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

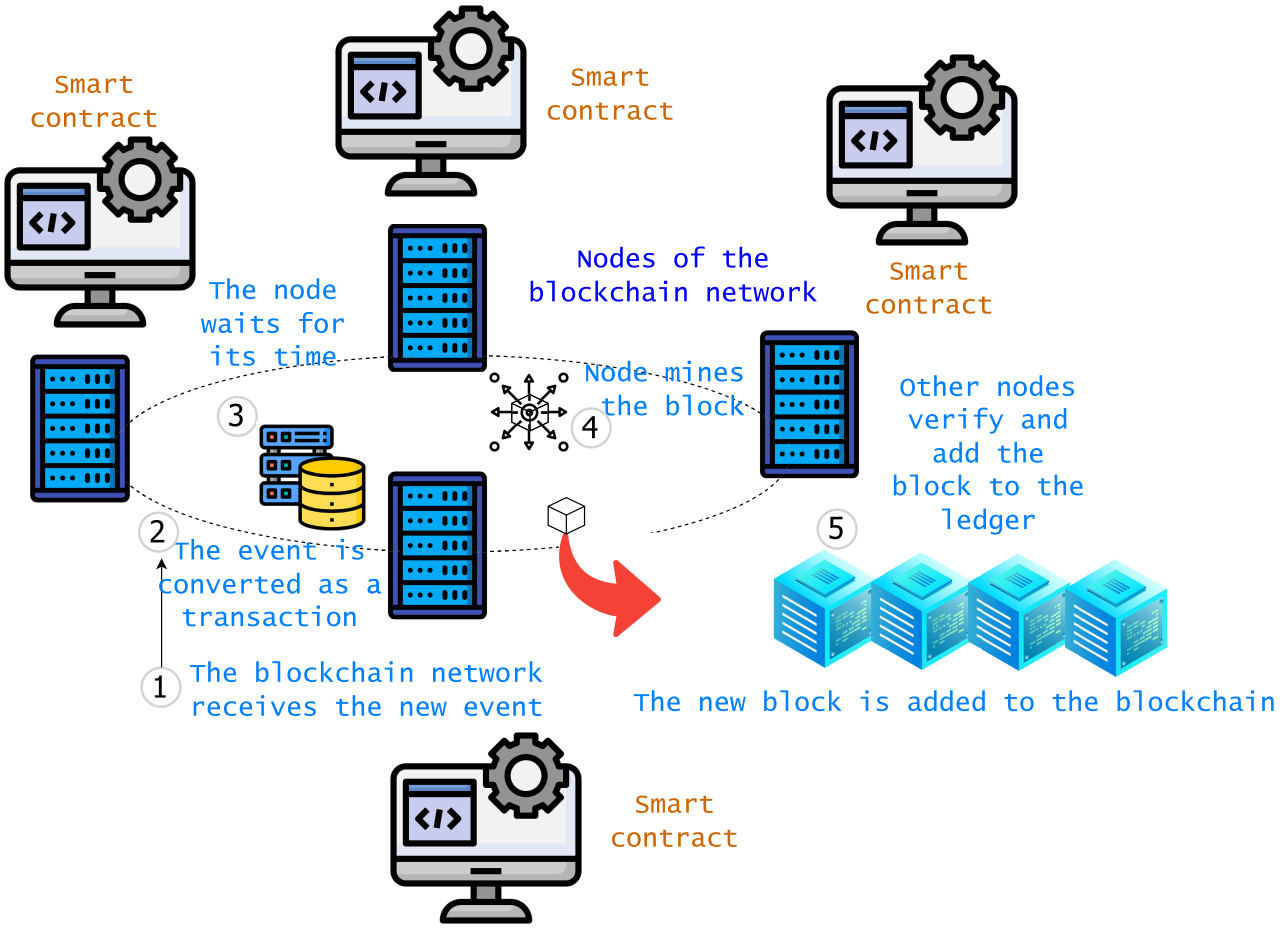


FIGURE 1. Blockchain workflow.

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]

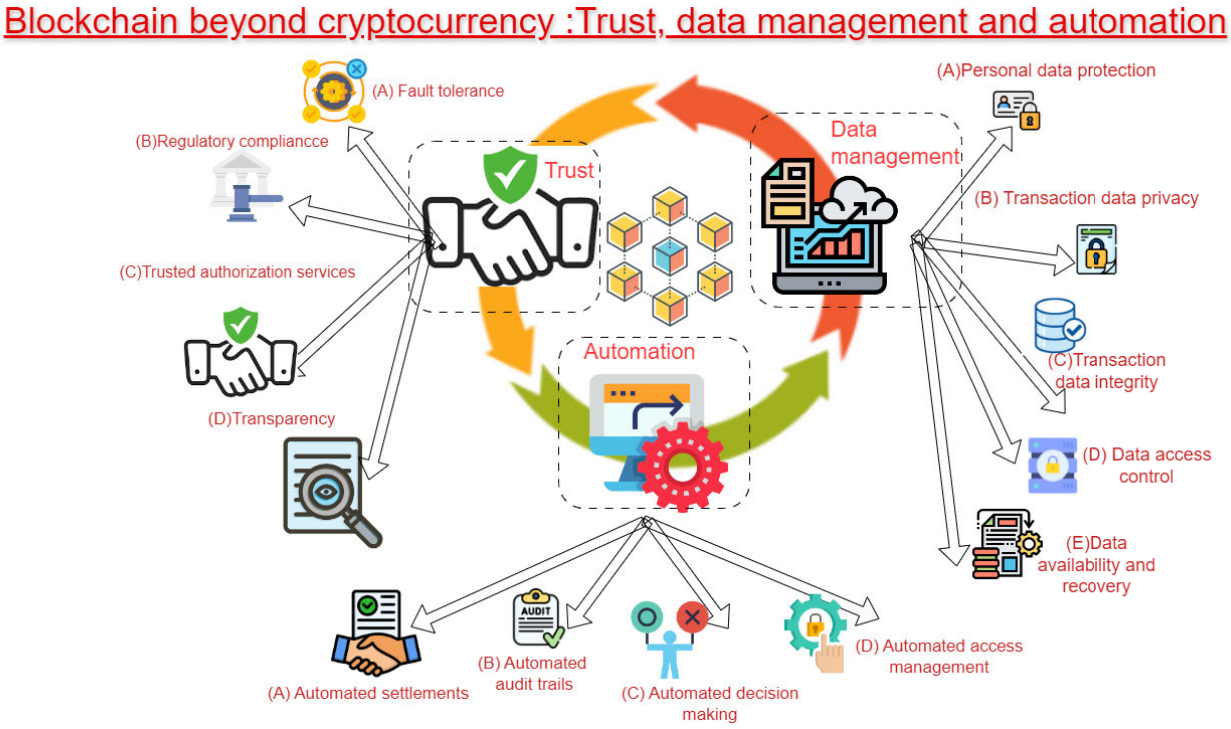


FIGURE 2. Summary of the contribution of blockchain beyond cryptocurrency.

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

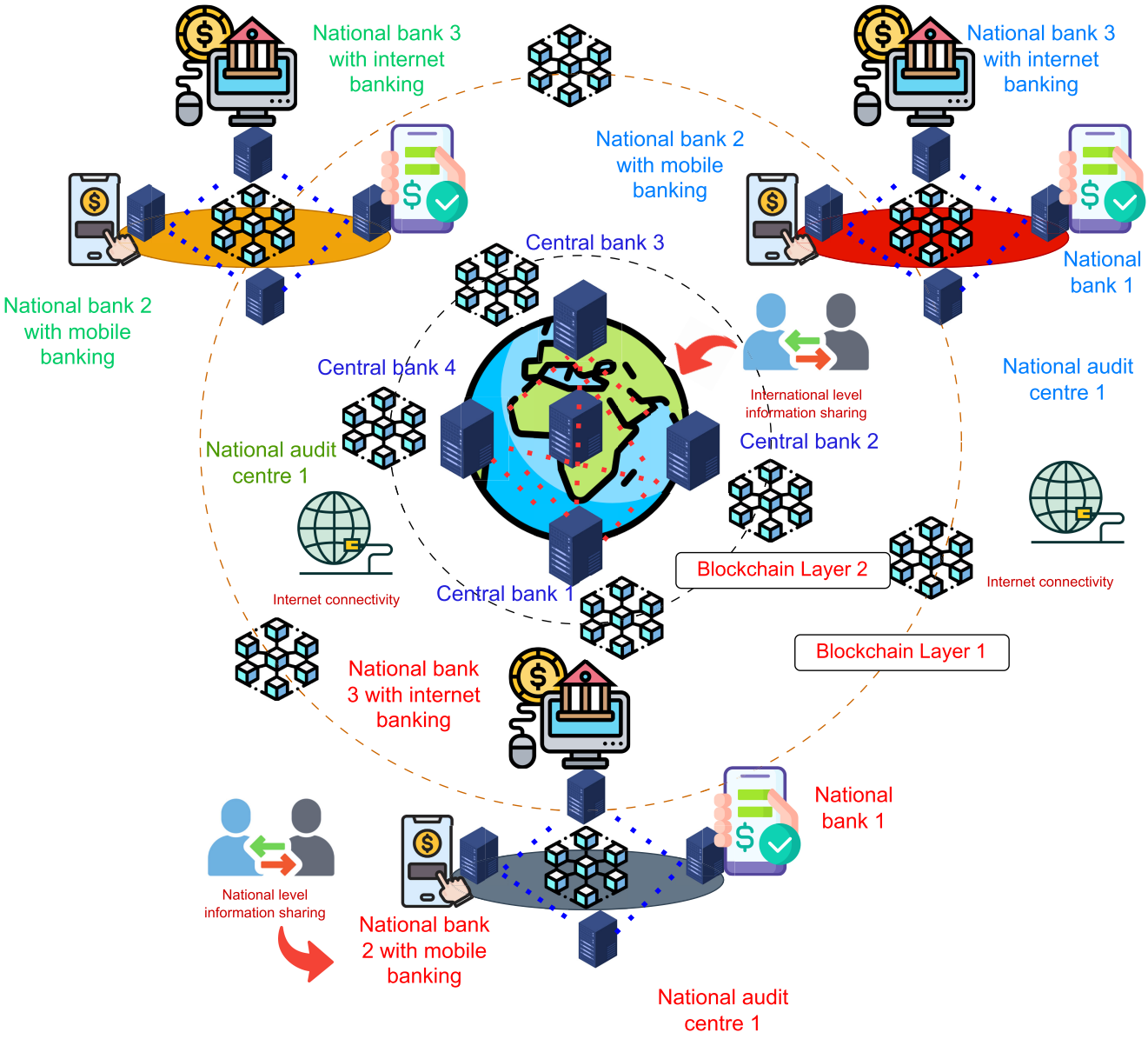


FIGURE 3. Integration architecture.

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.

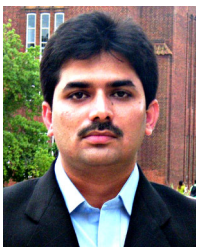
HANFANG CHEN was born in Yichang, Hubei, China, in 1982. She received the Ph.D. degree from the School of Public Finance and Taxation, Zhongnan University of Economics and Law, Wuhan, in 2019. She is currently working as a Lecturer with the School of Economics and Management, Hubei University of Technology, 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.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INTELLIGENT BIG DATA ANALYTICS FOR INTERNET OF THINGS, SERVICES AND PEOPLE

Received March 2, 2021, accepted March 19, 2021, date of publication April 13, 2021, date of current version April 28, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3072849

A Survey on Blockchain Technology: Evolution, Architecture and Security

MUHAMMAD NASIR MUMTAZ BHUTTA[1], AMIR A. KHWAJA[1], ADNAN NADEEM[2], (Member, IEEE), HAFIZ FAROOQ AHMAD[3], MUHAMMAD KHURRAM KHAN[4], (Senior Member, IEEE), MOATAZ A. HANIF[5], HOUBING SONG[5], (Senior Member, IEEE), MAJED ALSHAMARI[1], AND YUE CAO[6], (Member, IEEE)

[1]Information Systems Department, College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2]Faculty of Computer and Information System, Islamic University of Madinah, Medina 42351, Saudi Arabia
[3]Computer Science Department, College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al-Ahsa 31982, Saudi Arabia
[4]Center of Excellence in Information Assurance, King Saud University, Riyadh 12372, Saudi Arabia
[5]Security and Optimization for Networked Globe Laboratory (SONG lab), Embry-Riddle Aeronautical University, Prescott, AZ 86301, USA
[6]School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Corresponding authors: Muhammad Nasir Mumtaz Bhutta (mmbhutta@kfu.edu.sa) and Muhammad Khurram Khan (mkhurram@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research (DSR), King Faisal University, Saudi Arabia, under Grant 186218.

ABSTRACT Blockchain is a revolutionary technology that is making a great impact on modern society due to its transparency, decentralization, and security properties. Blockchain gained considerable attention due to its very first application of Cryptocurrencies e.g., Bitcoin. In the near future, Blockchain technology is determined to transform the way we live, interact, and perform businesses. Recently, academics, industrialists, and researchers are aggressively investigating different aspects of Blockchain as an emerging technology. Unlike other Blockchain surveys focusing on either its applications, challenges, characteristics, or security, we present a comprehensive survey of Blockchain technology's evolution, architecture, development frameworks, and security issues. We also present a comparative analysis of frameworks, classification of consensus algorithms, and analysis of security risks & cryptographic primitives that have been used in the Blockchain so far. Finally, this paper elaborates on key future directions, novel use cases and open research challenges, which could be explored by researchers to make further advances in this field.

INDEX TERMS Evolution of blockchain, blockchain architecture, smart contracts, blockchain applications, development frameworks, blockchain security.

I. INTRODUCTION

The concept of secured chain of blocks is not a new idea. It was presented by Stuart Haber *et al.* in 1991 as a means to digitally timestamp electronic documents to protect against tempering [2]–[4]. However, it gained popularity in the recent years when used in Blockchain technology to store transactions of a crypto currency called "Bitcoin" [1].

The Blockchain 1.0 technology is associated with Cryptocurrencies, especially Bitcoin. Bitcoin uses Blockchain as a way to solve the long-existing problems of double spending of digital cash and processing of digital transactions in a decentralized way without the need of any trusted third party.

The associate editor coordinating the review of this manuscript and approving it for publication was Jenny Mahoney.

In a layman term, Blockchain is defined as the chain of digital blocks connected and associated with each other as an open distributed ledger. Initially, it was used to store only transactions of digital currencies, but later it started to use in other applications beyond currency and payments [7].

There are also different types of Blockchains based on their usage and distinct attributes: 1) Public blockchains 2) Private blockchains and 3) Consortium blockchains. Public blockchains are truly decentralized and allow anyone to join the network and engage in managing them. While in private blockchains only invited people from a single organization can join the network and manage them. The consortium Blockchain also called "Federated Blockchain" is between public and private Blockchain, in terms of permissions and management. Invited people from multiple organizations are

TABLE 1. Comparison of Recent Blockchain Survey Articles with this SURVEY PAPER.

Topic	Details of Topic	Addressed in Previous Survey Papers	Addressed in this Article
Preliminaries	Preliminary Concepts related to understand Blockchain	[20]	✓
Evolution	Blockchain 1.0 (Cryptocurrency) , Blockchain 2.0 (Smart Contracts) Blockchain 3.0 (Blockchain Applications)	[15][29]	✓
	Types of Blockchain (Public, Consortium, Private, Hybrid)	[8][13][16]	✓
Architecture (Components and Working)	Blockchain 1.0 (Cryptocurrency) Components and their Working	[8],[9],[11],[12],[13],[14] [15],[16],[17] [18], [19], [20], [21], [23], [24], [25], [26], [27], [28]	✓
	Blockchain 2.0 (Smart Contracts) Components and their Working	[8][13]	✓
	Blockchain 3.0 (Blockchain Applications) Components and their Working	[9][12],[22],	✓
Development Frameworks	Application Development Frameworks	[9][17]	✓
Security and Privacy	Open Research Issues and Challenges	[8] [11][15][16][17]	✓
Characteristics	Decentralization, Disruptive Technology, Scalability, Computation	[8] [9][11][16][18]	✓
Scalability	Scalability in terms of changing its structure or divide in multiple committees	[48][67][73][160]	✓

allowed to join this Blockchain. These different types of blockchains are described in detail later in this paper. The main strength of the applicability of Blockchain to such wide domains is in its characteristics or features like decentralization, pseudonymity, transparency, democracy, immutability, auditability, fault tolerance and security. The success of Blockchain technology also heavily depends on the availability of the application development frameworks (ADFs).

As one of the present technologies that have managed to attain huge fame, there are still numerous open issues in security and privacy associated with Blockchain innovation.

A. CONTRIBUTION OF THIS SURVEY AND COMPARISON WITH RELATED SURVEY ARTICLES

This paper mainly contributes to the existing knowledge in two broad ways. First, the Blockchain evolution and architecture in cryptocurrencies is reviewed as well as architecture and research developments pertaining to Smart Contracts (Blockchain 2.0) and Blockchain-based applications or ecosystems in general (Blockchain 3.0) beyond financial transactions. Second, we also present a comparative analysis of existing Blockchain frameworks, consensus algorithms, security risks, and future perspectives in this single paper. Recently, many survey articles have attempted to review the Blockchain technology in varying degrees of depth with a specific scope. However, based on the literature review, no paper has addressed detailed aspects of various versions of Blockchain technology, review of consensus algorithms, and security issues together in a single survey paper. This lack of comprehensiveness motivates us to contribute through this survey of Blockchain evolutions, architecture, consensus, and security in-depth in this paper.

Many survey articles are written in the recent past with only a focus on cryptocurrencies [8], [9], [11]– [21], [23]– [28], or only consensus algorithms [20], [26], [157], [170]. Some articles have superficially discussed smart contracts [8], [13] and Blockchain applications architecture [9], [12], [22]. Some survey articles have also presented different Blockchain applications [26], [151] while major review focus has been on Blockchain applications with other technologies like IoT and smart cities [8], [9], [14], [21]– [25]. The Blockchain security is also reviewed in some survey articles including [11], [15], [16], [29], [152].

