓	✓	✓		✓	✓	✓				✓

who are migrating from one country to another, especially when the destination country requires them to enquire about their credit history or even blacklists. International-level information sharing enhances dynamic and global credit scoring mechanisms as well as insurance schemes to eliminate fraudulent practices. This is important to establish law and order to restrict unauthorized money flows and is eventually important for national and international security.

5) CONSUMER APPLICATIONS

The proposed architecture ensures more integration capabilities with third-party services with robust access control. More convenient consumer application integration ensures convenience and improved user experience for the people who use the financial applications with advanced trust which has been achieved by blockchain-based smart contracts.

B. POSITION OF THE REGULATORY COMPLIANCE

GDPR is a data protection law enacted in 2018. It defines the rules and regulations to enforce data protection in Europe. Especially in banking and finance, GDPR defines standards for personal data protection. In this context, we point out a few significant potentials of blockchain to achieve GDPR compliance.

In GDPR, Article 5 is entitled "Principles relating to the processing of personal data," which defines requirements

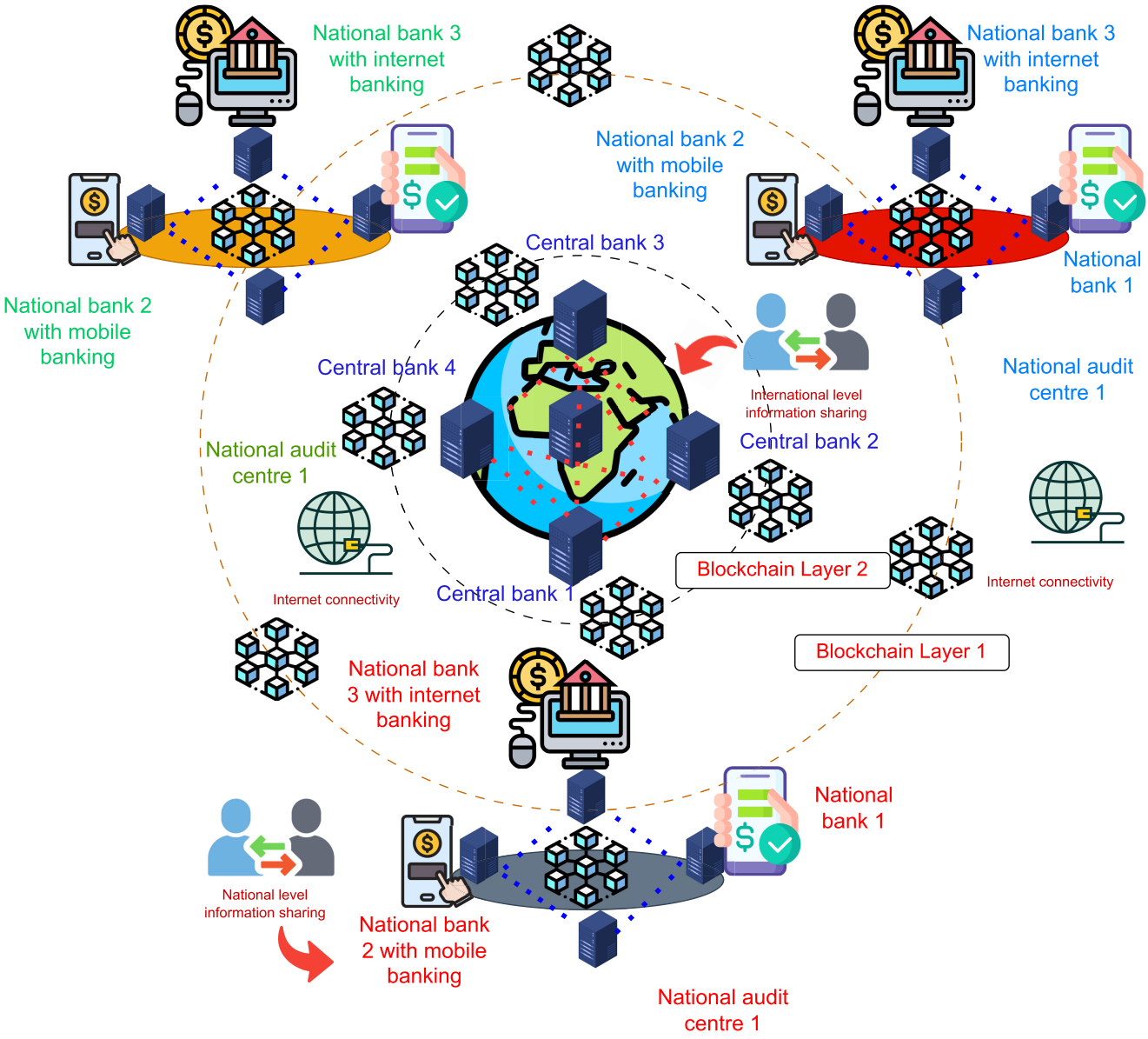


FIGURE 3. Integration architecture.

for data security and confidentiality. This article emphasizes the lawfulness, fairness, and transparency of personal data. Blockchain-based applications in finance especially improve transparency and fairness, which eventually construct trust in financial ecosystems from the perspective of personal data management. The transparent architecture of smart contracts ensures that fairness and transparency expectations are reached in financial applications that involve personal data, such as KYC, as explained in Section VI-1. GDPR Articles 12, 13, and 14 elaborate further on the context of personal data. The capabilities of blockchain ideally leverage the requirements of transparency and fairness in Articles 5, 12, 13, and 14.

Article 6 defines the regulatory conditions for the consent. In addition, Articles 7 and 8 elaborate on the conditions of the consent. Especially in Article 7, which specifically defines the right to withdraw data. The practical challenges and technical difficulties of dynamic consent management hinder the adaptability of banking and financial systems to the GDPR. It is important to identify that blockchain and smart contracts have stronger technical capabilities to incorporate consent management to deliver dynamic functionality, which is more suitable for banking systems.

Article 5 and Article 24 of GDPR are entitled "Principles relating to the processing of personal data." These articles highlight accountability for personal data.