However, on the other side, the contribution of this survey is as follows: preliminary technical concepts and characteristics and issues are discussed to enable the reader to understand the Blockchain concepts effectively. The architecture of all versions of Blockchain including cryptocurrencies, smart contracts, and generic applications, is reviewed in detail to guarantee the flow of understanding in a holistic manner. The design and working of components of all versions of Blockchain are presented with a clear distinction for different versions. The research related to consensus algorithms, development frameworks, and security is then reviewed in detail in this paper.

Ultimately the goal of this survey is to acquaint the researchers with inner technical details and research advancements of all versions of Blockchain technology. The similarities and differences of research areas addressed in this survey in comparison to previous survey articles are highlighted in Table 1.

B. ORGANIZATION OF THE SURVEY

The organization of the survey is as follows and shown in Figure 1: Section 2 discusses the background concepts as preliminaries for better understanding of core of this paper followed by characteristics of Blockchain. This section also highlights the challenges and issues of Blockchain technology. Section 3 presents evolution and types of Blockchain technology in detail. In section 4, we review existing

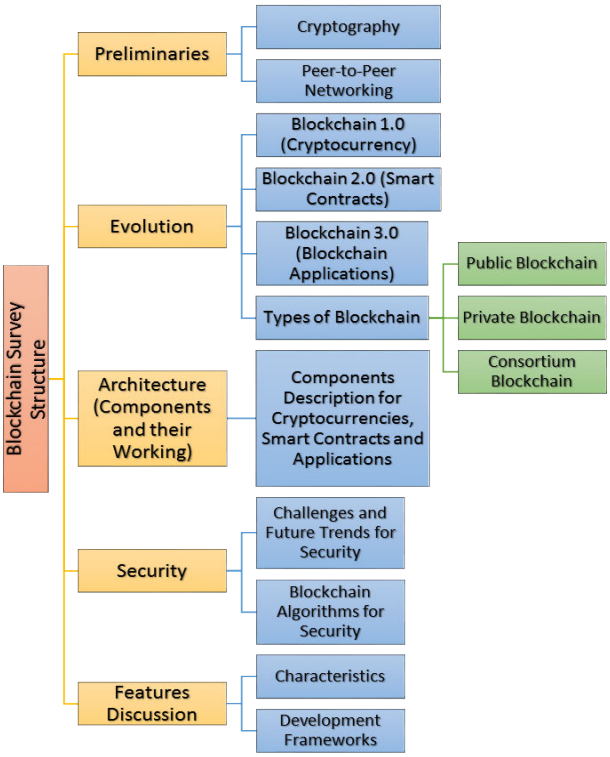


FIGURE 1. Structure and Contribution of this survey.

architectures and components of Blockchain in relation to cryptocurrencies, smart contracts and Blockchain applications in general. The research advancements in consensus algorithms are highlighted separately in section 5. A detailed discussion in research advancements and open research issues related to Blockchain security is included in Section 6. Section 7 describes the open research issues learned from the literature review to carry out in future and finally, Section 8 concludes the survey.

II. BACKGROUND, CHARACTERISTICS AND CHALLENGES

This section first presents the basic concepts of Blockchain technology and then discusses the characteristics and issues of technology.

1) PRELIMINARY CONCEPTS

a: PEER-TO-PEER (P2P) NETWORK

P2P network is a distributed network architecture to share resources among participants. The participants make their resources (processing power, link capacity, printers and storage capacity etc.,) available to be shared with other participants. Each participant node (peer) in such network acts in roles of both (client and server). At one time, peer A (acting as client) can directly request services and/or contents from other peer B (acting as server) of the network without any intermediate entities. Later, peer A may act as a server for a content or service request from peer B acting as client [1].

b: CRYPTOGRAPHY

The mathematical art of making communication secure is cryptography. It is commonly used in most modern security protocols [2]. In cryptography, a mathematical value called 'key' plays a central role. There are two types of modern cryptography:

- Symmetric key cryptography in which same key is used by sender and receiver for cryptographic operations.
- Asymmetric key cryptography in which, each communicating party has two different keys called public and private keys used for different cryptographic operations in different ways [2].

There are multiple operations performed in cryptography for provision of different security services like confidentiality (keeping information private to communicating parties), integrity (ensuring information remains in its original form), authentication (validating the identity of source) and non-repudiation (ensuring integrity and authentication) [2].

c: ENCRYPTION/DECRYPTION

Encryption is used for provision of confidentiality of security service. Encryption is a process to encode the plaintext (intelligible data) into cipher text (unintelligible data or ununderstandable data). The decryption is the reverse process to convert cipher text into plaintext. Encryption and decryption process can be implemented by using symmetric or asymmetric cryptography [3].

d: HASH

Hash is one-way mathematical function to protect the integrity of data. It works by calculating a fixed-sized unique value called "hash value" for every variable input. The hash function is one-way, which means original data cannot be calculated back from the unique output [3]. Its security strength lies on one-way characteristic, which is used to protect the integrity of data [3].

e: HASH CHAIN

A hash chain is generated by successively applying the hash function on a piece of data. For example, a hash value h_1 is generated by applying a hash function $f(x)$ on data x. The h_1 is input to the other hash function '$f(h_1)$' to calculate second hash value h_2 in the chain and so on. These calculated hash values $h_1, h_2, \ldots, h_n$ make a chain of hashes of length n. Because, hash functions are irreversible so h_1 cannot be computed from h_2 and then h_2 cannot be computed from h_3 and so on [4]. Hash chains have many applications for protection of data integrity and play a key role in Blockchain.

f: MERKLE TREE

Merkle trees also called hash trees provide efficient and secure verification of data by arranging the data and corresponding hash values in the form of a tree. In the tree structure, every leaf node is labelled with the hash value of some data and every non-leaf node contains the hash value of its child nodes. Figure 2 shows an example of a Merkle tree

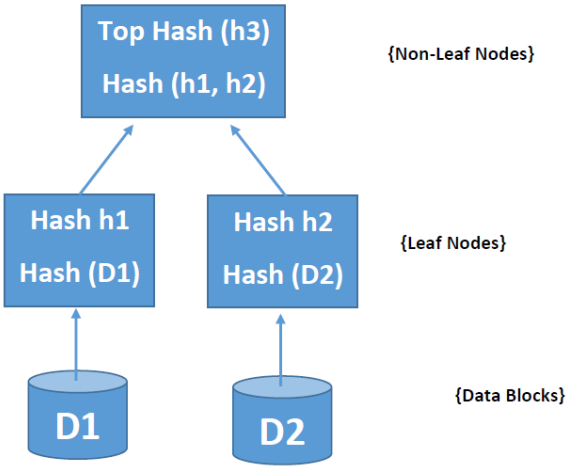


FIGURE 2. An Example of Merkle Tree (Binary Hash Tree).

in which data blocks represented as D1 and D2 are input to leaf nodes (hashes of D1 and D2) of Merkle Tree. From the hashes h_1 and h_2, another hash is calculated and is added as the parent node of child nodes [5].

g: DIGITAL SIGNATURES & TIMESTAMP

Digital signatures are used as a proof of authorship along with the contents. The signatures are usually applied using public key cryptography in which, a signer uses its private key to sign a document and a recipient can verify the signatures using signer's public key. Digital signatures are considered authentic, unforgeable, non-reusable and non-repudiated. It means that digital signature cannot be shifted for any other document/contents and one cannot deliberately claim the signature except the original signer and even original signer cannot repudiate it [3], [40]. Timestamp is the time at which event occurrence is recorded by a computer, rather than the time of event itself. Usually, it records the date and time of the day at which event occurred and is accurate to a small fraction of second. This timestamp's data is recoded in a consistent manner along with the actual data for easy comparison of two different records to track progress over time [6].

2) BLOCKCHAIN CHARACTERISTICS

This section synthesizes key Blockchain characteristics from literature. In doing so, the paper highlights variation in terminology for some of these characteristics which is quite natural for a technology considered in its infancy. The section attempts to unify the terminologies for various characteristics. The benefits and any possible issues related to each characteristic are also discussed. In addition, current issues with the Blockchain technology are identified and key research challenges are highlighted.

Following key characteristics have been identified for the Blockchain technology:

a: DECENTRALIZATION

Decentralization is perhaps the most important characteristic of the Blockchain. The Blockchain ledger exists on multiple computers, often referred to as nodes. These nodes form a Blockchain network with several of these nodes working in a P2P manner, validating access to the information without a centralized authority [50], [70] and [12]. The Blockchain system uses distributed system structure for recording, storing, updating, transmission, verification, maintenance, and several other processes related to the information in the Blockchain network [16], [71]. This decentralization characteristic eliminates the need for powerful central authorities and instead transfers control to the individual user making the system fair and considerably more secure. Information recording is performed, and the transactions are validated, using a set of rules and algorithms, called consensus protocols, among the Blockchain nodes to ensure that information is consistent and incorruptible [70] and [72]. Consensus is achieved when enough devices agree about what should be recorded onto a Blockchain. Chain nodes may use a pure mathematical method (asymmetric cryptography) to establish trust among each other without control of any central authority or regulatory agency to manipulate the data unilaterally [71]. Each distributed node in this network is relatively independent, have equal rights and obligations, and does not affect the entire network if there is a node level corruption, guaranteeing improved reliability and robustness of the Blockchain system [71]. Due to complex consensus mechanism required to edit or manipulate multiple copies of information recorded on the Blockchain; it can be certain that the information is genuine. Multiple copies of distributed information on the Blockchain also prevents the risk of information being lost or destroyed due to dependency on a centralized location. Moreover, removing a centralized body collecting, recording, maintaining, and, in general, unrestricted access to information, also improves privacy of users as well as eliminates misuse of the information. Finally, lack of reliance on a centralized body for executing and validating transactions can significantly reduce intermediary costs and improve performance bottlenecks at the central servers [71], [72].

b: TRANSPARENCY

Transactions on Blockchain ledger are completely transparent where anyone can see the details and history of any transaction. This level of transparency is unique to Blockchain technology and provides a high level of accountability and integrity to the information, ensuring that nothing is unduly altered, deceitfully added, or removed. This high level of transparency is unprecedented, especially for large financial systems. This level of transparency is achieved because a Blockchain network has several validating peer nodes without a centralized authority [12] as well as the fact that the holdings and transactions of each public address are accessible and open to viewing to anyone [70], resulting in traceable and transparent transaction records. Xinyi *et al.* [71] used the term openness to refer to the same concept. According to Xinyi *et al.* [71], the technical foundation of Blockchain is open source where any node can develop appropriate

applications through an open interface to query data of Blockchain resulting in the data content and the operating rules of the whole system to be highly public and transparent with no deception between nodes [71]. Same transparency rules apply on any updates to any data in the Blockchain [16]. Zheng *et al.* [72] and Ferrag *et al.* [42] used the term auditability for high visibility, easy tracking, and verification of the transactions. In addition to significant importance of this characteristic for financial auditability of large companies, another key area where transparency characteristic has found its applicability is in healthcare and clinical trials data transparency. In healthcare, Blockchain technology can be used by individual patients to easily view all their claims, medical history, transactions, and overdue payments. Clinical trials data has traditionally been held from researchers, doctors, and patients, resulting in a lack of trust and credibility of findings [55]. Blockchain based methods were suggested to trace the existence of documents containing pre-specified end points in clinical trials [45]. Use of smart contracts were also proposed to act as a trusted administrator to address data manipulation issues common in clinical trials [55]. Supply chain management malpractices as well as obscurity of product history is also shown to benefit from the transparency characteristic of Blockchain [30], [43] and [161]. Non-fraudulent public elections and increasing voters' trust in the electoral process is also suggested to benefit from the transparency characteristic [53].

c: AUTONOMY

All transactions are usually based on trust which guarantees that the parties involved can depend on each other in fulfilling their commitments. Blockchain technology provides a system where trust is no longer an issue. This ''trust free'' system means that the Blockchain system can function in a P2P manner without a reliable third party required to ensure trust [70]. Some have called such systems ''trustless'' [32], [61] and [69]. However, this term has a negative connotation and implies that there is trust missing among the parties transacting using a Blockchain system [47]. Blockchain uses cryptography to completely replace third party as the governor of trust. Using the privacy and unforgeability of asymmetric cryptography, the Blockchain system protects message contents and verifies the sender identity, ensuring reliable transactions in the Blockchain system [71]. Complex distributed consensus algorithms are used by participating nodes on the Blockchain network to unanimously and securely add or update data to the distributed ledger of Blockchain, while solving the problem of ownership confirmation in transaction process as well as maintaining the system integrity [71]. These Blockchain transactions are accomplished without intervention of a third party to ensure trust due to the use of the failsafe consensus protocols providing the basis for the trust [16]. Elimination of these ''middlemen'' to ensure trust results in decreasing the overall cost of transactions.

d: SECURITY

Blockchain systems are inherently secure as these systems use asymmetrical cryptography consisting of set of public keys visible to anyone and a set of private keys visible only to the owner. These keys are used to ensure the ownership of transaction as well as the un-tamperability of the transaction [42] and [71]. Security in the Blockchain system is related to the integrity, confidentiality, and authorization of transactions [70]. The distributed nature of Blockchain system requiring P2P consensus mechanism eliminates single point of failure for data [70] versus that which is centrally stored and is far more vulnerable to being compromised.

e: IMMUTABILITY

Immutability is also called un-tampereability [71], persistency [72], and unforgeability [50], and immutability for Blockchain [16], [42], [70] and [12] means that once data is added to a Blockchain, it cannot be altered or tampered with. The data blocks in a Blockchain structure are time stamped and each block is encrypted with hash algorithm, making the entry of data permanent and tamper-proof unless consensus of majority of the nodes of the whole system [16], [71] and [12]. The transactions can be viewed by anyone anytime, however, once validated and added to the Blockchain, these transactions cannot be changed or deleted, making them irreversible and immutable [56]. Any change, no matter how small, will generate a different hash and can be detected right away, making the shared ledger immutable [70]. This feature has a great benefit for financial transactions and financial audits since either as a provider or recipient of data it proves that the data has not been changed. This characteristic also generates trust in the Blockchain system. However, immutability for Blockchain has its own issues and challenges and some have now started to question the benefits of immutability [39] and [40].

f: TRACEABILITY

Data traceability is to track the source, destination, and sequence of various updates the data goes through in between nodes. Needed for data integrity and higher levels of trust on the information, data traceability also has several other benefits of better data governance, conformity with regulations, understanding impact of change, and improvement of data quality among others [46]. Blockchain technology provides support for data traceability as information added or updated in a Blockchain system is time stamped. Time stamp technology is used to add time dimension for each data block and the hash values stored in each block correctly identifies the current and parent block [71]. Data traceability has high impact in the areas of financial transactions, clinical trials [72], and supply chain management [49] and [62].

g: ANONYMITY

Anonymity characteristic of Blockchain supports privacy, which is defined to be protected from unauthorized intrusion or observation. Anonymity is achieved by authenticating

transactions without revealing any personal information of parties involved in the transaction. The data is exchanged between nodes using a defined algorithm establishing trust, hence the information of the nodes does not need to be revealed or verified and the information transfer can be carried out anonymously [31]. Users in a Blockchain system can interact with generated Blockchain addresses to keep their real identities hidden [16] and [72]. However, Blockchain cannot guarantee perfect privacy due to its inherent nature of distributed and public environment [72] and, hence, that is why some researchers have used the term pseudonymity [70] to define this characteristic of the Blockchain where anyone can create a Blockchain address and it is not possible to connect that address to a person without information from other sources [34].

h: DEMOCRATIZED

In a Blockchain system, decisions are made democratically by all nodes using P2P approach [70]. Consensus algorithms are used by all decentralized nodes to allow specific nodes for adding new blocks to an existing Blockchain as well as to ensure the block is appropriately appended to the shared ledger and its copies across the Blockchain nodes are synchronized properly [12], [70], [71]. All nodes participating in this decision process are relatively independent, possess equal rights and obligations, share data, and jointly maintain information in the Blockchain resulting in low maintenance cost overheads [71]. Nodes can vote based on their computing power, accepting valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them [54] and [72].

i: INTEGRITY

Blockchain systems, by design, are inherently resistant to changes in data. Data integrity is the assurance that the data in the Blockchain remains accurate and consistent over its entire life cycle [12]. This feature is achieved due to the decentralized and virtually immutable shared ledgers across the Blockchain network which means once a data block is agreed upon to be added to a Blockchain, the transaction record of that block cannot be edited or modified. This data is permanently preserved in the Blockchain system with multiple copies of it in various nodes across the Blockchain network, effectively guaranteeing the reliability and integrity of data [71].

j: INTEGRITY

Blockchain systems, by design, are inherently resistant to changes in data. Data integrity is the assurance that the data in the Blockchain remains accurate and consistent over its entire life cycle [12]. This feature is achieved due to the decentralized and virtually immutable shared ledgers across the Blockchain network which means once a data block is agreed upon to be added to a Blockchain, the transaction record of that block cannot be edited or modified. This data is permanently preserved in the Blockchain system with multiple copies of it in various nodes across the Blockchain network, effectively guaranteeing the reliability and integrity of data [71].

k: PROGRAMMABILITY

Blockchain technology is open source and users can develop applications through a common application programming interface [16] and [50]. The flexible script coding system can be used to create advanced smart contracts or other decentralized applications [71]. The SDN controllers of the nodes are used to provide programming interface for network management [42]. Li *et al.* [15] proposed a Blockchain-based data sharing system, called MeDShare, for cloud service providers consisting of user layer, data query layer, data structuring provenance layer, and existing database infrastructure layer. All Blockchain systems provide some programming language to implement transaction logic [70]. Ferrag *et al.* [42] suggest that these APIs should be as user friendly as possible. Examples of programmable blockchains consist of Ethereum, Tron, and Cardano among others.

l: FAULT TOLERANCE

Blockchain is inefficient and redundant by design to provide high levels of immutability and fault tolerance, both of which are important Blockchain characteristics [52]. Since Blockchain network uses P2P architecture, each node is considered equal to every other node and every node can act both as a client or as a server which gives the network an extremely high margin of error for nodes coming and going offline, for network transport issues, etc. [52]. Blockchains are designed to be Byzantine Fault Tolerant, which means the network will come to a consensus even if some nodes are down or not acting correctly. A consensus protocol is considered fault tolerant if it can recover from failure of a node participating in consensus [33]. Fault tolerance of the Blockchain system can recover from either fail-stop faults where some nodes fail to participate in the consensus protocol due to software or hardware reasons or Byzantine faults where nodes start to misbehave due to either software bugs or malicious attacks [33].

m: AUTOMATIC

Smart contracts on the Blockchain can automatically perform transaction generation, decision making, and data storage [70]. All nodes in the system can automatically transact and verify data using specific consensus protocols [50]. The Blockchain is maintained and validated automatically through a protocol without manual intervention [50]. However, just like any other computer program, smart contracts can also suffer from bugs and errors with no easy way to fix or update these contracts [51]. In addition, smart contracts can also be attacked by hackers just like any other software application.

3) CHALLENGES AND ISSUES

Even though Blockchain technology has gained fast momentum and has become the focus of research community, it is

not devoid of issues and challenges that need to be addressed for this technology to become mainstream and to be deployed widespread. Some of the Blockchain issues and challenges are as follows:

4) SCALABILITY

Blockchain systems, as these exist today, suffer from scalability issues [66] and [12]. These scalability issues rise from limitations of low throughput, high transactional latency, and increasingly high resource needs [12]. The storage space requirements for the Blockchain will continue to increase as the number of transactions increase. For example, in September 2017, the Bitcoin size was about 158 GB with bootstrap time of approximately four days for adding a new node [12]. Such large storage requirements may eventually result in few large businesses to take control of majority of the nodes and may cheat whereas the other nodes are not able to detect this fraud [36]. These large blockchains, ever growing bigger with new data nodes, may become unwieldy in terms of loading, computing, and synchronizing data and may bring big problems to client running the Blockchain based system [16]. On-chain scaling and off-chain scaling (state channels) are some of the suggested techniques to address the scalability issue, but these are in very early stages and unproven techniques [12]. Edge computing is another suggested approach to address high computational resources and storage requirements distributed at the network edge, offloading the Blockchain and mining computation from the power-limited nodes [12]. Kim *et al.* [48] provide a survey of various scalability solutions consisting of on-chain, off-chain, sidechain, child-chain, and inter-chain-based solutions [48]. Authors in [156], discuss Blockchain scalability challenges and then classify the existing scalability solutions in two layers. The first layer focuses on changing the Blockchain structure in terms of its size and second layer divides the Blockchain in multiple committees.

5) PERFORMANCE ISSUES

Blockchain systems suffer from performance issues such as throughput bottleneck, transactions latency, and storage constraints [68]. For example, smart contracts in the current Blockchain systems are executed serially by miners and validators, which significantly limit the throughput [68]. Bitcoin transactions usually are verified in one hour, which is acceptable but not good enough [16]. Lightning Network [60] is a proposed solution to this problem that uses Hashed Timelock Contracts (HTLCs) with bi-directional payment channels allowing secure payments routing across multiple P2P payment channels. Blockchain community needs to explore utilization of today's concurrent multicore and cluster architecture to address these performance issues [68]. In [154] authors have performed a systematic study of performance evaluation of Blockchain exiting solutions using empirical evaluation methods including experimental analysis and benchmarking. They also suggest recommendations to optimize performance of Blockchain-based systems.

6) COST OF DECENTRALIZATION

Even though decentralization is considered one of the most important characteristics of Blockchain, it is not without a cost. For example, there is the open issue of consensus algorithms balancing between security and resource efficiency regarding adaptively controlling the replication factor in shards [67]. Moreover, append-only chains with historical data, such as spent transactions, will continue to grow to sizes that ordinary nodes will eventually run out of storage and the Blockchain network may by controlled by few powerful nodes [67]. One of the possible solutions is to investigate pruning out-of-date blocks that need to be forgotten without compromising its immutability [37]. However, except for some experimental work [35] and [59], the data pruning problem remains an open issue [67]. Another important aspect of cost is the monitory cost of using public Blockchain.

7) IRREVERSIBLE BUGS

Due to the immutability of the Blockchain, if deployed smart contracts have any bugs, there is no direct way to fix these bugs [68]. There is no easy way to patch a buggy smart contract without reversing the Blockchain which is a significantly daunting task [51]. Even if there is a way to update the defect, when a new version of an existing contract is deployed, there is no way to automatically transfer data stored in the previous version and the data needs to be manually updated in the new contract which makes it quite unwieldly [68]. Hence, properly designing safe smart contracts using software engineering principles and verification before deployment is critical [38] and [51].

8) ENERGY INEFFICIENT

The Blockchain proof of work (PoW) consensus approach for Bitcoin is an energy inefficient approach since the power spent to reach consensus using the PoW approach is almost 15.77-Terawatt hour, which is 0.08% of world's electricity consumption [63]. Most of this power is spent in computing the irreversible SHA256 hashing function [63]. Furthermore, the resource-intensive design of the Blockchain system to verify its transactions and the inefficient use of scarce energy resources for these financial activities is a serious threat for the global climate due to the greenhouse gas emissions [65].

9) ATTACKS ON BLOCKCHAIN INTEGRITY

Despite high security characteristic of the Blockchain systems, these systems are still prone to several security and data integrity attacks. These attacks may consist of PoW consensus related such as 51% majority manipulation [41], consensus delay due to distributed denial of service [44] and [58], selfish mining, pollution log, Blockchain forking, orphaned blocks, de-anonymization, and block ingestion [64], double spending attacks [58], and liveness attacks [89].

10) CENTRALIZATION ASPECTS

Even though Blockchain is inherently mostly decentralized, there are still centralized aspects such as cryptocurrency exchanges that may result in vulnerability for hackers'

TABLE 2. Unified Blockchain Characteristics and Related Issues.

Unified Terminology	Mapped Terminology in Literature	Related Issues/Challenges
Decentralization	Decentralization [16] [51] [71] [72] [12] [74]	- Complex security control - Resource inefficiency - High resource needs - Long and out-of-date chains pruning - Low performance due to transaction latency & throughput bottlenecks - Energy inefficient - Scalability
Transparency	Transparency [51][71][12] Auditability [42] [74] Openness [72]	- Privacy concerns - Opposite of anonymity
Autonomy	Autonomy [16] Trustlessness [72] Trust-Free [71]	- Few large corporations overtaking decision making based on computing power
Security	Security [72][42][71]	- Various types of attacks
Immutability	Immutability [42][16][71][12] Persistency [74] Unforgeable [51] Untamperability [72]	- Irreversible bugs in smart contracts - Cumbersome deployment of smart contracts patches - Hinderance in some application domain such as health care privacy of patients
Anonymity	Anonymity [16] [51][72] [74] Transactional Privacy [42] Pseudonymity [71]	- Lack of transparency about actual users involved in transactions
Democratized	Democratized [71] Persistency [74] Collective Maintainability [72] Synchronized through Consensus [12]	- Low performance due to large number of nodes involved in decision making - Few large corporations overtaking decision making based on computing power
Integrity	Integrity [12] Reliable Database [72] Data Reliability & Integrity [42][71]	- Various types of attacks
Programmability	Programmability [42][71] [72] Open Source [16] Openness [51] Blockchain-Based Control [12]	- Non-friendly user interface
Fault Tolerance	Fault Tolerance [33][42][53]	- Duplication of data at multiple nodes resulting in high storage requirements - Overhead of synchronizing all nodes for any updates
Automatic	Automatic [71] Independence [51]	- Irreversible bugs in smart contracts - Cumbersome deployment of smart contracts patches - Prone to hacks and attacks as any other computer software

attacks. Hackers can attack the single point of cryptocurrency exchanges to gain access [57]. These hacks have given rise to consideration for decentralized exchanges that do not store funds in a centralized location but rather promotes P2P cryptocurrency trading which are more resistant to such hacking attacks.

11) IMMUTABILITY HINDERANCE

Immutability feature of Blockchain may cause hinderance in the use of Blockchain in some applications. If used in the healthcare domain, for instance, the immutability feature may hinder implementation of the privacy laws which requires that an individual has a right to request their personal health data to be erased and not visible to others [40]. This is a sensitive issue and application of Blockchain for healthcare cannot be done without addressing this legal obligation [40]. A summary of characteristics, mapping of related terminologies in literature and relevant issues are shown in the Table 2.

III. EVOLUTION AND TYPES OF BLOCKCHAIN

In this section, we classify Blockchain technology evolution in three versions.

12) EVOLUTION

The Blockchain 1.0 technology as part of Bitcoin is associated with an unknown company identified by a tag ''Satoshi Nakamoto'' from 2008 [1]. Bitcoin used Blockchain 1.0 as a way to solve the long-existed problems of double spending of digital cash and processing of digital transactions without the need of any trusted third party as described below:

13) TRANSACTION PROCESSING

For long time, the financial institutions have been relying on trusted third parties for processing electronic payments. These third parties provide mediation for disputes between merchants and customers. These third parties spend time to provide additional information to customers and reversing the transactions if required. It can increase the cost per

transaction and limit the transactions carried out for a merchant within a specific time however, there is no other mechanism to make payments over communication channel without a trusted third party. Blockchain provides a way to the willing parties to make transaction directly with each other without any existing trusted third party. The money of stakeholders is protected by providing a cryptographic proof instead of any already existing trusted party [1].

14) DOUBLE SPENDING PROBLEMS

The online payment system has been there for long time with inherent problem of double spending. The double spending problem is a potential flaw in online payment systems where same digital money can be spent more than one time to make different transactions. This becomes possible by exploiting the implementation details of saving money in the form of duplicated file or by providing falsified information [7].

Blockchain in cryptocurrencies is used as a public ledger to store all the transactions happening. Transactions are stored as a data structure in Blockchain called Blocks (described in detail in section 4 in this paper). New blocks are constantly added as transactions happen, thus continuously expanding the Blockchain.

Cryptocurrencies are considered the first application of Blockchain and have already been functional as a digital payment system on the Internet. With the ability of programming cryptocurrency as a network of decentralized trading of all resources, it had already been extended into Blockchain 2.0 to take advantage of more robust functionality of digital money.

Blockchain 2.0 was the next big tier in the development of Blockchain industry and is termed as ''Smart Contracts''. It is a concept for the decentralization of markets in general and support for transfer of many different kinds of assets like stocks, bonds, loans, mortgages, smart properties etc., beyond digital currency [7]. It was developed as a way to automatically enforce the rules agreed between interested parties like traditional business contracts. With the advancement in technology, it was realized that Blockchain can revolutionize all industries rather than just markets, payments, financial services and economies. This gave birth to Blockchain 3.0 called Blockchain Applications beyond financial markets in areas including government, health, literature and culture and so on [7].

Blockchain 3.0 is a platform to develop distributed and secure applications for all industries beyond the monetary markets. It supports a universal and global scope and scale by interconnection with the web technology. It is being seen as platform to contribute for the development of ''Smart World'', especially for resource allocation of physical-world and human assets [8], [9].

A. TYPES OF BLOCKCHAIN

Blockchains are classified into multiple types based on their usage and distinct attributes. All types of Blockchain examples are presented in all versions of Blockchain including cryptocurrencies like Bitcoin, smart contracts like Ethereum, and Blockchain applications like health sector.

1) PERMISSIONLESS OR PUBLIC BLOCKCHAIN

In permissionless or public Blockchain, system participants do not need any permission to join the network [10]. This Blockchain is truly decentralized as participants can participate in consensus process, read and send transactions and maintain the shared ledger [9]. New blocks can be published, accessed and validated by all participants thus they can maintain a copy of the complete Blockchain [8].

Public blockchains are secure in formation and operation. Though any participant can join the network and add transactions as blocks, these blocks are verified by computationally expensive consensus processes like puzzle solving or stacking one's own cryptocurrency. The tampering of the contents of blocks is protected by hashes and decentralized consensus. Also, a large number of nodes can be anonymous in Blockchain to protect their privacy [8].

Besides many benefits, public blockchains also have many open research issues as well. The challenges of achieving efficiency are influenced by the large number of participants and computationally expensive consensus mechanisms [10].

2) PERMISSIONED OR PRIVATE BLOCKCHAIN

Permissioned or private blockchains are designed for a single organization. Participants are allowed to join the network by invitation and play specific role to maintain the Blockchain in decentralized manner [10]. The private blockchains are different from public blockchains as only authorized entities are allowed to join the network and maintain the blocks [9].

Permissioned blockchains are considered more secure and efficient than public ones as only known participants join the network and tampering is similarly protected by hashes and consensus of participants as in the case of public blockchains. However, nodes in private blockchains are not anonymous [9]. The open research issues in private blockchains are related to tampering of blocks and network being hacked by internal authorized participants.

3) CONSORTIUM BLOCKCHAIN

Consortium blockchains are also private blockchains but are meant for multiple organizations. Only invited and trusted participants are allowed to join and maintain the network. The consensus process in this type is relatively slow as compared to private blockchains, but faster than public blockchains [10]. For security, consortium blockchains handle information in more protected way for alteration as compared to private blockchains. The hacking is also protected better in this type of Blockchain based on better security measures due to participants from multiple organizations [10].

IV. ARCHITECTURE OF BLOCKCHAIN

4) ARCHITECTURE OF BLOCKCHAIN 1.0 (CRYPTOCURRENCIES)

Blockchain 1.0 is a distributed ledger to store the digital cash transactions between two parties efficiently. The transactions

are stored as a growing list of records called ''Blocks''. These blocks are resistant to any modification in them and are verifiable in a permanent way. A group of users joined together by a P2P network typically manages the verification of the ledger records. In order to make any changes within blocks, a consensus is required between more than half of the users of the network. This section discusses the details of design, working and open research issues of these components of Blockchain including blocks, network and consensus.

5) BLOCK

A block is the data structure in Blockchain 1.0 to store transaction records. As shown in the Figure 3, it consists of two parts: 1) Block Header and 2) Block Body. The block header contains following fields:

- Block Version: specifies the rules for block validation.
- Merkle Tree Root Hash: it stores the hash value of all transactions in the block.
- Time Stamp: stamps the current time in seconds according to universal time since January 1, 1970.
- nBits: threshold for a valid block hash.
- Nonce: a mathematical value starts with 0 and increases with calculation of every hash.
- Parent Block Hash: points to the previous block.

The block body contains the transactions and transaction counter. The maximum capacity of block to store the transactions is determined by the block size and size of each transaction contained in it.

6) NETWORK

In general, there are two types of nodes in a Blockchain network: 1) Full node 2) Lightweight node. However, authors in [1] have further categorized these nodes based on their functionalities which is illustrated in Figure 4.

a: FULL NODE

The full node is a fully functional node in the Blockchain network that performs role of the server. The full node has the capability to store copy of Blockchain nodes data and history of Blockchain. In case of a transaction in Blockchain network, full node is responsible to maintain consensus among other nodes by applying consensus algorithm and verify the transaction. It also participates in future policy and decision making.

b: PRUNED NODE

This is a kind of reduced function nodes as compared to the archival node. It is easier to understand from recalling the blocks in Blockchain architecture [74]. The pruned nodes in the Blockchain have a set limit of block storage. These nodes keep the blocks information from the starts, but when they reach the set limit, they only retain the header of blocks and chain placement.

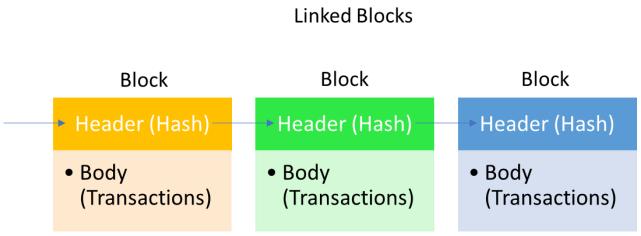


FIGURE 3. Blocks in the Blockchain architecture [74].

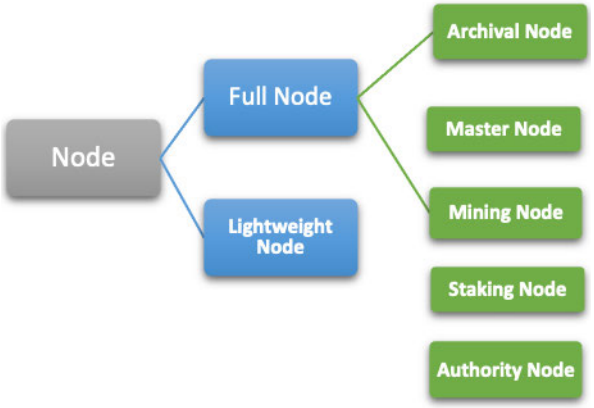


FIGURE 4. Categorization of Blockchain nodes [73].

c: ARCHIVAL NODE

It is a fully capable node in terms of space utilization. They can be seen as full server that can host all Blockchain. These nodes have the capability to add blocks in the Blockchain, validate blocks, and enforce consensus essential for a Blockchain transaction.

d: MINER NODES

All of the transactions are validated through special nodes, called 'miners' [75]. Miner nodes perform the required tasks to add a block in the network as long as all other nodes agree. After this consensus the transaction is stored in a decentralized node. In a public Blockchain these nodes can earn by validating the transaction.

e: STAKING NODE

Cryptocurrency Blockchain has a concept of staking node. This node determines based on rules and chance (proof of luck [76]) that which node will create next block in the Blockchain to get rewarded. The proof of work algorithm [77] decides which node will be rewarded. Cryptocurrency node such as raspberry pi cryptocurrency node [78] can also be considered as an example of this node.

f: AUTHORITY NODE

Nodes in the Blockchain network that will implement consensus algorithm or Proof-of-Authority are generally recognized as authority nodes in the network [73].

g: MASTER NODE

Master node in Blockchain network keeps full record of the transaction and validate them. Master nodes are also considered as back-end nodes of the network, which provide proof-of-stakes for cryptocurrency network [79]. Master nodes can also be considered as wallet running on millions of computers enabling the Blockchain up and running at real-time.

h: LIGHTWEIGHT NODE

A lightweight node is also considered as simple payment verification node [73]. According to authors in [80], lightweight nodes are becoming increasing feasible for Blockchain deployment because of their less resource consumption. Authors in [80] highlight the issue of reward for lightweight node and nothing for full node who serve lightweight client in Blockchain network. The authors suggest that smart contract can provide fair deployment environment. They suggest a unifying mechanism SmartLight that integrates payment routine to reward full node for serving lightweight client in the Blockchain network.

i: CONSENSUS

The Consensus is required to validate transaction and to update ledger. The first consensus algorithm used in Blockchain 1.0 was Proof-of-Work.