PCI DSS is a widely known specification in the context of finance that defines the data security standards to manage the lifecycle of credit card information. PCI-DSS compliance is required for the transmission, storage, and verification requests of credit card-related transactions. Especially Requirement 3 of PCI-DSS defines the requirements for secure storage, transmission, and processing of cardholder data. Stronger access control mechanisms and encryption mechanisms are the proposed measures to defend financial systems from potential data breaches. In this context, blockchain provides stronger capabilities to enforce stronger access control mechanisms with smart contract-driven improved transparency and efficiency. The smart contracts enable dynamic access control with decentralized services to operate efficiently in securing the card payment transaction-related data.

Table 9 summarizes the relevance of different articles of each regulatory requirement. Blockchain provides a more robust technical enabler for establishing regulatory systems that function technically and reduce the gap between regulatory requirements and implementations.

C. OPEN CHALLENGES AND OVERVIEW OF POTENTIAL SOLUTIONS

The blockchain system incorporates decentralized storage, smart contract services, and extra operational overheads for integrated applications. It is important to identify the limitations before adapting the financial systems. Especially the consistency, availability, and partition tolerance, known as CAP trilemma, emphasize the boundaries of blockchain systems.

1) STORAGE EXPANSION DUE TO LEDGER GROWTH

Blockchain storage expansion is one of the most vital challenges in the blockchain. Bitcoin is one of the most known blockchain-based applications in finance [2]. Bitcoin ledger expands to Giga Bytes with the growth of the storage. However, the storage expansion incurs significant overheads to the stakeholders. For example, hosting the database on cloud storage is expensive for business operators. Technically, it is important to preserve the ledger storage to align with the principles. Therefore, deletion or purging of the previous transactions/blocks violates the preliminary principles of blockchain.

Several approaches are investigated to cope with the blockchain storage scalability problem. Improved storage utilization for the block is one particular approach [135] which has been proposed along with a partitioning technique with lower complexity in storage. In addition, Rupasena et al. [136] explained the potential of off-chain storage integration to improve ledger storage.

2) INEFFICIENT CONSENSUS MECHANISMS

Consensus mechanism is one of the core components of blockchain. Consensus defines the utmost condition for block mining. The efficiency of the blockchain consensus is always being questioned to evaluate the applicability of blockchain to specific applications. Especially, the Proof of Work consensus and its extensive energy consumption [137] in Bitcoin [2] makes the adaptability as a currency with global acceptance compromises the environmental sustainability. The energy consumption of the blockchain increases the electricity consumption [138] and eventually affects the profitability of blockchain ecosystem operators. In addition, the extensive bandwidth overheads of proof-based consensus mechanisms affect the efficiency.

Energy-efficient consensus mechanisms are one of the most vibrant research topics. Especially, the energy efficient [139] consensus has been designed for power-restricted infrastructure such as IoT devices [140]. Rather than energy efficiency, bandwidth efficiency is also a wide consideration. For example, the BulletProof [91] protocol has been introduced for the Monero blockchain to provide shorter proofs in the consensus. It is important to design consensus mechanisms with improved efficiency to improve the adaptability of blockchain to banking applications.

3) INTEROPERABILITY

The infrastructure, services, and applications in the banking and financial ecosystems have evolved for decades. The innovations that leverage blockchain-based smart contracts require interoperability among the existing financial ecosystems to ensure seamless integration capability. However, interoperability challenges are significant limitations that hinder the adaptability of blockchain-based financial applications into the currently operating financial systems [141]. Since the regulatory bodies strongly govern the financial applications [142] the decentralized and publicly contributed nature of blockchain makes the adoption of blockchain challenging as the decentralization properties of blockchain are contradictory from the centralized applications that require governance of the statutory regulations.

However, interoperability can be improved by adapting interoperability standards such as ISO 8583 [143] which are dedicated to payment applications. In addition, the security standards ISO 27001 [144] can be implemented with smart contracts to ensure interoperability with improved transparency.

4) EVOLUTION OF QUANTUM COMPUTING

Quantum computing infrastructure has evolved in the past few years significantly with extensive computational capabilities. However, the evolution of quantum computing exposes the current cryptographic systems to huge risks. Especially, Quantum computers reduce the computational hardness of cryptographic problems, thereby emerging a set of consequences that affect the fundamental security properties of blockchain [145]. More specifically, the computationally hard problems that define the boundaries of mining can be compromised using quantum computers [146]. Such

consequences may end up in transferring the mining authority to the parties who own quantum computing power that will eventually end up with the 51% attack [147]. In addition, the cryptographic functions that have been utilized for data encryption, integrity preservation, and authentication are no longer secure if the underlying cryptographic problems can be resolved using the quantum computer.

Even though Quantum computing emerged with different innovations, the research is still in progress to investigate quantum-safe cryptographic algorithms [148]. Quantum-safe blockchain systems incorporate cryptographic algorithms [149] which are safe from quantum attacks. However, it is important to consider the safety of Quantum attacks while designing consensus mechanisms and blockchain applications.

D. FUTURE WORK

In this subsection, we shed light on the potential future work in finance with emerging research topics and their applicability of the blockchain for advancement.

1) BLOCKCHAIN FOR SECURED MACHINE LEARNING IN FINANCE

ML is widely incorporated in financial applications. AI is especially vulnerable to data poisoning and biasing attacks that will lead to improper decisions. This will eventually eradicate consumers' trust in financial services. In addition, smart contracts and distributed ledgers can be used to improve the security of training data with different applications such as data sharing [150]. Furthermore, blockchain-based smart contracts can be used to incorporate robust access control mechanisms to the machine learning data [151].

Blockchain provides transparency and immutability in machine learning applications [152]. In addition, blockchain provides trusted execution through smart contracts.

2) EXPLAINABLE AI(XAI)-BASED TRUST ESTABLISHMENT IN FINANCE

Explainable AI is one of the most prominent AI variants in future applications. XAI, in particular, provides insights into AI-based decisions rather than functioning AI-based applications as black boxes [153]. This is important when the AI is applied to automate the credit decisions. XAI provides explanations for AI-based decisions. This is important to the customers to convince of the AI-based decisions on credit evaluation [154].