7) PROOF-OF-WORK (PoW)

PoW is considered as main achievement of Bitcoin to reach consensus in a distributed decentralized Blockchain network that could consists of 1000 of nodes. Consensus algorithm decides how agreement is made between Blockchain nodes to append a new block in the chain and the verification process. To add a block and earn reward in PoW algorithm, the initiator node applies cryptographic algorithm to produce a winning value less than the set value of network. In case of more than one node producing value, then this situation is dealt by analyzing the maximum value of PoW, which represents the higher amount of work done by the node. This node then allows to add a block and earn reward. This method is more suitable for scalable Blockchain network. However, it has few drawbacks including the cost of equipment's for node to perform mining, low transaction rate and its vulnerability to be attacked. More consensus algorithms are described in detail in section 6 of this paper.

8) ARCHITECTURE OF BLOCKCHAIN 2.0 (SMART CONTRACTS)

The concept of Smart Contracts is also not new and existing in literature since 1994. It is defined as ''a computerized transaction protocol that executes the terms of a contract''. The vision was to translate contractual clauses (collateral, bonding, etc.) into code and implement them in the form of software or hardware to self-enforce them with minimal role of trusted intermediaries [23].

In terms of Blockchain, smart contract automatically enforces agreements between two or more parties without a trusted intermediary. These smart contracts are implanted as computer programs in Blockchain softwares like Ethereum and Hyperledger. Participants join the network depending upon the type of Blockchain and can request the execution of a particular contract for a transaction in the Blockchain P2P network. The history of these transactions is stored in Blockchain similar to digital currencies. The state of the contract and assets of participants are determined by the sequence of transaction in the Blockchain [142].

The correct execution of smart contracts does not rely on a trusted third party similar to cryptocurrencies. Consensus protocols [157] are there to resolve any potential conflict between contractual parties. There are different consensus algorithms available for conflict resolution depending on the platform [142].

1) Block

The blocks in smart contracts contain programming code for recording transaction for a particular contract. The further details of the design of blocks are same as for cryptocurrencies as discussed in section 4A.

2) Network

The types of nodes present in smart contract P2P network are same as described in section 4A. The permissions for nodes to join the network are dependent on type of Blockchain implementation from public, private or consortium choices.

3) Consensus

The consensus mechanism in smart contracts is used to resolve any dispute between participants and recording transactions for a particular contract. Different available platforms or frameworks for smart contracts (see section 7 for more details) implement different consensus algorithms (details of different consensus algorithms are available in section 6).

9) ARCHITECTURE OF BLOCKCHAIN 3.0 (BLOCKCHAIN APPLICATIONS)

Besides financial market, the Blockchain technology has been adopted in many industries for development of distributed applications e.g., games, user-generated content networks, internet of things (IoT), smart hardware, supply chain, source tracing and economy sharing credits etc. Blockchain technology provides many features to these distributed applications including better performance in terms of low latency and high throughput, simpler identity management and enabling them for offline transactions and flexible maintainability for system upgrades and easy bug recovery [10]. There are some novel applications of Blockchain and some are briefly reviewed, for example, authors in [153] claim that fusion of Blockchain technology in existing deployed cloud solution can reform cloud data centers in terms of their performance enhancement and security. Authors in [171], recently proposed the use of Blockchain for identity authentication issues in the smart grid through a secure and mutual authentication protocol. Similarly, in [173] authors first highlight

the potential security threat on smart grid infrastructure and then propose a Blockchain-based lightweight authentication protocol for the smart grid. Authors in [172] propose an efficient medical data storage and sharing mechanism using double Blockchain. From double blockchain, they mean two blockchains first one for data storage and second for data sharing between hospitals and healthcare organizations. Applications use Blockchain for their different needs e.g., verifying the identities, keeping track of manufactured items in the form of chain of item etc.

A general Blockchain architecture is presented in the literature as a layered architecture to develop distributed applications as shown in Figure 5 [9].

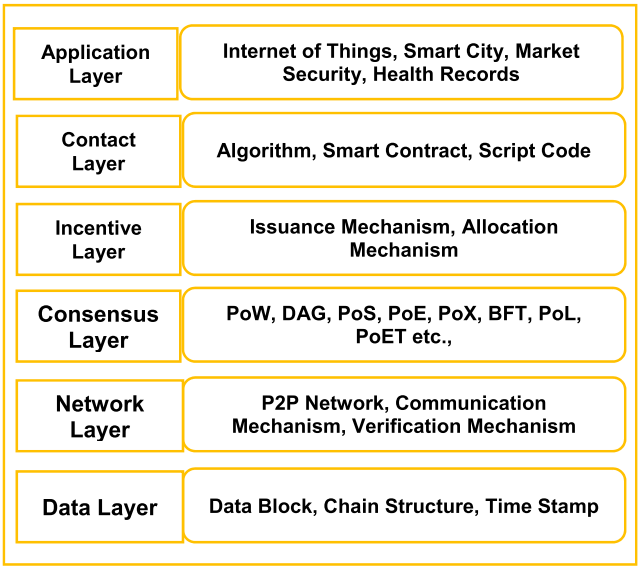


FIGURE 5. A general Blockchain Layered Architecture [9].

- Blockchain based business applications represent application layer.
- The contact layer show programming approaches available for Blockchain.
- The nodes participating in managing applications get incentives according to mechanisms listed in incentive layer.
- The consensus layer makes various consensus algorithms available for Blockchain applications.
- The network layer is composed of data propagation and data verification mechanisms along with distributed networking mechanisms.
- The timestamped data blocks are part of data layer. Chain structure, Merkle tree, cryptography and hash functions are used to manage security of these blocks.

10) BLOCKCHAIN FRAMEWORKS

Blockchain has been gaining widespread attention globally but the success of the technology depends on the availability of the application development frameworks. There are a number commercial as well as open-source application development frameworks (ADFs) available currently. The most common and widely use is Bitcoin. This section describes a number of important ADFs for developing commercial grade Blockchain applications [94], [95].

11) BITCOIN

Bitcoin has been the seminal research work to lay the foundation of Blockchain-based P2P digital currency systems [144]. Major contribution of the research on Bitcoin is the implementation of the concept of direct digital payments without relying on trusted third-party financial system. Digital signatures coupled with network timestamps transactions by constructing hashing chain exploit hash-based PoW. These interconnected blocks generate immutable distributed database records that cannot be changed without redoing the PoW. Bitcoin holds major shares in cryptocurrency world today, but there are a number of other platforms available.

12) ETHEREUM

Ethereum has been developed as open-source public Blockchain platform to implement decentralized applications (DApps) [102]. Ethereum facilitates users to develop fairly complex applications of different capabilities to perform arbitrary operations and hence it can be used to develop DApps other than Cryptocurrencies. DApps actually exploit smart contracts, a small immutable program stored in Ethereum network, to represent resources such as currency, land and house. The central component of this platform is Ethereum virtual machine (EVM) to run DApps for complex algorithms. The code for DApps is written in a contract-oriented programming language Solidity [103].

13) HYPERLEDGER

Hyperledger fabric has been introduced as permissioned Blockchain distributed operating system by IBM [85]. This hyperledger fabric is unique in a sense that it's a first programmable framework Blockchain system that allows user to run distributed application independent of native cryptocurrency. The authors in [85] firsts identified the limitation of order-execute architecture such as sequential execution, nondeterministic code & confidentiality of execution. Hyperledger fabric introduces execute-order-validate Blockchain architecture as shown in Figure 6. This proposal from the IBM became popular in Blockchain community. However, authors in [86] highlighted concerns in hyperledger fabric or Blockchain technology. The first is that they cannot use permission-less Blockchain, secondly lack of proven use cases and limited number of programmers that can develop applications using this hyperledger fabric.

The core theme behind Hyperledger project is to develop open-source Blockchain technology framework and the code base to be used by a large number of users from the different industries for heterogeneous application requirements [104]. The Hyperledger project is managed by the Linux foundation in cooperation with many industrial giants such as IBM, Hitachi, Fujitsu, NEC, Intel, and many more. The Linux Foundation adopts modular umbrella approach for

FIGURE 6. Execute-order-validate architecture [104].

Hyperledger project. At the top level, the Linux Foundation and Hyperledger provide support to build the infrastructure. Technical, legal, and marketing support is included in this infrastructure development task. Furthermore, below the infrastructure layer, is the Hyperledger's development and implementation of Fabric, Iroha, Sawtooth, Burrow, Grid, and Indy frameworks to cope with heterogeneous application requirements. The third layer in the Hyperledger project is tool support. A number of tools have been developed for these frameworks such as Composer, Explorer, Caliper, Cello, Quilt and Ursa. These tools have been developed based on a specific framework but gradually they are being modified to achieve portability to other frameworks. Composer provides an environment to facilitate block chain technology application development. Composer models business network and consolidates data from conventional systems. Explorer module can be used to develop web applications with user-centric interfaces to view status of the Blockchain application.

14) TRON

TRON is another open-source platform to realize decentralized Internet and associated infrastructure for Blockchain applications [106]. The main claim to propose TRON protocol is to provide support of high throughput, high scalability, and high availability for all DApps in the TRON ecosystem. The architectural design of the TRON consists of three layers, namely storage, core, and application layers. The TRON protocol is language neutral as it uses Google Protobuf. Core layer consists of a number of modules such as smart contracts, account management, and consensus. TRON has a stack-based virtual machine implementation with optimized instruction set. Solidity programming language can be used to develop DApps. A distributed storage protocol comprising of Block Storage and State Storage has been developed for the TRON. Google's LevelDB, an open-source on-disk key-value graph store, has been selected as storage to achieve high performance for the applications. All newly created fork chains can be stored for a certain period of time into a full-node memory database namely KhaosDB.

15) MULTICHAIN

MultiChain is a platform for designing and implementing private Blockchain applications. It helps easy to develop and deploy applications within an organization or between organizations in financial sectors [107]. Fundamentally, as a private Blockchain technology, it copes with the issues of mining, privacy and openness by managing user permissions at global level. In MultiChain, no one but participants can view the Blockchain's activity with full control over transactions. Moreover, proof of work is not needed for mining which minimizes the costs. MultiChain is available on Windows, Linux and Mac servers with a simple API and command line interface. Scalability is one prime requirement for many block chain applications and MultiChain addresses this issue by controlling the block size. Special metadata is used in network transactions to grant privileges to participants in MultiChain. All privileges are granted to the miner of the first ''genesis'' block and this user acts as the first administrator with sole authority for delegating privileges.

16) OPENCHAIN

OpenChain is one of the most popular open source Blockchain frameworks with focus to achieve interoperability with existing applications by supporting highly scalable Blockchain application developments [108], [109]. Interoperability essentially means that OpenChain presents unique decentralized application gateway for pluggable integration with existing applications' backend [109]. This is a significant technology achievement with the capability to promote mainstream adoption of Blockchain applications development and deployment. In order to achieve high scalability, OpenChain exploits multi-threading and data parallelization through OPEN Blockchain Load Balancing Protocol and ORapid consensus. In OpenChain, Scaffold, a new technology concept, constitute payment schema for an application, which is transformed into OPEN state in the Blockchain application [108]. OpenChain supports heterogeneous Blockchain platform and hence an application deployed on OpenCahin is essentially deployed on other Blockchain platforms with their own consensus algorithm through OPEN cluster. At the start of the transaction processing in the OpenChain, ORapid consensus technique has the capacity to handle fairly high volume of the transactions. However, while the number of transactions increases to the limit of the techniques, OpenChain executes OPEN Blockchain Load Balancing Protocol to dispatch transactions toward other blockchains and hence archives data parallelization at very large scale.

17) QUORUM

Quorum is permissioned Blockchain open-source platform supported by J P Morgan, one of largest financial institutions on the globe [110]. Indeed, the support of J P Morgan for the Blockchain technology Quorum is based on the Ethereum codebase, but unlike Ethereum it provides permissioned Blockchain platform with enhanced contract privacy and high-performance applications [111]. The baseline functional model of Quorum is very similar to Ethereum, but with substantial difference in the Network and peer permissions management, greater transaction and contract privacy, voting-based consensus mechanisms and performance.

18) IOTA

IOTA is open source Blockchain platform for Internet of Things (IoT) to facilitate secure communication and payment [112]. It is a Blockchain platform for IoT which employs DAG (Directed Acyclic Graph). Figure 7 illustrates

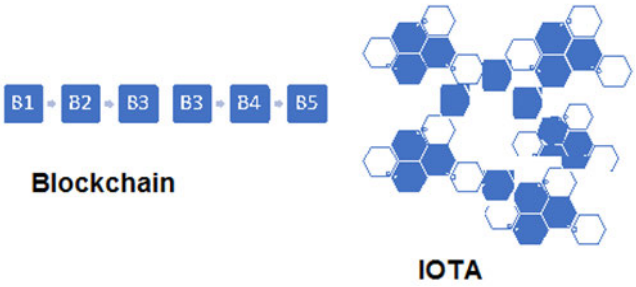


FIGURE 7. IOTA vs Bitcoin technology [24].

both IOTA DAG and Bitcoin Blockchain based technology [23].

19) EXONUM

Exonum is an open-source application development framework for developing heterogeneous domain such as legal, financial and governmental fields [113] and [114]. The framework targets permissioned Blockchain applications in these domains and its core has been developed in Rust programming language based on service-oriented architecture. Java Binding tool for Exonum facilitates application services development on the Exonum framework for permissioned blockchains.

Few more promising Blockchain frameworks are proposed recently including Corda and Ripple. In the presence of a large number of frameworks, it is challenging to select one appropriate to satisfy application requirements. Though there can be a number of criteria but we opt the criteria given in the Table 3 to meet the users' needs [115].

A comparison of various development frameworks in terms of different characteristics and properties is shown in Table 3.

V. CONSENSUS MECHANISMS

The consensus mechanism is used for validating the transaction and to reach a consensus in effect of a transaction on ledger update. There have been various consensus models proposed in literature and are implemented by different Blockchain platforms. According to authors in [87], Quorum is the first Blockchain platform to employ different consensus model. In this section, we review, classify and compare various consensus algorithms used and proposed for Blockchain technology.

Figure 8 shows our classification of Blockchain consensus model based on the review of literature. As it can be seen from Figure 8 that consensus models are classified in eight major categories and some of them have further types based on minor variations of their working.

A. PROOF OF WORK (PoW)

Proof of Work is termed as one of pioneering consensus models for Blockchain technology. The main idea in PoW is to compete for generating new block in the Blockchain based on computational power. This algorithm requires miner to perform a computation and produce a value. The wining value is less than the predefine value set by the network. In PoW, there is a possibility of forking (i.e., two nodes produce wining value), which is dealt by the network by proof of work through the nodes. Research community has proposed different variations of PoW algorithms, which are highlighted in our classification in Figure 8.

1) PROOF OF WEIGHT

Proof of Weight consensus [145] model is based on Algorand consensus that has an additional feature of ''weight'' in the core idea of PoW. These weights are relative to the values produced by nodes to represent their contribution in the network. The main idea is to prevent problem of ''double spending'' forking by adding the feature of relative weight.

2) PROOF OF REPUTATION

Proof of reputation [146] consensus mechanism builds the reputation of a node based on its participation, transactions and assets. The node with the highest reputation value generates a new block and this block is validated by voting in the Blockchain. This mechanism allows degradation in the reputation of nodes in case of misconduct in the past and also adds to the security of the Blockchain.

3) PROOF OF SPACE

Proof of space [147] is a flavor of PoW where a node that requests service must dedicate the ample amount of disk space as compared to do the computation in PoW. Information is sent to the verifier node as a proof that ample amount of space is allocated against a service request.

4) PROOF OF HISTORY

Proof of history consensus mechanism requires node to provide a proof of history [147]. It creates a historical record to provide evidence that an event is occurred at specific time. This provides as alternative of trusting the timestamp on the transaction.

5) PROOF OF BURN

Proof of burn [148] consensus mechanism is based on the concept of burning coins to compete to mine the upcoming block in the Blockchain. Burning coins here means sending the digital currency to an address where it is irretrievable. The nodes burn more coins to increase their chances of getting selected in the lottery.

In comparison to PoW, Directed Acyclic Graph (DAG) [144] is proposed as promising Blockchain consensus technology for Internet of Things Blockchain framework namely IoTA. DAG has a prominent feature of scalability as the blocks are added in parallel in the Blockchain in DAG. It allows to add a block immediately into the ledger as they process previous transaction. DAG also deal with the issue of ''double spending'' by using effective algorithms.