Blockchain-based smart contracts provide transparency in smart contract execution [155]. The smart contracts are especially aligned with the transparency by design principle of XAI. This is important to improve customers' confidence in XAI-based decisions. In addition, previous decisions

3) FEDERATED LEARNING WITH BLOCKCHAIN IN FINANCE

Federated Learning(FL) is one of the most renowned decentralized learning mechanisms that enable decentralized machine learning. Federated learning is advantageous in several aspects when compared with the centralized machine learning techniques as FL trains locally and shares the model updates to the centralized server, instead of sharing the data. This is beneficial to improve the scalability of the overall system as the training computational overhead is decentralized across multiple nodes. However, FL suffers from significant challenges in trust establishment as the local workers can deliberately bias the training data.

Blockchain-based smart contracts are ideal for establishing trust in the federated learning [156]. It is challenging to identify the model updates and malicious manipulations and blockchain-based consensus provides a decentralized approval process to ensure more robust federated learning with improved trust [157]. The distributed nature of blockchain is compatible with deploying the local workers as blockchain nodes and global aggregation through a consensus mechanism.

VIII. CONCLUSION

This paper starts by providing an overview of blockchain's technical features and reviewing its core components, including smart contracts, consensus mechanisms, and widely used applications in cryptocurrency. We have highlighted the strong capabilities of blockchain and smart contracts for trust, data management, and automation in the financial application domain. We reviewed related works and pointed out how blockchain is a distinguishing enabler for trust, data management, and automation, along with six prominent application avenues in the financial ecosystem. In addition, we proposed a two-layered blockchain architecture, which is envisioned towards the development of a global decentralized platform for seamless cross-border facilitation of trust, data management, and automation in financial applications. In addition, we highlighted the position of blockchain in enforcing regulatory requirements that apply to financial applications through its unique technical capabilities. We highlighted the potential of blockchain for emerging and related topics in finance, including machine learning and explainable artificial intelligence. Our work sums up the strong potential of blockchain to advance financial systems with security for the improvement of trust and efficiency in data management as well as automation.

REFERENCES

[1] E. V. Murphy, M. M. Murphy, and M. V. Seitzinger, "Bitcoin: Questions, answers, and analysis of legal issues," in *Proc. Library Congr., Congressional Res. Service*, 2015, pp. 1–32.

[2] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[3] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, p. 37, 2014.

[4] R. B. Adams, "Trust in finance: Values matter," *J. Japanese Int. Economies*, vol. 60, Jun. 2021, Art. no. 101123.

[5] M. A. Al-Hawari, "The role of bank automated services in gaining customers' trust: A practical study in UAE," *Jurnal Pengurusan*, vol. 33, pp. 45–52, Dec. 2011.

[6] A. Miremadi, S. Ghalamakri, and A. Ramezani, "Challenges in trust and security by implementation of e-CRM among banks and financial institution: A case study of e-banking in Iran," *Int. J. Inf. Sci. Manage.*, vol. 10, pp. 99–118, Jul. 2012.
[7] O. Borgogno and G. Colangelo, "Consumer inertia and competition-sensitive data governance: The case of open banking," *J. Eur. Consum. Market Law*, vol. 9, no. 4, pp. 143–150, 2020.
[8] T. Butler and L. O'Brien, "Understanding regtech for digital regulatory compliance," in *Disrupting Finance: FinTech and Strategy in the 21st Century*. Cham, Switzerland: Springer, 2019, pp. 85–102.
[9] G. Dorfleitner, L. Hornuf, and J. Kreppmeier, "Promise not fulfilled: FinTech, data privacy, and the GDPR," *Electron. Markets*, vol. 33, no. 1, p. 33, Dec. 2023.
[10] L.-D. Ibáñez, K. O'Hara, and E. Simperl, "On blockchains and the general data protection regulation," EU Blockchain Forum Observatory, Brussels, Belgium, Project Rep. 422879, 2018. [Online]. Available: http://eprints.soton.ac.uk/id/eprint/422879
[11] M. Kunwar, "Artificial intelligence in finance: Understanding how automation and machine learning is transforming the financial industry," Ph.D. thesis, Centria Univ. Appl. Sci., Finland, 2019. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/227560/Manju%20Kunwar%20Thesis.pdf?sequence=2
[12] A. Rijanto, "Blockchain technology adoption in supply chain finance," *J. Theor. Appl. Electron. Commerce Res.*, vol. 16, no. 7, pp. 3078–3098, Nov. 2021.
[13] J. Kondabagil, *Risk Management in Electronic Banking: Concepts and Best Practices*, vol. 454. Hoboken, NJ, USA: Wiley, 2007.
[14] C. Lewis and S. Young, "Fad or future? Automated analysis of financial text and its implications for corporate reporting," *Accounting Bus. Res.*, vol. 49, no. 5, pp. 587–615, Jul. 2019.
[15] P. Saha, I. Bose, and A. Mahanti, "A knowledge based scheme for risk assessment in loan processing by banks," *Decis. Support Syst.*, vol. 84, pp. 78–88, Apr. 2016.
[16] G. Merlonghi, "Fighting financial crime in the age of electronic money: Opportunities and limitations," *J. Money Laundering Control*, vol. 13, no. 3, pp. 202–214, Jul. 2010.
[17] J. A. Jaoude and R. G. Saade, "Blockchain applications–usage in different domains," *IEEE Access*, vol. 7, pp. 45360–45381, 2019.
[18] 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.
[19] Y. Zhang, Z. Wang, J. Deng, Z. Gong, I. Flood, and Y. Wang, "Framework for a blockchain-based infrastructure project financing system," *IEEE Access*, vol. 9, pp. 141555–141570, 2021.
[20] T. A. Almeshal and A. A. Alhogail, "Blockchain for businesses: A scoping review of suitability evaluations frameworks," *IEEE Access*, vol. 9, pp. 155425–155442, 2021.
[21] L. Zhang, Y. Xie, Y. Zheng, W. Xue, X. Zheng, and X. Xu, "The challenges and countermeasures of blockchain in finance and economics," *Syst. Res. Behav. Sci.*, vol. 37, no. 4, pp. 691–698, Jul. 2020.
[22] Q. K. Nguyen, "Blockchain—A financial technology for future sustainable development," in *Proc. 3rd Int. Conf. Green Technol. Sustain. Develop. (GTSD)*, Nov. 2016, pp. 51–54.
[23] F. Schär, "Decentralized finance: On blockchain-and smart contract-based financial markets," *Federal Reserve Bank St. Louis*, vol. 103, no. 2, pp. 153–174, 2021.
[24] T. Yu, Z. Lin, and Q. Tang, "Blockchain: The introduction and its application in financial accounting," *J. Corporate Accounting Finance*, vol. 29, no. 4, pp. 37–47, Oct. 2018.
[25] R. Patel, M. Migliavacca, and M. E. Oriani, "Blockchain in banking and finance: A bibliometric review," *Res. Int. Bus. Finance*, vol. 62, Dec. 2022, Art. no. 101718.
[26] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees," *Technological Forecasting Social Change*, vol. 158, Sep. 2020, Art. no. 120166.
[27] B. Sriman and S. G. Kumar, "Decentralized finance (DeFi): The future of finance and defi application for Ethereum blockchain based finance market," in *Proc. Int. Conf. Adv. Comput., Commun. Appl. Informat. (ACCAI)*, Jan. 2022, pp. 1–9.
[28] Y. Tian, Z. Lu, P. Adriaens, R. E. Minchin, A. Caithness, and J. Woo, "Finance infrastructure through blockchain-based tokenization," *Frontiers Eng. Manage.*, vol. 7, no. 4, pp. 485–499, Dec. 2020.
[29] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manage.*, vol. 3, no. 4, Dec. 2018, Art. no. 1850015.
[30] S. Thakur and V. Kulkarni, "Blockchain and its applications—A detailed survey," *Int. J. Comput. Appl.*, vol. 180, no. 3, pp. 29–35, Dec. 2017.
[31] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum, Zug, Switzerland, White Paper 705168a, 2014, vol. 151, pp. 1–32.
[32] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, and Y. Manevich, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.
[33] E. Bandara, W. K. Ng, K. De Zoysa, N. Fernando, S. Tharaka, P. Maurakirinathan, and N. Jayasuriya, "Mystiko—Blockchain meets big data," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 3024–3032.
[34] H. Fabric. (2018). *Hyperledger Fabric*. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/07/
[35] N. Szabo, "Smart contracts: Building blocks for digital markets," *EXTROPY, J. Transhumanist Thought 16*, vol. 18, no. 2, p. 28, 1996.
[36] M. L. Perugini, "Monete digitali alternative: Ripple (altcoins: Ripple)," *SSRN 2665756*, pp. 1–10, Feb. 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2665756, doi: 10.2139/ssrn.2665756.
[37] G. Wood, "POLKADOT: Vision for a heterogeneous multi-chain framework," *White Paper*, vol. 21, no. 2327, p. 4662, 2016.
[38] D. D. H. Shin, "Blockchain: The emerging technology of digital trust," *Telematics Informat.*, vol. 45, Dec. 2019, Art. no. 101278.
[39] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018.
[40] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1256–1270, Nov. 2020.
[41] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 12–23, Jul. 2018.
[42] B. Tang, H. Kang, J. Fan, Q. Li, and R. Sandhu, "IoT passport: A blockchain-based trust framework for collaborative Internet-of-Things," in *Proc. 24th ACM Symp. Access Control Models Technol.*, 2019, pp. 83–92.
[43] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *IJ Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.
[44] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Blockchain and trust for secure, end-user-based and decentralized IoT service provision," *IEEE Access*, vol. 8, pp. 119961–119979, 2020.
[45] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, vol. 34, no. 14, pp. 11475–11490, Jul. 2022.
[46] J. Chen, Z. Lv, and H. Song, "Design of personnel big data management system based on blockchain," *Future Gener. Comput. Syst.*, vol. 101, pp. 1122–1129, Dec. 2019.
[47] H. Tian, J. He, and Y. Ding, "Medical data management on blockchain with privacy," *J. Med. Syst.*, vol. 43, no. 2, pp. 1–6, Feb. 2019.
[48] S. Cheng, M. Daub, A. Domeyer, and M. Lundquvist, "Using blockchain to improve data management in the public sector," Mckinsey Digit., New York, NY, USA, Tech. Rep., 2017.
[49] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Comput. Netw.*, vol. 200, Dec. 2021, Art. no. 108500.
[50] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A blockchain-based solution," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1746–1761, 2020.
[51] P. V. Kakarlapudi and Q. H. Mahmoud, "Design and development of a blockchain-based system for private data management," *Electronics*, vol. 10, no. 24, p. 3131, Dec. 2021.
[52] M. Kassen, "Blockchain and e-government innovation: Automation of public information processes," *Inf. Syst.*, vol. 103, Jan. 2022, Art. no. 101862.
[53] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 1, pp. 693–703, Jan. 2022.
[54] H. Hamledari and M. Fischer, "Construction payment automation using blockchain-enabled smart contracts and robotic reality capture technologies," *Autom. Construction*, vol. 132, Dec. 2021, Art. no. 103926.

[55] J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A. K. Bashir, and R. Nawaz, "Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4478–4488, Jul. 2020.

[56] R. Cohen, P. Smith, V. Arulchandran, and A. Sehra, "Automation and blockchain in securities issuances," *Butterworths J. Int. Banking Financial Law*, vol. 33, pp. 144–150, Mar. 2018.

[57] F. B. Schneider and L. Zhou, "Distributed trust: Supporting fault-tolerance and attack-tolerance," Cornell Univ., Ithaca, NY, USA, Tech. Rep. 2004-1924, 2004.

[58] O. Gulyás and G. Kiss, "Impact of cyber-attacks on the financial institutions," *Proc. Comput. Sci.*, vol. 219, pp. 84–90, 2023.

[59] D. Trabay, A. Asem, I. El-Henawy, and W. Gharibi, "A hybrid technique for evaluating the trust of cloud services," *Int. J. Inf. Technol.*, vol. 13, no. 2, pp. 687–695, Apr. 2021.

[60] N. Zivic, C. Ruland, and O. Ur-Rehman, "Addressing Byzantine fault tolerance in blockchain technology," in *Proc. 8th Int. Conf. Model. Simul. Appl. Optim. (ICMSAO)*, Apr. 2019, pp. 1–5.

[61] D. A. Bamrara, G. Singh, and M. Bhatt, "Cyber attacks and defense strategies in India: An empirical assessment of banking sector," *Int. J. Cyber Criminol.*, vol. 7, no. 1, pp. 49–61, Jun. 2013. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2488413

[62] P. V. R. P. Raj, S. K. Jauhar, M. Ramkumar, and S. Pratap, "Procurement, traceability and advance cash credit payment transactions in supply chain using blockchain smart contracts," *Comput. Ind. Eng.*, vol. 167, May 2022, Art. no. 108038.