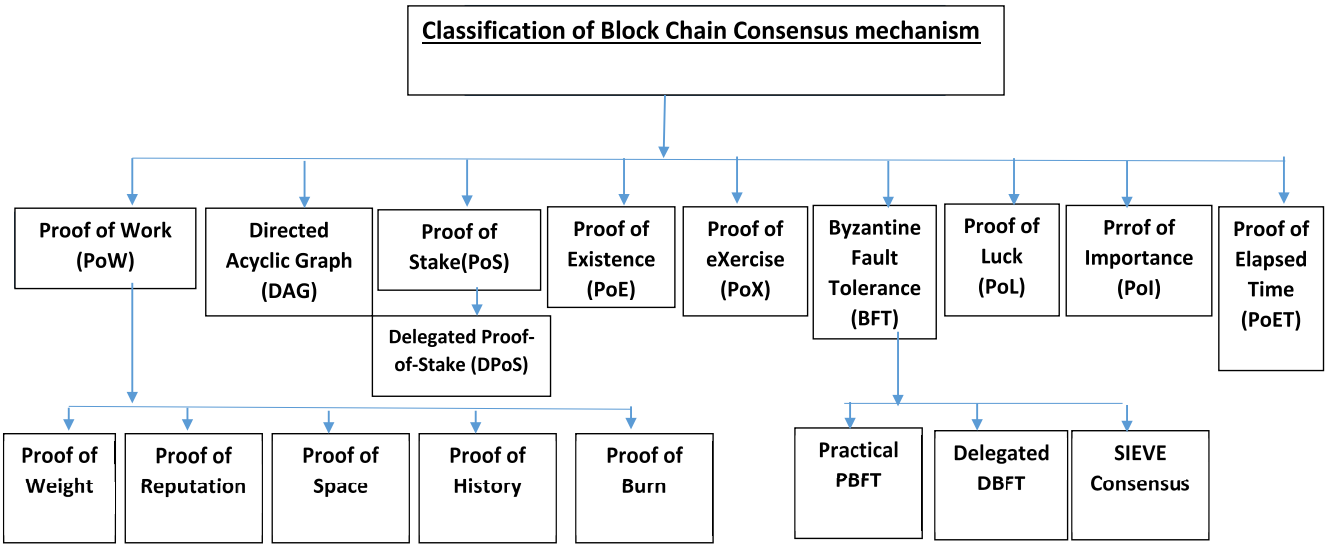


FIGURE 8. Classification of Blockchain consensus mechanisms.

TABLE 3. Comparative analysis of the Characteristics of Various Frameworks.

Framework	License(a)	Development Community (b)	Support model	Enterprise Activity	Enterprise Regulatory Compliance	Roadmap	Ease of programming	Reliable Backing
Ethereum	✓	✓	×	✓	×	✓	✓	×
Hyperledger	✓	✓	×	✓	✓	✓	×	✓
Tron	✓	✓	×	✓	✓	✓	✓	✓
MultiChain	✓	✓	✓	✓	✓	✓	✓	✓
Open Chain	✓	✓	✓	✓	✓	✓	✓	✓
Quorum	✓	✓	✓	×	✓	✓	✓	✓
IOTA	✓	✓	✓	×	×	✓	×	×
Exonum	✓	✓	✓	✓	×	✓	×	×

✓ MEANS IT IS OPEN SOURCE BUT SOME LICENSE FEE MAY BE INVOLVED UNDER CERTAIN CONDITIONS

B. PROOF OF STAKE (PoS)

The main advantage of Proof-of-Stake is that it does not require its node to purchase expensive equipment to perform mining. In PoS, a node can perform mining or validating a block based on proofing its stake i.e., number of coins. PoS suggests purchasing cryptocurrency and uses the same to buy chances of block creation [88], [89].

1) DELEGATED PROOF OF STAKE (DPoS)

A variation of PoS algorithm is proposed in [96] called Delegated Proof-of-Stake. It is suggested to use voting from stakeholders to elect the witness node, which will create block in the chain. The witness node gets payment for block creation, but if the selected witness node cannot produce block, then it will not be allowed in future voting process.

C. PROOF OF EXISTENCE (PoE)

PoE is proposed as a system to verify the existence of certain documents at specific time by timestamp of transaction. It could be used to provide data ownership information without disclosing the actual data. This PoE model is helpful in proving existence of copyright documents e.g., a patent.

D. PROOF OF eXercise (PoX)

Another alternate to the PoW is proposed by authors in [99] called Proof-of-exercise (PoX). In PoX, an exercise is a matrix based on real world scientific problem. The miners will solve matrix-based problems given by employee in the system. They suggest DNA and RNA sequencing and data comparison as an example of matrix solving problems.

E. BYZANTINE FAULT TOLERANCE (BFT)

In case of loss of system service or failure because of Byzantine fault in Blockchain require consensus [20]. The nodes in the network should reach to consensus even some nodes fail to respond and maintain consistency of this information in the Blockchain network. It is a challenge considering the distributing system.

1) PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

Authors in [93] propose "Practical Byzantine Fault Tolerance", an algorithm to deal with Byzantine faults. To efficiently survive Byzantine faults in asynchronous network, the authors in [93] propose first state-machine

replication protocol. They consider distributed file system and implement Byzantine fault tolerance.

2) DELEGATE BYZANTINE FAULT TOLERANCE (DBFT)

NEO whitepaper presents a variation of standard Byzantine Fault Tolerance called delegated byzantine fault tolerance [97]. It is currently used by the NEO Blockchain core library. They suggest it as a novel mathematical model that can verify consensus behavior using a discrete model. This can deal with untrustworthy participants better than other algorithms.

3) SIEVE CONSENSUS

Sieve [149] is considered a type of Practical Byzantine Fault Tolerance (PBFT) consensus to deal with non-deterministic chain code execution. Different output can be produced in non-deterministic chain code execution by replicas. Sieve can analyze the output in case of minor divergence detected in small number of replicas.

F. PROOF OF LUCK (PoL)

Authors in [98] have considered the limitations of PoW and proposed a new consensus model called Proof-of-Luck to reduce the required computational power for a transaction and increase its throughput. This algorithm is based on TEE (trusted execution environment). It mainly consists of two functions PollRound and PollMine. A luck value a random number between 0 and 1 is assigned to each block as it is mined. A cumulative luck value is calculated through summation of all luck values within each block of the chain. Miner will prefer to append their block to the chain with highest luck value.

G. PROOF OF IMPORTANCE (PoI)

This algorithm is used by NEM (XEM) [101]. This cryptocurrency introduces the concept of harvesting which is similar to mining. This algorithm uses the concept of network theory to define rating of each account mainly based on vested and unvested coins. PoI relies on a number of days' coins are in the account of a node in the network to estimate ''importance''. It allows 10% of current unvested amount vests every day. It is also calculated based on the rank of account within the network considering the number of vested coins held.

H. PROOF OF ELAPSED TIME (PoET)

This consensus mode uses lottery-based election model to randomly select the new leader for adding block in the Blockchain. Trusted Execution Environment (TEE) is used to ensure secure environment for this process of election. The major steps in the process of election of leader are as follows:

- Validator and miner nodes run TEE by Intel SGX.
- Every validator node requests a wait time
- The node with the shortest wait time wins the election to become a leader node.

Since it relies on specialized hardware, it is the main drawback of utilizing this consensus mechanism [90], [91].

Table 4 shows the comparison of consensus algorithms based on key parameters such as the prominent feature of consensus model, its fault tolerance and scalability.

VI. BLOCKCHAIN SECURITY

This section reviews various security issues and related research developments in detail.

A. CHALLENGES AND FUTURE TRENDS RELATED TO SECURITY

Blockchain utilizes a P2P network instead of a central authority such as a central bank to carry out financial transactions [122]. The fact that Blockchain is decentralized implies that an individual can verify and undertake financial transactions in real-time. Over the recent past, researchers have managed to invent several Blockchain applications. Nevertheless, Bitcoin has been exposed to a wide variety of privacy and security issues. For instance, after an individual links a public key with a person's identity, he can browse previous transactions on the Blockchain and examine all transactions related to the specific public key. Therefore, the main challenge is balancing the privacy and security of an individual and accountability [163]. Authors in [162] study Blockchain-based identity management systems.

According to [118], it is estimated that Blockchain technology firms will earn a revenue of more than six billion by the year 2020. However, these earnings may be affected by the vulnerabilities that are present in the Blockchain security and this factor is yet to be tackled by the distributed ledger technology (DLT) [123].

The Internet of Things (IoT) usually enables a smart workforce, such as an interaction between human beings and machines, as well as machine to machine interaction [124]. Evidence indicates that although there are numerous benefits of IoT and Blockchain technologies, there are several challenges that still exist. These challenges are related to tackling the security factors and dealing with privacy concerns. In addition to privacy and security concerns, other challenges that face IoT and Blockchain technology include interoperability, legal issues, lack of standards, access control, regulatory issues, developmental issues, and emerging IoT economy issues.

Evidence indicates that most of the challenges associated with Blockchain technologies tend to be interrelated. In [123], authors argue that the security challenges associated with IoT and Blockchain technologies can be examined from the perspective of Bitcoin, which enables transactions to occur in a decentralized manner [125]. In [155], authors have performed a systematic exploration of Blockchain attack surfaces. First, they highlight various attacks on a Blockchain-based system and then explored the relationships between these attacks. Now we briefly present the most common vulnerabilities and attacks in the Blockchain system.

TABLE 4. Comparison of Consensus Algorithms.

Consensus Algorithm	Main Feature	Fault Tolerance	Power Consumption	Scalability
Proof-of-Work (PoW)	Computational Power	Low	High	High
Proof-of- Stake (PoS)	Stake (amount of coins)	<51% stake [29]	low	High
Delegated Proof-of- Stake (DPoS)	Voting to elect witness node	<51% validators	low	high
Proof-of-Elapsed Time (PoET)	Lottery based election	Yes	high	
Byzantine Fault Tolerance (BFT)	Reach consensus even some node failed to response	33% nodes being faulty	Low	low
Delegated Byzantine Fault Tolerance (DBFT) [22]	Reach consensus with untrustworthy participants	<33 % replicas [29]	medium	low
Proof-of-Importance	Estimate importance based on no of days coins in	Unknown	Low energy saving	Fair
Proof-of-Luck	Cumulative luck value	Not applicable	Reduce computational power	Does not scale well
Proof-of-eXercise (PoX)	Miner will solve matrix-based problem	Not applicable	Partial energy saving	Un known
Proof-of-Existence (PoE)	Use timestamp of transaction to verify existence of document	Not applicable	Unknown	Unknown
Directed Acyclic Graph (DAG)	Consensus for IoT Blockchain	Not applicable	High	Very high

B. 51% VULNERABILITY

Blockchain depends on a disseminated agreement mechanism to create a common trust. Nonetheless, the mechanism of consensus has a vulnerability of 51%, which attackers might exploit to manage the whole Blockchain. Most notably, in blockchains based on PoW, in case a miner's hashing control is accountable to above 50% of the entire hashing control of the whole Blockchain, then a launch of 51% might occur. Therefore, the concentration on mining power on a small number of mining pools might lead to uncertainties of unintended situations, for example, a pool being in charge of over half of the entire computing control. After the *ghash.io* pool in January 2014 reached 42 percent of the entire computing control of Bitcoin, many minors willingly left the pool, and a press announcement was issued by ghash.io to give the Bitcoin community reassurance of its avoidance in getting to the threshold of 51%. In blockchains based on PoS, there is a probability of an attack of 51% if the coin's figures being in possession by one miner is above 50% of the whole Blockchain.

Through the launch of the 51% attack, the information on Blockchain might be arbitrarily manipulated and modified by an invader. Specifically, vulnerability can be exploited by an invader to perform the attacks given below:

1) Overturn operation and start twofold spending strike (similar coins are used numerous times).
2) Eliminate and adjust transactions ordering.
3) Obstruct normal operations of mining for additional miners.
4) Hamper the operation's confirmation of ordinary transactions.

C. PRIVATE KEY SECURITY

When utilizing Blockchain, the private key of the user is considered as credentials of recognition as well as security, which the user generates and maintains rather than intermediary agencies. For instance, when building a cold storage holder in Bitcoin Blockchain, the private key must be imported by the user. A vulnerability scheme in Elliptic Curve Digital Signature Algorithm (ECSA) was discovered by which, an invader might get the private key of the user as randomness cannot be generated by it during the process of signing. It will be hard to recover the private key of the user the moment it gets lost. In case criminals steal the private key, the Blockchain account of the user will deal with the danger of others tampering with it. Because Blockchain does not rely on a centralized intermediary trusted organization, in case the private key of the user is stolen, it will be complex to trace the conduct of the criminal and salvage the Blockchain's modified information.

D. CRIMINAL ACTIVITY

Users of Bitcoin might possess numerous addresses of Bitcoin, yet the address is not related to their actual identity in real life. Hence Bitcoin is vulnerable to illegitimate activities

through certain intermediary platforms of trading that assist Bitcoin. Because the procedure is anonymous, user's conduct is difficult to trace, therefore they avoid legitimate sanctions.

E. MONEY LAUNDERING

A Dark Wallet is an application of Bitcoin that might cause the transaction of Bitcoin to be totally private. Information on transaction might be encrypted and user's legitimate coins are mixed with chaff money by the Dark Wallet. This makes money laundering easier.

F. UNDERGROUND MARKETPLACE

Inside the secretive marketplace, Bitcoin is always utilized as the legal tender. For instance, Silk Road is an international nameless marketplace that functions as unknown services, and Bitcoin is applied as its currency of exchange. The majority of merchandise being traded in the Silk Road are illegal drugs or certain items that are regulated within the ordinary world. Because global dealings make up for Silk Road major proportion, the underground market transaction is made more convenient by Bitcoin, which could lead to harm the safety of the society.

G. DOUBLE SPENDING

Though the consensus mechanism of Blockchain can authenticate transactions, it is still challenging to evade dual spending. Double spending means that consumers can use the same single digital token multiple times. For instance, an invader could control race invasion for dual payments. It is relatively easy to execute this method of attack in blockchains based on PoW since the invader might take advantage of the intermediary period between double transactions' launch as well as confirmation to initiate an attack quickly. Before the subsequent operation is mined as null, the invader has by now gotten the output of the initial transaction, leading to dual spending.

H. TRANSACTION PRIVACY LEAKAGE

It is easy to trace the behavior of the user in Blockchain, the Blockchain platform takes actions to guard the user's transaction secrecy. Zcash and Bitcoin apply one-time financial records to keep the received cryptocurrency. Furthermore, the user is required to give every transaction a private key. Thus, the invader cannot deduce if the cryptocurrency in a dissimilar transaction is acknowledged via the equivalent user. Users could include a few chaff coins (known as ''mixis'') in Montero during transaction initiation such that the invader might not deduce the connection of real coins used via the deal.

I. COMPUTATION AND MINING NODES

In the majority of present applications, nodes are simple, and the capabilities of computation are not high. Specifically, the client of Blockchain requires to remain simple to meet the reduced needs of computation. Conversely, the services of security, generally require high computation capability. Furthermore, the minor nodes of Blockchain require high power of computation. Nonetheless, the required high power of computation for the nodes contributes to the system cost. An enhanced method involves decreasing the computation need for mining and associating the powers of the mining node towards its trustworthiness or its reputation within the platform. Additionally, simpler schemes of cryptocurrency might be built to decrease the need for computation for data encryption and signing.

J. SCALABILITY

Blockchain technology is scaling better compared to contemporary centralized methods. Though, there are reports of reduced levels of performance of the technology because higher number of nodes. This remains a main challenge, particularly with applications of network safety, where numerous users require service and there is a fast scaling of the network. Also, the system dynamicity contributes to issues of scaling because there is need for nodes to regularly send transaction updates. The Hyperledger and Ethereum platform possess their individual scalability promises. Nonetheless, the operation experiments reveal that the two platforms continue to improve in certain aspects related to scalability.

K. TIME CONSUMPTION

Offering services of security require fast capabilities of processing, particularly within the existing networks, where billions of dollars can be the cost of milliseconds. Besides, mining as well as accomplishing consensus still consume time in blockchains.

L. CONFIDENTIALITY, INTEGRITY AND AUTHENTICATION

There is a considerable need for elevating privacy and security issues concerning the attributes of various IoT elements. Researchers argue that the current technology can be used to authorize, authenticate, and audit data that has been generated by these devices. Blockchain can create new foundations for both social and economic systems. Blockchain can also be described as more than just a foundation for the circulation of cryptocurrency, and it also provides a secure means of exchanging various services, goods, and transactions [131].

A decentralized strategy can provide numerous benefits in terms of information authenticity, neutrality, security, and fault tolerance. Peers in the blockchain network must contain some functionalities such as storage, routing, mining, and wallet services. Nevertheless, researchers argue that scalability and storage capacity of Blockchain has been questioned over the years. The main reason is that the chain in this technology has been expanding at a rate of one megabyte per block every ten minutes in Bitcoin [132]. Furthermore, evidence indicates that numerous copies have been stored within the nodes in the network. Manual processes have been optimized and transformed by IoT to ensure that they fit in the digital era through making resolutions from limited logs of Blockchain without dissemination of consensus. Authors in [175], proposed a covert communication

TABLE 5. Cryptographic Primitives used for Security in Blockchain.

S. No	*Name*	*Function*
1	Hash	Maps casual size information to a string of fixed size.
2	Digital Signature	Source verification
3	Zk-SNARK in Zerocash	Breaks bitcoins and gives them anonymity
4	Zero-Knowledge (Range) Proofs	Protect privacy and anonymity of transaction

system for Bitcoin, which uses Blockchain as a covert communication channel to transmit covert messages for Bitcoin. Similarly, in [176], the authors provide a scheme and theoretical support for covert communication over Blockchain using a special Bitcoin address using the tool Vanitygen.

M. COMMUNICATION OVERHEAD

The nodes in blockchain are forced to dispatch transactions regularly to revise the Access Control List or amend the information on the provenance. Conversely, the technology of Blockchain is a P2P network, where considerable operational cost is due to the traffic of the network and the processing abilities of the system. The blocks and transactions require broadcasts. Therefore, the added overhead to the network is imperative as well as a challenge. The processing and storage overhead present a challenge in adapting blockchains applications of security [133].

Evidence indicates that most of the security problems are due to the three major areas, network links, authentication, and transactions. Therefore, technologies that allow incorrect connections, and their expansion with other technologies could raise numerous security concerns. A summary of risks and related causes is shown in Table 5.

N. CRYPTOGRAPHIC PRIMITIVES

Despite the fact that numerous works of literature are dedicated to the privacy and security of Blockchain issues, there is a lack of systematic evaluation of the cryptographic primitives in blockchains. Evidence indicates that there are a number of strategies that can be used to deal with these hurdles.

Blockchain technology utilizes a decentralized architecture which implies that all devices must be connected to a network in order to corporate and interact using predefined protocols. Recent research efforts have managed to significantly improve Blockchain technology in terms of security. For instance, every person who accesses the Blockchain network is provided with a distinct identity that is directly linked to his account. Such a mechanism ensures that only the account owner performs transactions and other operations.

Analysts argue that Blockchain technologies offer decentralized privacy and security, but they use a huge amount of energy despite being exposed to computational overhead and delays. Such challenges are the main factors that are actively being tackled by experts since they are not favorable for most resource-constrained IoT devices connected to the blockchain. To solve these problems, experts have attempted to develop numerous approaches that are specifically geared towards resource utilization.

The blockchain-based smart homes work in three basic tiers which are known as an overlay network, cloud storage, and smart home. The system requires that every smart home will be equipped with a highly capable device called a ''miner.'' Such a device will have the capability of handling various forms of communications that take place within and outside the home. The miner node in the Blockchain can audit and managing all forms of communication. Researchers claim that this Blockchain-based smart home framework is capable of examining security issues such as integrity, confidentiality, and availability.

Authors in [134], suggest Bitcoin technologies provide weak anonymity, and they propose a system that can safeguard the privacy of the user in Bitcoin.

O. BLOCKCHAIN ALGORITHMS FOR SECURITY

In Blockchain, privacy is a significant issue. For example, the address of Bitcoin payer can be seen by anyone and every transaction's content in the Blockchain of Bitcoin. This can be counter by various advanced cryptographic primitives such as:

1) HASH FUNCTIONS

The hash function has two basic requirements, which are known as collision-resistance and one-way functionality. The key use of hash is to ensure data integrity for online or offline transactions. A hash function could be used to ensure that a file is downloaded from the online source is authentic. In blockchain applications, the hash functions could be used in the generation of address, PoW, bridge mechanism, generation of random or pseudo numbers (PNG), generation of the blocks, and message digest in signatures (MDS). The use of hashes in Blockchain gain popularity in cryptocurrency applications. The most commonly used hash function in blockchains is SHA256 [141].

2) DIGITAL SIGNATURE

The concept of digital signature was built in 1976 by Hellman and Diffie when they first developed the public key cryptography [141]. As a basic primitive of public-key cryptography, the applications of digital signature are used for the authentication of source, integrity, and non-repudiation [141]. The

Digital signature algorithm (DSA) ensures that the message legitimate signatures cannot be forged.

3) ZCASH, zk-SNARK

Miers *et al.* proposed Zerocoin to offer the anonymity of Bitcoin through breaking coins traces [141]. Nonetheless, the e-cash result could not sustain full-edge nameless payments, because Zerocoins utilize fixed value coins. Also, nameless coins have to be transferred by someone into coins that are nameless before payment. On the other hand, in transactions, metadata or amount cannot be hidden. Therefore, Zerocash was proposed to handle these problems. Particularly, Zerocash offers anonymity and data transaction privacy with nameless coins. Furthermore, Zerocash extensively decreases transaction's size with a coin to below a kilobyte and reduce the period of verification of a transaction below 6 minutes.

4) ZERO-KNOWLEDGE (RANGE) PROOFS

A normal concept to protect the confidentiality and anonymity of a transaction is to make them unlikable. The system of electronic cash needs to authenticate if the online payer possesses classified information similar to the address from where the cash is coming to process the transaction. It is pertinent to mention that the zero-knowledge proof was created to handle this situation.

5) MONERO RING SIGNATURE

Monero employs ring signature technology to preserve the privacy of users. Moreover, the ring signature is a type of digital signature in which a group of potential signatories is combined together to produce a distinct signature that can use to authorize a transaction [23].

VII. FUTURE PROSPECTS

This survey paper has covered architecture of cryptocurrencies, smart contracts and general Blockchain based applications. Blockchain has a great potential to revolutionize the way of doing businesses and making payments across the world without consideration of geographical boundaries and trusted intermediaries. Blockchain has also has phenomenal potential in establishing transparent, democratic and secure fabric for other industries of the world. Many aspects of all versions of Blockchain are going to remain hot research topics including consensus mechanisms, network management in terms of efficiency. Some key findings and future research directions are discussed below in this section.

The business and research community has shown incredible interest in adopting Blockchain technology in the last decade. Consensus algorithms play a vital role in ensuring consistent operations of Blockchain application. The important future direction in terms of consensus algorithms is the transition from PoW to new algorithms such as PoS. Ethereum has already started working on it and will be looking towards the implementation and performance analysis aspect of this transition. Another interesting future prospect is how new Cryptocurrencies like NEM and EOS will motivate business to build Blockchain solutions using new consensus algorithms.

For the Blockchain technology to become mainstay technology of the future for varying domains, it must resolve several current issues. First, the Blockchain technology needs to become scalable and must solve the limitations of low throughput, high latency, and increasingly high storage demands. For example, it needs to investigate significantly improving transaction execution performance by exploiting high concurrency of multicore and cluster architectures. The resource inefficiency and monopoly by large organizations with powerful nodes can be addressed by investigating controlling chain sizes by pruning out-of-date and unneeded blocks without affecting immutability. The efficient deployment of updated smart contracts without much overhead is another issue for the research community to solve. Finally, the Blockchain community must eventually address environmental effects from the high energy consumption of a large number of nodes participating in reaching consensus, which may become a serious global climate issue.

Microsoft and Intel have already joined hands to support enterprise Blockchain [158] and the alliance believes that enterprise Blockchain success needs to cater the performance, confidentiality and governance issues [116]. ADFs essentially need to integrate support for these issues to have wider acceptability in various business domains. Blockchain technology has given rise to autonomous trust management in a decentralized way between two concerned parties in the form of smart contracts while artificial intelligence (AI) paves the way for intelligent decision-making for machines at par with humans, and even in some cases with more efficiency [117]. Integrated capabilities of Blockchain and AI have great potential for emerging applications in various domains. For instance, trust of Blockchain and decision making of AI in healthcare and autonomous vehicles will result in excellent match for highly useful applications [170-173, 120]. Consequently, future ADFs will be required to provide inherent support for such functionalities.

In future, there are two major challenges in promoting Blockchain security. One is to balance the privacy and security of an individual and accountability, mainly due to DLT. The other is to address security and privacy issues brought by the IoT, such as interoperability, legal challenges, lack of standards, rights issues, regulatory issues, developmental issues, and emerging IoT economy issues, etc.

Prospects of future Blockchain projects are discussed by authors in [158] including future development directions and future trends. There are a number of novel use cases where this technology could excel in the future including energy trading [165], vehicle life cycle tracking [164], smart grid [160], and Blockchain for tax management system etc.

VIII. CONCLUSION

Blockchain is a transformational technology, which provides a basis to develop distributed and secure applications for all industries beyond the monetary markets. Due to its

vast and rapid applications development, it is envisaged that Blockchain will do for trusted transactions what the internet did for communications. After the first appearance of Bitcoin in 2008, the concept of Blockchain has got considerable attention by the research and scientific community. On the basis of detailed and comprehensive analysis of the Blockchain evolution, frameworks, architectures, security and privacy characteristics, this paper has presented a survey of relevant works and elaborated on their contributions and limitations with a critical comparative analysis. The paper has provided a perspective to describe the Blockchain architectures in relation to cryptocurrencies, smart contracts and other applications. The research advances in consensus algorithms are also highlighted with some key development and application frameworks. A detailed discussion with respect to future and open research avenues is also performed, which could help to pave the way for researchers to explore the key challenging areas in the Blockchain field.

REFERENCES

[1] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Proc. 1st Int. Conf. Peer Peer Comput.*, Linkoping, Sweden, 2001, pp. 101–102.
[2] J. R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Indianapolis, IN, USA; Wiley, 2008.
[3] B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.
[4] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[5] C. R. Merkle, "Method of providing digital signatures," U.S. Patent 4 309 569, Sep. 5, 1979.
[6] A. P. Bernstein and E. Newcomer, *Principles of Transaction Processing*, 2nd ed. Burlington, VT, USA: Morgan Kaufmann, 2009.
[7] M. Swan, *Blockchain, Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.
[8] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.
[9] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey on blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8642861, doi: 10.1109/COMST.2019.2899617.
[10] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018, doi: 10.1109/ACCESS.2018.2870644.
[11] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019, doi: 10.1109/COMST.2018.2863956.
[12] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019, doi: 10.1109/COMST.2019.2894727.
[13] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.
[14] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[15] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/j.future.2017.08.020.
[16] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, Sep. 2017, doi: 10.6633/IJNS.201709.19(5).01.
[17] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018, doi: 10.3390/s18082575.
[18] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.10016848.
[19] I. Ahmed and M. A. Shilpi, "Blockchain technology a literature survey," *Int. Res. J. Eng. Technol.*, vol. 5, no. 10, pp. 1490–1493, Oct. 2018. [Online]. Available: https://www.irjet.net/archives/V5/i10/IRJET-V5I10284.pdf
[20] W. Wang, D. T. Hoang, Z. Xiong, D. Niyato, P. Wang, P. Hu, and Y. Wen, "A survey on consensus mechanisms and mining management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019, doi: 10.1109/ACCESS.2019.2896108.
[21] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–6.
[22] M. Atzori. *Blockchain-Based Architectures for the Internet of Things: A Survey*. Accessed: 2017. [Online]. Available: https://ssrn.com/abstract=2846810
[23] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
[24] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.
[25] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[26] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.
[27] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.
[28] T. Neudecker and H. Hartenstein, "Network layer aspects of permissionless blockchains," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 838–857, 2018.
[29] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey on attacks on Ethereum smart contracts," in *Proc. 6th Int. Conf. Princ. Secur. Trust*, vol. 29, Apr. 2017, pp. 164–186.
[30] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *Int. J. Res. Eng. Technol.*, vol. 5, no. 9, pp. 1–10, Sep. 2016.
[31] Anonymous, "New kid on the blockchain," *New Scientist*, vol. 225, no. 3009, p. 7, Feb. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0262407915603219, doi: 10.1016/S0262-4079(15)60321-9.
[32] A. Banafa, "IoT and blockchain convergence: Benefits and challenges," *IEEE IoT Newslett.*, vol. 10, Jan. 2017. [Online]. Available: https://iot.ieee.org/newsletter/january-2017.html
[33] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 2017, no. 4, pp. 1–14, 2017. [Online]. Available: https://ieeexplore.ieee.org/ielx7/6287639/6514899/09184895.pdf
[34] H. Berg. *How is Blockchain Verifiable by Public and Yet Anonymous?* Accessed: May 11, 2019. [Online]. Available: https://www.quora.com/How-is-Blockchain-verifiable-by-public-and-yet-anonymous
[35] J. Bruce. *The Mini-Blockchain Scheme Rev 3*. Accessed: May 12, 2019. [Online]. Available: http://cryptonite.info/files/mbc-scheme-rev3.pdf
[36] V. Buterin. *A Next Generation Smart Contract and Decentralized Application Platform*. Accessed: May 13, 2019. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper
[37] R. Dennis, G. Owenson, and B. Aziz, "A temporal blockchain: A formal analysis," in *Proc. Int. Conf. Collaboration Technol. Syst. (CTS)*, Orlando, FL, USA, Oct. 2016, pp. 430–437.
[38] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, and R. Hierons, "Smart contracts vulnerabilities: A call for blockchain software engineering?" in *Proc. Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Campobasso, Italy, vol. 20, Mar. 2018, pp. 19–25.
[39] M. Dunjic. (Jun. 3, 2018). *Blockchain Immutability. Blessing or Curse?* Blog Article. Accessed: May 11, 2019. [Online]. Available: https://www.finextra.com/blogposting/15419/Blockchain-immutability–blessing-or-curse

[40] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K.-R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[41] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur.* Christ Church, Barbados: Springer, Mar. 2014, pp. 436–454.

[42] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[43] K. Francisco and D. Swanson, "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency," *Logistics*, vol. 2, no. 1, p. 2, Jan. 2018, doi: 10.3390/logistics2010002.

[44] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Perform. Eval.*, vol. 104, pp. 23–41, Oct. 2016.

[45] G. Irving and J. Holden, "How blockchain-timestamped protocols could improve the trustworthiness of medical science," *FResearch*, vol. 5, p. 222, Mar. 2017. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4866630/

[46] A. Javed. *Managing Data Traceability: Impact and Benefits*. Accessed: May 11, 2019. [Online]. Available: http://www.xorlogics.com/2017/04/10/managing-data-traceability-impact-and-benefits/

[47] P. Kasireddy. *ELI5: What do we Mean by 'Blockchains are Trustless'?* Accessed: May 10, 2019. [Online]. Available: https://medium.com/preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6

[48] S. Kim, Y. Kwon, and S. Cho, "A survey of scalability solutions on blockchain," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Jeju Island, South Korea, Oct. 2018, pp. 1204–1207.

[49] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Softw.*, vol. 34, no. 6, pp. 21–27, Nov. 2017.

[50] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manage.*, vol. 3, no. 4, Dec. 2018, Art. no. 1850015.

[51] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 254–269.

[52] D. Massessi. *Blockchain Consensus and Fault Tolerance in a Nutshell*. Accessed: May 12, 2019. [Online]. Available: https://medium.com/coinmonks/Blockchain-consensus-and-fault-tolerance-in-a-nutshell-765de83b8d03

[53] T. Moura and A. Gomes, "Blockchain voting and its effects on election transparency and voter confidence," in *Proc. 18th Annu. Int. Conf. Digit. Government Res.*, Staten Island, NY, USA, Jun. 2017, pp. 574–575.

[54] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[55] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *FResearch*, vol. 5, p. 2541, Oct. 2016, doi: 10.12688/f1000research.9756.1.

[56] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, Mar. 2018.

[57] S. Russolillo and E.-Y. Jeong, "Cryptocurrency exchanges are getting hacked because it's easy," *Wall Street J.*, Jul. 2018. Accessed: May 12, 2019. [Online]. Available: https://www.wsj.com/articles/why-cryptocurrency-exchange-hacks-keep-happening-1531656000

[58] S. Sayadi, S. Ben Rejeb, and Z. Choukair, "Blockchain challenges and security schemes: A survey," in *Proc. 7th Int. Conf. Commun. Netw. (ComNet)*, Hammamet, Tunisia, Nov. 2018, pp. 1–7.

[59] J. Sidhu, "Syscoin: A peer-to-peer electronic cash system with blockchain-based services for E-business," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, vol. 3, Jul. 2017, pp. 1–6.

[60] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *Proc. 19th Int. Conf. Financial Cryptogr. Data Secur.*, San Juan, Puerto Rico. Berlin, Germany: Springer, Jan. 2015, pp. 507–527.

[61] M. Swan, *Blockchain: Blueprint for a New Economy*. Newton, MA, USA: O'Reilly, 2015.

[62] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, Dalian, China, Jun. 2017, pp. 1–6.

[63] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. Njilla, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," in *Proc. IEEE 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York City, NY, USA, Oct. 2017, pp. 469–474.

[64] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, Madrid, Spain, May 2017, pp. 458–467.

[65] J. Truby, "Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies," *Energy Res. Social Sci.*, vol. 44, pp. 399–410, Oct. 2018.

[66] M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.*, Zurich, Switzerland, vol. 29, Oct. 2015, pp. 112–125.

[67] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[68] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[69] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[70] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, Feb. 2019.

[71] Y. Xinyi, Z. Yi, and Y. He, "Technical characteristics and model of blockchain," in *Proc. 10th APCA Int. Conf. Control Soft Comput. (CONTROLO)*, Jun. 2018, pp. 562–566.

[72] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE 6th Int. Congr. Big Data*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[73] J. Evans. (Jan. 10, 2019). *Blockchain Nodes: An in Depth Guide*. Nodes.com. Accessed: Mar. 13, 2019. [Online]. Available: https://nodes.com/

[74] Pluralsight. (Jan. 19, 2019). *Blockchain Architecture*. Pluralsight.com. Accessed: Mar. 13, 2019. [Online]. Available: https://www.pluralsight.com/guides/Blockchain-architecture

[75] E. J. A. Kroll, "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries," in *Proc. 12th Workshop Econ. Inf. Secur. (WEIS)*. Washington, DC, USA: Georgetown Univ., 2013, p. 11.

[76] M. Milutinovic, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. 1st Workshop Syst. Softw. Trusted Execution*, New York, NY, USA, Dec. 2016.

[77] E. J. Becker, "Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency," in *The Economics of Information Security and Privacy*. Springer, 2013, pp. 135–156.

[78] Raspnode. (Jun. 10, 2015). *DIY Raspberry Pi Cryptocurrency Node*. Raspnode. Accessed: Mar. 14, 2019. [Online]. Available: http://raspnode.com/

[79] L. Hertig. (Nov. 18, 2018). *Hidden Blockchain Opportunities (2): Masternodes & Enterprise Blockchain Hosting*. Plesk.com. Accessed: Mar. 18, 2019. [Online]. Available: https://www.plesk.com/blog/product-technology/hidden-Blockchain-opportunities-2-masternodes-enterprise-hosting/

[80] D. Gruber, W. Li, and G. Karame, "Unifying lightweight blockchain client implementations," in *Proc. Workshop Decentralized IoT Secur. Standards (DISS)*, San Diego, CA, USA, 2018.