[63] M. Du, Q. Chen, J. Xiao, H. Yang, and X. Ma, "Supply chain finance innovation using blockchain," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1045–1058, Nov. 2020.

[64] H. Kang, H. R. Kim, and S.-p. Hong, "A study on the design of smart contracts mechanism based on the blockchain for anti-money laundering," *J. Internet Comput. Services*, vol. 19, no. 5, pp. 1–11, 2018.

[65] J. Böszörmenyi and E. Schweighofer, "A review of tools to comply with the fourth EU anti-money laundering directive," *Int. Rev. Law, Comput. Technol.*, vol. 29, no. 1, pp. 63–77, Jan. 2015.

[66] *Regulatory Efficiency and Effectiveness*, Financial Crimes Enforcement Netw., Vienna, VA, USA, 2007. [Online]. Available: https://www.fincen.gov/regulatory-efficiency-and-effectiveness and https://perma.cc/H7MNPEUZ

[67] C. Xu, C. Liu, D. Nie, and L. Gai, "How can a blockchain-based anti-money laundering system improve customer due diligence process?" *J. Forensic Investigative Accounting*, vol. 13, no. 2, pp. 273–287, 2021.

[68] E. Aryee, "Enhancing mobile banking security through blockchain technology: Mitigating unauthorized access and protecting financial assets," *Int. J. Finance Banking Res.*, vol. 9, no. 2, p. 30, 2023.

[69] A. B. Jibril, M. A. Kwarteng, R. K. Botchway, J. Bode, and M. Chovancova, "The impact of online identity theft on customers' willingness to engage in e-banking transaction in ghana: A technology threat avoidance theory," *Cogent Bus. Manage.*, vol. 7, no. 1, Jan. 2020, Art. no. 1832825.

[70] J. F. Dolan, "Impersonating the drawer: A comment on professor Geva's consumer liability in unauthorized electronic funds transfers," *Can. Bus. LJ*, vol. 38, no. 38, p. 282, 2003.

[71] A. Luvanda, D. S. Kimani, and D. M. Kimwele, "Identifying threats associated with man-in-the-middle attacks during communication between a mobile device and the back end server in mobile banking applications," *IOSR J. Comput. Eng.*, vol. 16, no. 2, pp. 35–42, 2014.

[72] J. Chod, N. Trichakis, G. Tsoukalas, H. Aspegren, and M. Weber, "On the financing benefits of supply chain transparency and blockchain adoption," *Manage. Sci.*, vol. 66, no. 10, pp. 4378–4396, Oct. 2020.

[73] Z.-M. Zadorozhnyi, I. Ometsinska, and V. Muravskyi, "Determinants of firm's innovation: Increasing the transparency of financial statements," *Marketing Manage. Innov.*, vol. 5, no. 2, pp. 74–86, 2021.

[74] S. Darusalam, M. Janssen, J. Said, N. Omar, and M. I. Saputra, "Smart contracts for creating transparent transactions to reduce corruption," in *Proc. 24th Annu. Int. Conf. Digit. Government Res.*, Jul. 2023, pp. 355–361.

[75] H. Baber, "Blockchain-based crowdfunding," in *Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment*. Singapore: Springer, 2020, pp. 117–130.

[76] T. Vishwanath and D. Kaufmann, "Towards transparency in finance and governance," *SSRN 258978*, pp. 1–30, Sep. 1999. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=258978

[77] D. Gerace, C. Chew, C. Whittaker, and P. Mazzola, "Stock market manipulation on the Hong Kong stock exchange," *Australas. Accounting, Bus. Finance J.*, vol. 8, no. 4, pp. 105–140, 2014.

[78] M. Al-Okaily, M. Al-Kofahi, F. S. Shiyyab, and A. Al-Okaily, "Determinants of user satisfaction with financial information systems in the digital transformation era: Insights from emerging markets," *Global Knowl., Memory Commun.*, Jul. 2023, doi: 10.1108/GKMC-12-2022-0285.

[79] H. Stewart and J. Jürjens, "Data security and consumer trust in FinTech innovation in Germany," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 109–128, Mar. 2018.

[80] R. Bose, X. R. Luo, and Y. Liu, "The roles of security and trust: Comparing cloud computing and banking," *Proc. Social Behav. Sci.*, vol. 73, pp. 30–34, Feb. 2013.

[81] C. Moiso and R. Minerva, "Towards a user-centric personal data ecosystem the role of the bank of individuals' data," in *Proc. 16th Int. Conf. Intell. Next Gener. Netw.*, Oct. 2012, pp. 202–209.

[82] J. Soloway and P. Covington, "Data privacy security: Recent developments affecting consumer finance," *Bus. Law.*, vol. 62, no. 2, p. 631, 2006.

[83] R. Shaidulov and Z. Kenzhegalieva, "Blockchain as data protection in finance," *Sci. J. Astana IT Univ.*, pp. 113–121, Dec. 2022.

[84] B. Faber, G. C. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS: A blockchain-based personal data and identity management system," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2019, pp. 6855–6864.

[85] H. H. H. Aldboush and M. Ferdous, "Building trust in fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust," *Int. J. Financial Stud.*, vol. 11, no. 3, p. 90, Jul. 2023.

[86] C. M. Gupta and D. Kumar, "Identity theft: A small step towards big financial crimes," *J. Financial Crime*, vol. 27, no. 3, pp. 897–910, Oct. 2020.

[87] L. Găbudeanu, I. Brici, C. Mare, I. C. Mihai, and M. C. şcheau, "Privacy intrusiveness in financial-banking fraud detection," *Risks*, vol. 9, no. 6, p. 104, Jun. 2021.

[88] J. Serrado, R. F. Pereira, M. Mira da Silva, and I. S. Bianchi, "Information security frameworks for assisting GDPR compliance in banking industry," *Digit. Policy, Regulation Governance*, vol. 22, no. 3, pp. 227–244, Aug. 2020.

[89] S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18, Dec. 2016.

[90] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox, "Zcash protocol specification," Zerocoin Electric Coin Company, Denver, CO, USA, Tech. Rep. 2016-1.10, 2016.