[81] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," *AI Matters*, vol. 1, no. 2, pp. 19–21, Dec. 2014.

[82] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[83] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, "Untrusted business process monitoring and execution using blockchain," in *Proc. Int. Conf. Bus. Process Manage.* Cham, Switzerland: Springer, 2016, pp. 329–347.

[84] P. E. O'Neil, "The escrow transactional method," *ACM Trans. Database Syst.*, vol. 11, no. 4, pp. 405–430, Dec. 1986.

[85] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, and S. Muralidharan, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Lisbon, Portugal, Apr. 2018, doi: 10.1145/3190508.3190538.
[86] A. Davies. (Aug. 18, 2018). *Pros and Cons of Hyperledger Fabric for Blockchain Networks*. DevTeam.Space. Accessed: Mar. 19, 2019. [Online]. Available: https://www.devteam.space/blog/pros-and-cons-of-hyperledger-fabric-for-Blockchain-networks/
[87] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017.
[88] P. Vasin. (2018). *Blackcoin's Proof-of-Stake Protocol V2*. Accessed: Mar. 20, 2019. [Online]. Available: https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper. pdf
[89] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake Blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA. Cham, Switzerland: Springer, 2018.
[90] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.* Cham, Switzerland: Springer, 2017.
[91] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," 2018, *arXiv:1805.02707*. [Online]. Available: http://arxiv.org/abs/1805.02707
[92] K. Driscoll, B. Hall, H. Sivencrona, and P. Zumsteg, "Byzantine fault tolerance, from theory to reality," in *Proc. Int. Conf. Comput. Saf.* Berlin, Germany: Springer, 2003.
[93] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Operating Syst. Design Implement.*, New Orlin, LA, USA, 1999.
[94] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. Int. Conv. Inf. Commun. Technol., Electron. Microelectron.*, Zagreb, Croatia, 2018.
[95] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Elsevier Future Gener. Comput.*, vol. 88, pp. 173–190, Nov. 2018.
[96] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," 2018, *arXiv:1801.10228*. [Online]. Available: https://arxiv.org/pdf/1801.10228.pdf
[97] D. Larimer, "DPOS consensus algorithm—The missing white paper," Steemit, New York, NY, USA, White Paper, 2018.
[98] V. N. C. P. L. E. Z. Igor and M. Coelho, "Delegated Byzantine fault tolerance: Technical details, challenges and perspectives," NEO, Shanghai, China, Tech. Rep., Mar. 2019, sec. 8. [Online]. Available: https://neoresearch.io/assets/yellowpaper/yellow_paper.pdf
[99] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. 1st Workshop Syst. Softw. Trusted Execution*, Trento, Itlay, Dec. 2016.
[100] A. Shoker, "Sustainable blockchain through proof of exercise," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Oct. 2017.
[101] NEM. (2018). *Investor Harvesting: Proof-of-Importance*. NEM (XEM). Accessed: Apr. 22, 2019. [Online]. Available: https://nem.io/xem/harvesting-and-poi/
[102] (2019). *Vitalik Buterin*. Accessed: May 23, 2019. [Online]. Available: http://Blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
[103] (2019). *TRON: Advanced Decentralized Blockchain Platform*. Accessed: May 23, 2019. [Online]. Available: https://tron.network/static/doc/white_paper_v_2_0.pdf
[104] *An Introduction to Hyperledger*. Accessed: May 23, 2019. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf
[105] *Hyperledger Publications*. Accessed: May 23, 2019. [Online]. Available: https://www.hyperledger.org/resources/publications
[106] *TRON*. Accessed: May 23, 2019. [Online]. Available: https://ipfs.io/ipfs/QmWh3LEWUQN8LsoHerQecmwfACXAPNKE9wigx6t9dLitmE/tron/Tron-Whitepaper-1031-V18-EN.pdf
[107] G. Greenspan. (2019). *MultiChain Private Blockchain*. Accessed: May 23, 2019. [Online]. Available: https://www.multichain.com/download/MultiChain-White-Paper.pdf
[108] *OPEN Chain: Scalability Through Data Parallelization*. Accessed: May 23, 2019. [Online]. Available: https://s3.amazonaws.com/openmoney/OPEN_Chain_-_Scalability_Through_Data_Parallelization_-_Google_Docs.pdf
[109] *OPEN Chain*. Accessed: May 23, 2019. [Online]. Available: https://drive.google.com/file/d/0B7ljBZOyjFLkYi0teUN6T3NweU1FUjVnaUVVc2M2SXE2UTI0/view
[110] *Smart Quorum*. Accessed: May 23, 2019. [Online]. Available: https://smartquorum.com/download/WhitePaperSmartQuorum.pdf
[111] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance evaluation of the quorum blockchain platform," 2018, *arXiv:1809.03421*. Accessed: May 23, 2019. [Online]. Available: http://arxiv.org/abs/1809.03421
[112] S. Popov. (2018). *The Tangle*. Accessed: May 23, 2019. [Online]. Available: https://docs.iota.org/
[113] Y. Yanovich, I. Ivashchenko, A. Ostrovsky, A. Shevchenko, A. Sidorov. (2018). *Exonum: Byzantine Fault Tolerant Protocol for Blockchains*. Accessed: May 23, 2019. [Online]. Available: https://bitfury.com/content/downloads/wp_consensus_181227.pdf
[114] *Exonum*. Accessed: May 23, 2019. [Online]. Available: https://exonum.com/doc/version/latest/
[115] *6 Blockchain Frameworks to Build Enterprise Blockchain & How to Choose Them*. Accessed: May 23, 2019. [Online]. Available: https://dreamztechusa.com/blog/6-Blockchain-frameworks-build-enterprise-Blockchain-choose/
[116] D. B. Black. (2019). *Microsoft and Intel Detail the Deep-Seated Problems With Blockchain*. Accessed: May 23, 2019. [Online]. Available: https://www.forbes.com/sites/davidblack/2019/05/13/microsoft-and-intel-detail-the-deep-seated-problems-with-Blockchain/#4a90d9c36b06
[117] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.
[118] R. Martin. *5 Blocked Security Risks and How to Reduce Them*. Accessed: Nov. 29, 2018. [Online]. Available: https://igniteoutsourcing.com/Blockchain/Blockchain-security-vulnerabilities-risks/
[119] D. He, K.-K.-R. Choo, N. Kumar, and A. Castiglione, "IEEE access special section editorial: Research challenges and opportunities in security and privacy of blockchain technologies," *IEEE Access*, vol. 6, pp. 72033–72036, 2018.
[120] Q. Wang, X. Li, and Y. Yu, "Anonymity for bitcoin from secure escrow address," *IEEE Access*, vol. 6, pp. 12336–12341, 2018.
[121] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.
[122] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Comput. Sci.*, vol. 132, pp. 1815–1823, Jan. 2018.
[123] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.
[124] J. Baumann and A. Lesoismier, "Cryptocurrencies outlook 2018. Stairway to heaven," Swiss Borg, Lausanne, Switzerland, Tech. Rep. 25, 2017.
[125] A. Narayanan, J. Bonneau, E. Felten, M. A. Andrew, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*. Princeton, NJ, USA: Princeton Univ. Press, 2016.
[126] P. D. DeVries, "An analysis of cryptocurrency, bitcoin, and the future," *Int. J. Bus. Manage. Commerce*, vol. 1, no. 2, pp. 1–3, 2016.
[127] E. Teo. (Accessed: Mar. 4, 2009). *How Do Cryptocurrencies Work?* [Online]. Available: https://skbi.smu.edu.sg/sites/default/files/skbife/HowDoCryptocurrenciesWorkErnieTeo.pdf
[128] A. P. Joshi, M. Han, and Y. Wang, "A survey on security and privacy issues of blockchain technology," *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018.
[129] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.
[130] A. Chakravorty, T. Wlodarczyk, and C. Rong, "Privacy preserving data analytics for smart homes," in in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2013, pp. 23–27.
[131] A. Dorri, S. S. Kanhare, R. Jurdak, and P. Gauravara. *Blockchain for IoT Security and Privacy: The Case Study of a Smart Home*. Accessed: Mar. 2017. [Online]. Available: https://www.researchgate.net/publication/312218574_Blockchain_for_IoT_Security_an_Privacy_The_Case_Study_of_a_Smart_Home

[132] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[133] S. He, Q. Wu, X. Luo, Z. Liang, D. Li, H. Feng, H. Zheng, and Y. Li, "A social-network-based cryptocurrency wallet-management scheme," *IEEE Access*, vol. 6, pp. 7654–7663, 2018.

[134] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "Cryptographic primitives in blockchains," *J. Netw. Comput. Appl.*, vol. 127, pp. 43–58, Feb. 2019, doi: 10.1016/j.jnca.2018.11.003.

[135] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[136] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[137] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2013, pp. 397–411.

[138] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," 2018, *arXiv:1802.06993*. Accessed: Mar. 27, 2019. [Online]. Available: http://arxiv.org/abs/1802.06993

[139] F. Alkurdi, I. Elgend, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "Blockchain in IoT security: A survey," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf.*, 2018, pp. 1–4.

[140] X. Lia, P. Jianga, T. Chenb, X. Luoa, and Q. Wenc, Dept. Comput., Hong Kong Polytech. Univ., Hong Kong Center Cybersecurity, Univ. Electron. Sci. Technol. China, Chengdu, China, Tech. Rep. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17318332

[141] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 1st Quart., 2019.

[142] N. Atzei, M. Bartoletti, T. Cimoli, S. Lande, and R. Zunino, "SoK: Unraveling Bitcoin smart contracts," in *Proc. Int. Conf. Princ. Secur. Trust*, 2018, pp. 217–242.

[143] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (PoET)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.*, 2017.

[144] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph based blockchain for Internet of Things: Performance and security analysis," 2019, *arXiv:1905.10925*. [Online]. Available: https://arxiv.org/abs/1905.10925

[145] P. Compare. *What is Proof of Weight, a Web Article Published by Coincodex*. Accessed: 2019. [Online]. Available: https://coincodex.com/article/2617/what-is-proof-of-weight/

[146] Q. Zhuang, Y. Liu, L. Chen, and Z. Ai, "Proof of reputation: A reputation-based consensus protocol for blockchain based systems," in *Proc. Int. Electron. Commun. Conf. (ACM IECC)*, Okinawa, Japan, Jul. 2019, pp. 131–138.

[147] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Proc. 35th Annu. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 2015, pp. 585–605.

[148] R. Smith. (2019). *Proof of Burn | Consensus Through Coin Destruction, Article Published by Coin Central*. [Online]. Available: https://coincentral.com/proof-of-burn/

[149] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 2017, no. 4, p. 114, 2017.

[150] *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Dec. 21, 2019. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[151] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019, doi: 10.1109/ACCESS.2019.2957660.

[152] M. S. Siddiqui, T. Ali, A. Nadeem, W. Nawaz, and S. S. Albouq, "BlockTrack-L: A lightweight blockchain-based provenance message tracking in IoT," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 4, pp. 463–470, 2020.

[153] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 2009–2030, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2989392.

[154] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126927–126950, 2020, doi: 10.1109/ACCESS.2020.3006078.

[155] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, 3rd Quart., 2020, doi: 10.1109/COMST.2020.2975999.

[156] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020, doi: 10.1109/ACCESS.2020.3007251.

[157] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020, doi: 10.1109/COMST.2020.2969706.

[158] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020, doi: 10.1109/TEM.2019.2926471.

[159] Y. Zou, T. Meng, P. Zhang, W. Zhang, and H. Li, "Focus on blockchain: A comprehensive survey on academic and application," *IEEE Access*, vol. 8, pp. 187182–187201, 2020, doi: 10.1109/ACCESS.2020.3030491.

[160] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 3–19, Jan. 2021, doi: 10.1109/TII.2020.2998479.

[161] S. E. Chang and Y. Chen, "When blockchain meets supply chain: A systematic literature review on current development and potential applications," *IEEE Access*, vol. 8, pp. 62478–62494, 2020, doi: 10.1109/ACCESS.2020.2983601.

[162] Y. Liu, D. He, S. M. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, Jun. 2020, Art. no. 102731.

[163] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[164] T. A. Syed, M. S. Siddique, A. Nadeem, A. Alzahrani, S. Jan, and M. A. K. Khattak, "A novel blockchain-based framework for vehicle life cycle tracking: An end-to-end solution," *IEEE Access*, vol. 8, pp. 111042–111063, 2020, doi: 10.1109/ACCESS.2020.3002170.

[165] T. Li, W. Zhang, N. Chen, M. Qian, and Y. Xu, "Blockchain technology based decentralized energy trading for multiple-microgrid systems," in *Proc. IEEE 3rd Conf. Energy Internet Energy Syst. Integr. (EI)*, Changsha, China, Nov. 2019, pp. 631–636, doi: 10.1109/EI247390.2019.9061928.

[166] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

[167] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[168] Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo, and L. Zhou, "On emerging family of elliptic curves to secure Internet of Things: ECC comes of age," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 3, pp. 237–248, Jun. 2017.

[169] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, M. K. Khan, M. Karuppiah, and R. Baliyani, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3527–3542, Nov. 2016.

[170] S. Wan, M. Li, G. Liu, and C. Wang, "Recent advances in consensus protocols for blockchain: A survey," *Wireless Netw.*, vol. 26, no. 8, pp. 5579–5593, Nov. 2020, doi: 10.1007/s11276-019-02195-0.

[171] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efcient mutual authentication protocol for smart grid under blockchain," *Peer Peer Netw.*, vol. 13, no. 6, pp. 1–3, Nov. 2020.

[172] Z. Lejun, P. Minghui, W. Weizheng, S. Yansen, C. Shuna, and K. Seokhoon, "Secure and efficient medical data storage and sharing scheme based on double blockchain," *Comput., Mater. Continua*, vol. 66, no. 1, pp. 499–515, 2020.

[173] W. Wang, H. Huang, L. Zhang, Z. Han, C. Qiu, and C. Su, "BlockSLAP: Blockchain-based secure and lightweight authentication protocol for smart grid," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Guangzhou University, China, Jan. 2021, pp. 1332–1338.

[174] W. Wang and C. Su, "CCBRSN: A system with high embedding capacity for covert communication in bitcoin," *ICT Systems Security and Privacy Protection* (IFIP Advances in Information and Communication Technology), vol. 580, M. Hölbl, K. Rannenberg, and T. Welzer, Eds. Cham, Switzerland: Springer, 2020.
[175] L. Zhang, Z. Zhang, W. Wang, R. Waqas, C. Zhao, S. Kim, and H. Chen, "A covert communication method using special bitcoin addresses generated by vanitygen," *Comput., Mater. Continua*, vol. 65, no. 1, pp. 597–616, 2020.

MUHAMMAD NASIR MUMTAZ BHUTTA received the B.C.S. degree (Hons.) from International Islamic University, Islamabad, Pakistan, in 2004, and the M.Sc. and Ph.D. degrees from the University of Surrey, U.K., in 2007 and 2012, respectively. He is currently working as an Assistant Professor with King Faisal University. He is an active researcher with numerous publications in international conferences and journals. He has contributed to several research projects, including three research projects funded from EADS Astrium U.K., ESA, and ESPRC U.K. He is also focusing on technical and management aspects of Cyber Security for the IoT, smart cities, and blockchain.

AMIR A. KHWAJA received the bachelor's degree in computer engineering from NED University of Engineering and Technology, Karachi, Pakistan, and the M.S. and Ph.D. degrees in computer science from Arizona State University, Arizona, USA. Since 2014, he has been an Assistant Professor with the College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia. Prior to that he had 21 years of semiconductor industry experience. He worked for 20 years at Intel Corporation, USA, in various capacities, such as a CAD Software Developer, an XScale and Atom Mobile System-on-a-Chip (SoC) Validation Architect, a Validation Program Manager, and a Senior Engineering Manager. He worked as a Principal Engineer and Senior Manager for one year at Qualcomm, San Diego, California, USA, leading the successful completion of the validation of Qualcomm's Femtocell SoC product. He has also worked as an Adjunct Faculty with Arizona State University and the University of Phoenix. He is currently serving at Qualcomm.

ADNAN NADEEM (Member, IEEE) received the Ph.D. degree from the Institute for Communication Systems, U.K., in 2011. He has been an Associate Professor and the Coordinator of MS Security Technology Program with the Faculty of Computer and Information System (FCIS), Islamic University of Madinah, KSA, since 2016. He is currently with the Federal Urdu University of Arts Science and Technology, Pakistan. For the last five years, he earned several research grants. He has published more than 50 articles in international conferences and journals, including a patent accepted and sealed by the Government of Pakistan. He has mainly worked on network layer security, QoS and reliability issues of mobile Ad Hoc, and sensors networks. He is currently focusing on Blockchain technology and the IoT applications and security. He received the 5th HEC Outstanding Research Award 2013/14 for his article published in the IEEE Communication Survey & Tutorials. During his pedagogical journey, he has received several awards and achievements, including the Foreign Ph.D. Scholarship, Associate Fellowship of Higher Education Academy (AFHEA), U.K., in 2009, and the Best Paper and Best Track Paper Award in the ICICTT 2013 and ICEET 2016 conferences, respectively. He received Nishan-e-Imtiaz for his outstanding research from Federal Urdu University, Pakistan, in August 2016. He received the Best Academic Advisor and Best Researcher Award from FCIS, Islamic University of Madinah, in 2018.

HAFIZ FAROOQ AHMAD received the Ph.D. degree in distributed computing from Tokyo Institute of Technology, Tokyo, Japan. He is currently an Associate Professor with the College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al Ahsa, Saudi Arabia. He is the pioneer for Semantic Web Application Firewall (SWAF) in cooperation with DTS Inc., Japan, in 2010. He contributed in agent cites project, a European funded research and development project for agent systems. He initiated Scalable fault tolerant Agent Grooming Environment (SAGE) Project and proposed the concept of decentralized multi agent systems SAGE back, in 2002. He has more than 100 international publications, including a book on security in sensors. His research interests include semantics systems, machine learning, health informatics, and Web application security. He has been awarded a number of national and international awards, such as the Best Researcher Award of the Year 2011 by NUST, the PSF/COMSTECH Best Researcher of the Year 2005, and the Star Laureate Award, in 2004.