[91] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. IEEE Symp. Secur. Privacy*, May 2018, pp. 315–334.

[92] J. Zhou, Y. Feng, Z. Wang, and D. Guo, "Using secure multi-party computation to protect privacy on a permissioned blockchain," *Sensors*, vol. 21, no. 4, p. 1540, Feb. 2021.

[93] T. Maurer, A. Levite, and G. Perkovich, "Toward a global norm against manipulating the integrity of financial data," Econ. Discuss. Papers, Kiel Inst. World Economy (IfW Kiel), Kiel, Germany, Work. Paper 2017-38, 2017. [Online]. Available: https://www.econstor.eu/handle/10419/162579

[94] M. Sumathi and S. Sangeetha, "Blockchain based sensitive attribute storage and access monitoring in banking system," *Int. J. Cloud Appl. Comput.*, vol. 10, no. 2, pp. 77–92, Apr. 2020.

[95] M. M. Rahman, D. A. Elshamly, S. U. Rehman, Z. Jameel, and R. Hameed, "Blockchain technology and its impact on European Bank's cyber security and data integrity," *J. Namibian Stud. Hist. Politics Culture*, vol. 34, pp. 1796–1813, Jun. 2023.

[96] M. U. Chowdhury, K. Suchana, S. M. E. Alam, and M. M. Khan, "Blockchain application in banking system," *J. Softw. Eng. Appl.*, vol. 14, no. 7, pp. 298–311, 2021.

[97] C.-H. Liao, X.-Q. Guan, J.-H. Cheng, and S.-M. Yuan, "Blockchain-based identity management and access control framework for open banking ecosystem," *Future Gener. Comput. Syst.*, vol. 135, pp. 450–466, Oct. 2022.

[98] K. Zheng, L. J. Zheng, J. Gauthier, L. Zhou, Y. Xu, A. Behl, and J. Z. Zhang, "Blockchain technology for enterprise credit information sharing in supply chain finance," *J. Innov. Knowl.*, vol. 7, no. 4, Oct. 2022, Art. no. 100256.

[99] H. Zhao, Y. Zhang, Y. Peng, and R. Xu, "Lightweight backup and efficient recovery scheme for health blockchain keys," in *Proc. IEEE 13th Int. Symp. Auto. Decentralized Syst. (ISADS)*, Mar. 2017, pp. 229–234.

[100] C. Zhang, Z. Ni, Y. Xu, E. Luo, L. Chen, and Y. Zhang, "A trustworthy industrial data management scheme based on redactable blockchain," *J. Parallel Distrib. Comput.*, vol. 152, pp. 167–176, Jun. 2021.

[101] W.-T. Tsai, Y. Luo, E. Deng, J. Zhao, X. Ding, J. Li, and B. Yuan, "Blockchain systems for trade clearing," *J. Risk Finance*, vol. 21, no. 5, pp. 469–492, Apr. 2020.
[102] T. Mori, "Financial technology: Blockchain and securities settlement," *J. Securities Oper. Custody*, vol. 8, no. 3, pp. 208–227, 2016.
[103] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based e-commerce," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, Jun. 2019.
[104] J. Dai and M. A. Vasarhelyi, "Toward blockchain-based accounting and assurance," *J. Inf. Syst.*, vol. 31, no. 3, pp. 5–21, Sep. 2017.
[105] S. Kozlowski, "An audit ecosystem to support blockchain-based accounting and assurance," in *Continuous Auditing*. Bingley, U.K.: Emerald Publishing Limited, 2018, pp. 299–313.
[106] D. Francati, G. Ateniese, A. Faye, A. M. Milazzo, A. M. Perillo, L. Schiatti, and G. Giordano, "Audita: A blockchain-based auditing framework for off-chain storage," in *Proc. 9th Int. Workshop Secur. Blockchain Cloud Comput.*, May 2021, pp. 5–10.
[107] E. Bonsón and M. Bednárová, "Blockchain and its implications for accounting and auditing," *Meditari Accountancy Res.*, vol. 27, no. 5, pp. 725–740, Oct. 2019.
[108] R. Henriquez, N. Bittan, and K. Tulbassiyev, "Blockchain and business model innovation: Designing a p2p mortgage lending system," in *Proc. 4th Int. Workshop P2P Financial Syst.*, Cleveland, OH, USA, 2018. [Online]. Available: https://www.researchgate.net/publication/326830940_Blockchain_and_business_model_innovation_Designing_a_P2P_mortgage_lending_system
[109] F. Yang, Y. Qiao, Y. Qi, J. Bo, and X. Wang, "BACS: Blockchain and AutoML-based technology for efficient credit scoring classification," *Ann. Oper. Res.*, pp. 1–21, Jan. 2022.
[110] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for IPFS," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1499–1506.
[111] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A smart contract enabled decentralized capability-based access control mechanism for the IoT," *Computers*, vol. 7, no. 3, p. 39, Jul. 2018.
[112] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innov.*, vol. 2, no. 1, p. 24, Dec. 2016, doi: 10.1186/s40854-016-0034-9.
[113] 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.
[114] A. Biryukov, D. Khovratovich, and S. Tikhomirov, "Privacy-preserving KYC on Ethereum," in *1st ERCIM Blockchain Workshop, Rep. Eur. Soc. Socially Embedded Technol.*, W. Prinz and P. Hoschka, Eds., 2018. [Online]. Available: https://core.ac.uk/reader/158569430, doi: 10.18420/BLOCKCHAIN2018_09.
[115] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of Money," in *Banking Beyond Banks and Money*. Cham, Switzerland: Springer, 2016, pp. 239–278.
[116] A. Bogner, M. Chanson, and A. Meeuw, "A decentralised sharing app running a smart contract on the Ethereum blockchain," in *Proc. 6th Int. Conf. Internet Things*, Nov. 2016, pp. 177–178.
[117] R. Hans, H. Zuber, A. Rizk, and R. Steinmetz, "Blockchain and smart contracts: Disruptive technologies for the insurance market," in *Proc. 23rd Americas Conf. Inf. Syst.*, 2017, pp. 1–10.
[118] (2017). *Allianz | B3i To Present Smart Contract Management System At 2017 Monte Carlo RVS Conference*. [Online]. Available: https://www.allianz.com/en/press/news/commitment/sponsorship/170719-b3i-to-present-smart-contract-management-system.html
[119] M. Crawford, "The insurance implications of blockchain," *Risk Manage.*, vol. 64, no. 2, p. 24, 2017.
[120] Y. Guo, Z. Qi, X. Xian, H. Wu, Z. Yang, J. Zhang, and L. Wenyin, "WISChain: An online insurance system based on blockchain and DengLu1 for web identity security," in *Proc. 1st IEEE Int. Conf. Hot Information-Centric Netw. (HotICN)*, Aug. 2018, pp. 242–243.
[121] J. Bird. (Dec. 2018). *'Smart' Insurance Helps Poor Farmers to Cut Risk*. [Online]. Available: https://www.ft.com/content/3a8c7746-d886-11e8-aa22-36538487e3d0
[122] *Etherisc White Paper*, Etherisc, Munich, Germany, 2017.
[123] H. T. Vo, L. Mehedy, M. Mohania, and E. Abebe, "Blockchain-based data management and analytics for micro-insurance applications," in *Proc. ACM Conf. Inf. Knowl. Manage.*, Nov. 2017, pp. 2539–2542.
[124] *Salt Lending White Paper*. Accessed: Jan. 20, 2024. [Online]. Available: https://www.cryptoground.com/salt-lending-white-paper
[125] ETHLend. *Ethlend/documentation*. Accessed: Jan. 20, 2024. [Online]. Available: https://github.com/ETHLend/Documentation/blob/master/ETHLendWhitePaper.md
[126] (2020). *Blockchain-Powered Money Transfers and Microfinance Services*. [Online]. Available: https://www.everex.io/cn/everexhow-it-works
[127] *Debitum Network (DEB) Price, Chart, Info—CoinSchedule*. Accessed: Jan. 20, 2024. [Online]. Available: https://www.coinschedule.com/cryptocurrency/debitum-network
[128] X. Zou, X. Deng, T.-Y. Wu, and C.-M. Chen, "A collusion attack on identity-based public auditing scheme via blockchain," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*. Singapore: Springer, 2020, pp. 97–105.
[129] A. M. Rozario and M. A. Vasarhelyi, "Auditing with smart contracts," *Int. J. Digit. Accounting Res.*, vol. 18, pp. 1–27, Aug. 2018.
[130] D. Yermack, "Corporate governance and blockchains," *Rev. Finance*, vol. 21, no. 1, pp. 7–31, Mar. 2017, doi: 10.1093/rof/rfw074.
[131] *TITA Project Whitepaper*. Accessed: Jan. 20, 2024. [Online]. Available: https://icosbull.com/eng/ico/titaproject/whitepaper
[132] *ASX Details Timeline, Features for New Blockchain-inspired System*. Accessed: Jan. 20, 2024. [Online]. Available: https://www.computerworld.com.au/article/640596/asx-details-timeline-features-new-blockchain-inspired-system/
[133] (Nov. 2018). *Hong Kong Stock Exchange and Digital Asset Partner To Create New Blockchain Trade Platform*. [Online]. Available: https://bitcoinexchangeguide.com/hong-kong-stock-exchange-and-digital-asset-partner-to-create-new-blockchain-trade-platform/
[134] A. Sharon. (Feb. 2019). *World's First Blockchain-powered Diamond Trading Platform to Launch in Hong Kong*. [Online]. Available: https://www.opengovasia.com/worlds-first-blockchain-powered-diamond-trading-platform-to-launch-in-hong-kong/
[135] Z. Du, X. Pang, and H. Qian, "PartitionChain: A scalable and reliable data storage strategy for permissioned blockchain," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 4, pp. 4124–4136, Apr. 2023.
[136] J. Rupasena, T. Rewa, K. T. Hemachandra, and M. Liyanage, "Scalable storage scheme for blockchain-enabled IoT equipped food supply chains," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 300–305.
[137] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Exp. Syst. Appl.*, vol. 154, Sep. 2020, Art. no. 113385.
[138] J. Li, N. Li, J. Peng, H. Cui, and Z. Wu, "Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies," *Energy*, vol. 168, pp. 160–168, Feb. 2019.
[139] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: An energy-efficient blockchain proof-of-work consensus algorithm," *Comput. Netw.*, vol. 214, Sep. 2022, Art. no. 109118.
[140] S. Wadhwa, S. Rani, Kavita, S. Verma, J. Shafi, and M. Wozniak, "Energy efficient consensus approach of blockchain for IoT networks with edge computing," *Sensors*, vol. 22, no. 10, p. 3733, May 2022.
[141] D. Mohanty, D. Anand, H. M. Aljahdali, and S. G. Villar, "Blockchain interoperability: Towards a sustainable payment system," *Sustainability*, vol. 14, no. 2, p. 913, Jan. 2022.
[142] M. Zachariadis, G. Hileman, and S. V. Scott, "Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services," *Inf. Org.*, vol. 29, no. 2, pp. 105–117, Jun. 2019.
[143] M. Knorr, "Developments in industry standards for cross-border payments," *J. Payments Strategy Syst.*, vol. 16, no. 3, pp. 283–291, 2022.
[144] L. König, M. Pirker, H. Geyer, M. Feldmann, S. Tjoa, and P. Kieseberg, "Disa—A blockchain-based distributed information security audit," in *Proc. Int. Conf. Inf. Integr. Web Intell.* Cham, Switzerland: Springer, 2023, pp. 27–34.
[145] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.
[146] D. A. Bard, J. J. Kearney, and C. A. Perez-Delgado, "Quantum advantage on proof of work," *Array*, vol. 15, Sep. 2022, Art. no. 100225.
[147] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% attack on blockchains: A mining behavior study," *IEEE Access*, vol. 9, pp. 140549–140564, 2021.
[148] J. Wang, L. Liu, S. Lyu, Z. Wang, M. Zheng, F. Lin, Z. Chen, L. Yin, X. Wu, and C. Ling, "Quantum-safe cryptography: Crossroads of coding theory and cryptography," *Sci. China Inf. Sci.*, vol. 65, no. 1, Jan. 2022, Art. no. 111301.

[149] A. Holcomb, G. Pereira, B. Das, and M. Mosca, "PQFabric: A permissioned blockchain secure from both classical and quantum attacks," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 1–9.
[150] W. Xiong and L. Xiong, "Smart contract based data trading mode using blockchain and machine learning," *IEEE Access*, vol. 7, pp. 102331–102344, 2019.
[151] A. Outchakoucht, E. Hamza, and J. P. Leroy, "Dynamic access control policy based on blockchain and machine learning for the Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, pp. 417–424, 2017.
[152] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, "When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 1178–1187.
[153] D. Calvaresi, Y. Mualla, A. Najjar, S. Galland, and M. Schumacher, "Explainable multi-agent systems through blockchain technology," in *Proc. Int. Workshop Explainable, Transparent Auto. Agents Multi-Agent Syst. (EXTRAAMAS)*, vol. 11763, Montreal, QC, Canada. Berlin, Germany: Springer, May 2019, pp. 41–58.
[154] A. S. Madhav and A. K. Tyagi, "Explainable artificial intelligence (XAI): Connecting artificial decision-making and human trust in autonomous vehicles," in *Proc. 3rd Int. Conf. Comput., Commun., Cyber-Secur. (IC4S)*. Singapore: Springer, 2022, pp. 123–136.
[155] M. Nassar, K. Salah, M. H. ur Rehman, and D. Svetinovic, "Blockchain for explainable and trustworthy artificial intelligence," *WIREs Data Mining Knowl. Discovery*, vol. 10, no. 1, p. e1340, Jan. 2020.
[156] X. Bao, C. Su, Y. Xiong, W. Huang, and Y. Hu, "FLChain: A blockchain for auditable federated learning with trust and incentive," in *Proc. 5th Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Aug. 2019, pp. 151–159.
[157] A. Haddaji, S. Ayed, and L. Chaari, "Federated learning with blockchain approach for trust management in IoV," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.* Cham, Switzerland: Springer, 2022, pp. 411–423.

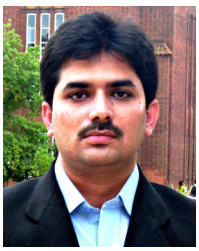
HANFANG CHEN was born in Yichang, Hubei, China, in 1982. She received the Ph.D. degree from the School of Public Finance and Taxation, Zhongnan University of Economics and Law, Wuhan, in 2019. She is currently working as a Lecturer with the School of Economics and Management, Hubei University of Technology, and is a Postdoctoral Fellow at the Jiangxi University of Finance and Economics. Her research interests include financial management, accounting, and taxation.

NIANKUN WEI was born in Jingmen, Hubei, China, in 1997. He is currently pursuing the master's degree in accounting with the School of Economics and Management, Hubei University of Technology, Wuhan. His research interests include financial management, accounting, and taxation.

LEYAO WANG was born in Wuhan, Hubei, China, in 1999. He is currently pursuing the master's degree in accounting with the School of Economics and Management, Hubei University of Technology, Wuhan. His research interests include financial management, accounting, and taxation.

WAEL FAWZY MOHAMED MOBARAK was born in Egypt, in 1979. He received the Ph.D. degree in applied engineering mathematics from the Faculty of Engineering, Alexandria University, Alexandria, Egypt, in 2013. He joined Alexandria University as an Assistant Professor, till 2015. He is currently delegated as an Assistant Professor with the College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia. His research interests include dynamics, mathematical modeling, and engineering management.

MARWAN ALI ALBAHAR received the B.S. degree in computer science from King Faisal University, in 2011, the M.Sc. degree (Hons.) in computer science from Frostburg State University, in 2015, and the Ph.D. degree from the University of Eastern Finland, in 2018. He is currently an Associate Professor of computer science with the Department of Computer Science, Umm Al-Qura University, Mecca, Saudi Arabia. His main research interests include computer networks and security, cybersecurity, and artificial intelligence.



ZAFFAR AHMED SHAIKH (Member, IEEE) received the Ph.D. degree from the Institute of Business Administration, Karachi, Pakistan, in 2017, under the supervision of Prof. Shakil Ahmed Khoja. The title of his dissertation was Guided Personal Learning Environment Model: Concept, Theory, and Practice. He is currently an Associate Professor of computer science and information technology with Benazir Bhutto Shaheed University, Lyari, Karachi. His teaching portfolio includes a range of subjects, such as assembly language, business intelligence and analytics, compiler construction, computer architecture, digital logic design, human–computer interaction, semantic analysis, semantic web, statistical inference, and automata theory. He spent six months, in 2014, as a Visiting Doctoral Fellow with the REACT Research Group, École Polytechnique Fédérale de Lausanne, Switzerland, due to his contributions to personalized recommender systems and technology-enhanced learning and semantic analysis-based personalized recommender systems. His academic career spans more than 23 years, during which he received many prestigious scholarships and travel grants from national and international organizations, including the M.S. leading to Ph.D. scholarship for five years and the International Research Support Initiative Program (IRSIP) scholarship for six months from HEC Pakistan, and several international travel grants for presenting research: four grants from HEC Pakistan, two grants from IBA-Karachi, and two grants from the Ministry of Education, Saudi Arabia, for the 3rd and 4th eLi conferences. He has published more than 70 peer-reviewed articles in high-ranked journals many of which are indexed in SSCI, SCIE, and Scopus. His current research interests include artificial intelligence, blockchain, business intelligence, cybersecurity, educational technologies, energy economics, expert systems, fault detection and diagnosis, green computing, healthcare systems, the Internet of Things, large language models, learning environments, machine learning methods, medical image processing, metaverse, pharmacy informatics, recommender systems, and fintech. He has presented his work at leading international conferences, such as ACM SIGITE, IEEE iCALT, IEEE IANA, and the PLE Conference. He is a Senior Editorial Board Member and a Reviewer of many prestigious journals, such as *Australasian Journal of Educational Technology*, *British Journal of Educational Technology*, *Behavior & Information Technology*, *BMJ Open*, *Complexity*, *Computers in Human Behavior*, *Computers & Education*, *Cogent Education*, *Cybernetics and Systems*, *Human-centric Computing and Information Sciences*, IEEE Access, IEEE Sensors Journal, *Interactive Learning Environments*, *Multimedia Tools and Applications*, *PLoS ONE*, *System*, *Wireless Communications and Mobile Computing*, and many MDPI journals.