MUHAMMAD KHURRAM KHAN (Senior Member, IEEE) is currently working as a Professor of cybersecurity with the Center of Excellence in Information Assurance, King Saud University, Saudi Arabia. He is the Founder and the CEO of the Global Foundation for Cyber Studies and Research, Washington DC, USA, an independent and non-partisan cybersecurity think-tank. He has published more than 400 papers in the journals and conferences of international repute. In addition, he is an Inventor of ten US/PCT patents. His research interests include cybersecurity, digital authentication, the IoT security, biometrics, multimedia security, cloud computing security, cyber policy, and technological innovation management. He is a Fellow of the IET, U.K., the BCS, U.K., and the FTRA, South Korea. He is the Vice Chair of IEEE Communications Society Saudi Chapter. He is a Distinguished Lecturer of the IEEE. He is the Editor-in-Chief of *Telecommunication Systems* (Springer-Nature) with its recent impact factor of 1.73 (JCR 2020). He has edited ten books/proceedings published by Springer-Verlag, Taylor & Francis, and IEEE. He is on the editorial board of several journals including, IEEE Communications Surveys & Tutorials, *IEEE Communications Magazine*, IEEE Internet of Things Journal, IEEE Transactions on Consumer Electronics, *Journal of Network & Computer Applications* (Elsevier), IEEE Access, *IEEE Consumer Electronics Magazine*, *PLOS One*, and *Electronic Commerce Research*.

MOATAZ A. HANIF received the master's degree in cybersecurity engineering from Embry-Riddle Aeronautical University. He is currently a Computer Engineer and AI Enthusiast. He has participated in several publications in the Blockchain field and is currently working in the cybersecurity field as IR Team Lead.

HOUBING SONG (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in August 2012, and the M.S. degree in civil engineering from the University of Texas, TX, USA, in December 2006.

In August 2017, he joined the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, FL, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab). From August 2012 to August 2017, he served on the Faculty of West Virginia University. In 2007, he was an Engineering Research Associate with the Texas A&M Transportation Institute. He is the author of more than 100 articles. His research interests include cyber-physical systems, cybersecurity and privacy, the Internet of Things, edge computing, AI/machine learning, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, USA Today, U.S. News & World Report, Fox News, Association for Unmanned Vehicle Systems International (AUVSI), Forbes, WFTV, and New Atlas.

Dr. Song is a Senior Member of ACM and an ACM Distinguished Speaker. He was a recipient of the Best Paper Award from the 12th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom-2019), the Best Paper Award from the 2nd IEEE International Conference on Industrial Internet (ICII 2019), the Best Paper Award from the 19th Integrated Communication, Navigation and Surveillance technologies (ICNS 2019) Conference, the Best Paper Award from the 6th IEEE International Conference on Cloud and Big Data Computing (CBDCom 2020), and the Best Paper Award from the 15th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2020). He has been serving as an Associate Technical Editor for IEEE Communications Magazine, since 2017, an Associate Editor for IEEE Internet of Things Journal, since 2020, and IEEE Journal on Miniaturization for Air and Space Systems (J-MASS), since 2020, and a Guest Editor for IEEE Journal on Selected Areas in Communications (J-SAC), IEEE Internet of Things Journal, *IEEE Network*, IEEE Transactions on Industrial Informatics, IEEE Sensors Journal, IEEE Transactions on Intelligent Transportation Systems, and IEEE Journal of Biomedical and Health Informatics. He is the editor of six books, including *Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things* (Elsevier, 2019), *Smart Cities: Foundations, Principles and Applications* (Hoboken, NJ: Wiley, 2017), *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications* (Chichester, UK: Wiley-IEEE Press, 2017), *Cyber-Physical Systems: Foundations, Principles and Applications* (Boston, MA: Academic Press, 2016), and *Industrial Internet of Things: Cybermanufacturing Systems* (Cham, Switzerland: Springer, 2016).

MAJED ALSHAMARI received the B.Sc. degree in computer information systems from King Faisal University, Saudi Arabia, and the M.Sc. and Ph.D. degrees in information systems from University of East Anglia, Norwich, U.K. Prior to that, he has been an Assistant Professor, since 2011. Since 2012, he has been the Dean of the College of Computer Sciences and Information Technology, King Faisal University. Since 2017, he has been an Associate Professor with the College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia. He has been leading a number of academic and scientific funded projects related to usability, HCI, and HIS. His research interests include HCI, information systems developments, and big data.

YUE CAO (Member, IEEE) received the Ph.D. degree from the Institute for Communication Systems (ICS) (formerly known as Centre for Communication Systems Research), University of Surrey, Guildford, U.K., in 2013. Further to his Ph.D. study, he had conducted research as a Research Fellow with the University of Surrey, and as an Academic Faculty with Northumbria University, Lancaster University, U.K., and Beihang University, China. He is currently a Professor with the School of Cyber Science and Engineering, Wuhan University, China. His research interests include intelligent transport systems, including e-mobility, V2X, and edge computing.

Blockchain as a General-Purpose Technology: Patentometric Evidence of Science, Technologies, and Actors

Sercan Ozcan and Serhan Unalan

***Abstract*—Blockchain is considered to be a general-purpose technology (GPT) by many scholars. However, previous studies offer no proof that Blockchain is a GPT. Thus, approximately 2500 Blockchain-related patent data are investigated by deploying the mixed-method approach, using patentometrics with the support of semi-structured interviews conducted with Blockchain experts. This article investigates six main GPT indicators: pervasiveness, improvement, spawning, prevalence, reallocation of resources, and inclusive democratization. Overall, the results demonstrate that Blockchain has not yet become a GPT, though it already shows some GPT characteristics. There are six specific findings: 1) Blockchain shows pervasive characteristics; 2) Blockchain is capable of further improvement; 3) Blockchain facilitates and encourages the creation of innovations; 4) several countries with strong R&D capabilities, particularly China and the United States, are showing the prevalence of Blockchain technology; 5) the Blockchain landscape is witnessing greater participation of "younger" companies; and 6) Blockchain is strongly related to the Information and Communication Technology domain with the potential of inclusivity and democratization. China and the United States have the potential to influence the future development of Blockchain technology. This article is assumed to be of great interest to a broad spectrum of stakeholders, such as scholars and policymakers.**

***Index Terms*—Blockchain, distributed ledger technologies, general-purpose technology, Patentometrics, technology analysis.**

I. Introduction

BLOCKCHAIN is a particular type of Distributed Ledger Technology (DLT), that is, a decentralized database with no central trusted party maintaining and storing it [1]. DLTs are expected to have a structural impact on the whole of society and the economy due to their pervasive use in various sectors [1]. The DLT (or Blockchain) is considered to be a general-purpose technology (GPT) by many scholars, such as Kane and Filippova *et al*. [1]–[3]. GPTs, such as the steam engine and the semiconductor, play the role of "enabling technologies" in multiple sectors of the economy, undergoing continual technological improvements and spurring complementary investment by the adopting sectors [4]–[6]. A body of literature, including [4], [7]–[11], investigates the GPT characteristics of various technologies.

There are currently a limited number of Blockchain-related studies published in Business and Management related domains, and very few studies can be found in Innovation [12], [13]. In the literature, such as [3], [14]–[16], many authors refer to Blockchain either as a GPT or as a key enabling technology (KET). Thus, in line with the literature, it is necessary to investigate whether and to what extent Blockchain will be the source of the next GPT. Currently, [1]–[3] and [14] are the only studies to investigate Blockchain from a GPT perspective. The findings of [1] show that Blockchain displays the main characteristics of GPT based on a qualitative assessment methodology by investigating Blockchain-oriented applications from a GPT perspective. The findings of this article are helpful but limited due to the amount of data, the generalizability of the approach and the focus area, in which the majority of the applications are being developed by small groups of entrepreneurs and individuals.

Following an investigation of GPT characteristics, consisting of pervasiveness, technological spawning and technological improvement, Filippova [3] asserts that Blockchain represents an emerging GPT; meanwhile, Filippova *et al*. [2] claim that Blockchain deserves attention as an emerging GPT as it already possesses scope for improvement in important GPT characteristics. However, this article claims that Blockchain has not yet become a GPT, although it already shows some GPT characteristics. Moreover, this article has a wider scope, encompassing six GPT characteristics, while [2] and [3] are based on a smaller number of GPT characteristics. For instance, prevalence is not considered in [2] and [3], although a number of scholars, such as [7], [9], and [17], already point to prevalence as a GPT characteristic. A methodological comparison between [2], [3] and this article shows that [2] and [3] are based solely on quantitative data, whereas this article improves the reliability and validity of the results due to the use of a mixed-method approach consisting of quantitative analysis enhanced with expert opinion.

Thus, an investigation of Blockchain with regard to its potential for GPT requires the most comprehensive approach possible, which is provided in this article, while covering different

Manuscript received June 29, 2019; revised January 30, 2020 and May 29, 2020; accepted July 8, 2020. Date of publication August 13, 2020; date of current version February 21, 2022. Review of this manuscript was arranged by Department Editor K.-K. R. Choo. *(Corresponding author: Serhan Unalan.)*

Sercan Ozcan is with Portsmouth Business School, University of Portsmouth, Portsmouth PO1 2UP, U.K., and with the Department of Engineering Management, Bahcesehir Universitesi, Istanbul 34349, Turkey, and also with the National Research University Higher School of Economics (Russian Federation), 101000 Moscow, Russia (e-mail: sercan.ozcan@port.ac.uk).

Serhan Unalan is with Portsmouth Business School, University of Portsmouth, Portsmouth PO1 2UP, U.K., and also with the Smart Cities Innovation Lab, 34435 Istanbul, Turkey (e-mail: serhan.unalan@myport.ac.uk).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEM.2020.3008859

approaches from the conceptual and methodological perspectives. Moreover, this approach is particularly important as Blockchain is counted by some studies, such as [14], as a disruptive institutional technology, which refers to two Blockchain platforms, namely 1) Backfeed and 2) Steem; however, this is not based on an empirical investigation.

Quantitative and advanced approaches, such as scientometrics (a research method for examining scientific publications) or patentometrics (a research method for examining patent documents), could be better options to establish whether the progress of Blockchain shows it to be a GPT or whether it can become a GPT. These approaches are the most widely accepted ones in the literature in terms of the technological and scientific analyses necessary to deal with a volume of data of which the purpose is to show technological diffusion, progress, and change. These quantitative approaches may have weaknesses, such as limitations to the in-depth analysis. However, these weaknesses can be reduced through qualitative approaches, such as interview analysis using expert opinion.

This article aims to understand the extent to which Blockchain technology may be considered as a GPT based on patentometrics analysis validated with five semi-structured expert interviews, but it does not claim that Blockchain may be considered as a GPT. Moreover, it emphasizes Blockchain's role in financial and social inclusion, especially important for improved social capital and Bottom of Pyramid BoP [18], which enable inclusive democratization. The Blockchain-related literature fails to use patent data with extensive analysis. This article adopted patentometrics to examine the degree of Blockchain's GPT characteristics and to validate further and deepen the patentometric results, five semi-structured interviews with Blockchain experts were conducted.

This research offers the following three distinct contributions:

1) it provides practical findings regarding Blockchain from the GPT perspective;
2) it extracts a comprehensive list of the GPT parameters based on an in-depth literature review of corresponding scholars;
3) it offers a methodological contribution by assessing Blockchain-specific patent data.

The findings of this article should be of great interest to decision-makers in the public and private sector who must decide how to deal with the associated benefits provided as well as the potential challenges posed by the appearance of Blockchain.

The rest of this article is organized as follows: Section II investigates the existing GPT and Blockchain literature and highlights the key findings. Section III introduces the mixed-method approach. Section IV presents the results and discussion; and, finally, Section V concludes this article.

II. General-Purpose Technologies

Our civilization is influenced periodically by particular technological innovations, that is, GPTs, which have a hugely disruptive impact on our civilization.

GPTs follow their technical trajectory with incremental improvements, ultimately producing newer GPTs, to find their dominant design [19], [20]. For instance, electromotive engines, based on electricity (a GPT), were technically improved over time and spawned other application areas, such as electric trams or electric locomotives, based on electric power (a GPT), as well as electric lamps, based on electric light (a GPT). These developments ultimately led to the communication revolution, that is, ICT (a GPT).

It is important to underline that GPTs do not immediately lead to improved economic productivity and growth. As pointed out in [9], [11], and [21], the emergence of a new GPT may cause a slowdown or even result in negative economic activity. The emergence of a new GPT triggers a new economic cycle, as this is not used immediately in the most productive manner possible [6]. Moreover, it usually takes years for a GPT to have a significant impact on the economy [22], [23]. A technology that shows GPT characteristics sometimes may not turn out to be a GPT due to many factors, which proves the difficulty in predicting important technologies and therefore the underinvestment in them [4].

This article is based on an extensive literature review to identify GPT-relevant parameters, while some of which can be assessed directly through quantitative measures, that is, GPT characteristic parameters, such as technology spawning, while some other GPT parameters are particularly subject to interpretation, that is, GPT-enabling parameters, such as the effect of religion or culture on Blockchain. In this context, GPT-enabling parameters were excluded, as this article investigated GPT characteristic parameters caused by Blockchain, which is measured quantitatively.

The characteristic parameters of GPT, for example, pervasiveness, technological improvement capabilities and technological spawning capabilities have been widely referenced in GPT-related studies. On the other hand, some further GPT parameters, namely prevalence, reallocation of resources, and inclusive democratization, have been referenced less often and were included in this article to achieve the most comprehensive coverage. In this regard, Table I provides a list of GPT characteristic parameters, which were selected from highly cited GPT-related studies, such as [4], [7]–[9], [11], [17], [24]–[28], to achieve an unique academic contribution based on extensive coverage all the GPT-relevant parameters.

A. GPT Characteristic Parameters

GPTs are usually characterized by the following:

1) pervasiveness;
2) a series of significant changes to the economic and social systems;
3) many incremental innovations;
4) a wide range of applications in a large number of sectors, making prior products obsolete and giving rise to increasing returns to scale, that is, creative destruction [4], [10], [11], [17], [27].

Furthermore, significant incentives are required to persuade entrepreneurs to attempt to make technological advances in highly uncertain environments, so a GPT is also defined by

TABLE I
GPT PARAMETERS

ID	Parameters	Literature	Description
1	Pervasiveness	[4], [7], [8], [11], [9]	GPTs should spread to most sectors. They should have an impact on technical change and productivity growth across a large number of industries.
2	Technological Improvement Capabilities	[4], [7], [8], [11], [9]	GPTs should improve over time and hence should keep lowering the costs of their users. They should lead to sustained productivity growth and cost reductions in several industries.
3	Technological Spawning Capabilities	[4], [7], [8], [11], [9]	GPTs should make it easier to invent and produce new products and processes.
4	Prevalence	[7], [9], [17]	The prevalence of technology is given by its persistency over time. In other words, such a technology is unlikely to be challenged by new alternative technologies – it seems to be incontestable, at least for some time.
5	Reallocation of Resources	[9], [11], [27]	The available resources are reallocated, dedicated partly to the development of the skills necessary for the use of the new technology and partly to the replacement of the old capital goods with new assets that allow the exploitation of all the potentialities expressed by the GPT.
6	Inclusive Democratisation	[11], [24], [28]	Progress in democracy and innovation foster growth by improving the accumulation of social capital and by lowering income inequality. This is exemplified by several GPTs, such as steam engines or electricity, which particularly emerged during industrial revolutions in democratic European and North American countries. For instance, the diffusion of electrically powered household appliances helped to increase female labour force participation by freeing up women's time from housework.

5) its prevalence, being present in the system for a long period and being accepted on a large scale so that the specific allocation of resources by stakeholders is stable over time.

GPTs lead to institutional change as well as economic development and improve the accumulation of social capital, which ultimately enables

6) inclusive democratization.

1) Pervasiveness: Pervasive technology is adopted by many market segments which reflects performance of its certain function that is vital to the functioning of a large segment of existing or potential products and production systems [4], [9]. However, for the pervasive deployment of technology, its adoption must be convenient, particularly from a cost perspective, with a potential to reach a certain level of efficiency so that it can be claimed to show technological improvement capabilities, and it must lead to the development of new so-called "secondary" or "complementary" technologies, thus demonstrating technological spawning capabilities [9]. ICT is a good example of pervasiveness, which is strongly related to network externality. An increasing number of users enabled higher profits, which were triggered by a particularly comprehensive system based on cable connections to a neighborhood [11].

2) Technological Improvement Capabilities: GPTs must undergo continual technological improvements over time; hence, their adoption must be convenient from a cost consideration perspective by reaching a certain level of efficiency, facilitating the creation of new organizations, processes, or technologies. Furthermore, GPTs should enable permanent technological development at every stage of the value chain [9], [29]. For instance, the scope for improvement of nanotechnology is related to reductions in size, lower costs, and greater complexity [29], so it may lead to sustained productivity growth and cost reductions in several industries.

3) Technological Spawning Capabilities: The technological spawning capabilities of a GPT show the extent to which it may make it easier to invent and produce new products and processes. A GPT triggers the development of "secondary" or "complementary" technologies, that is, technological spawning capabilities [9], so that GPTs lead to product and process innovation with a broad range of uses/application sectors [17]. It is important to underline that complementary technologies are developed as long as the various actors involved share the belief that the GPT is spawning innovations in multiple technological areas [9]. Hybrid corn is counted as an invention of a method of breeding superior corn for specific localities rather than an invention that is immediately adaptable everywhere [11].

4) Prevalence: A GPT is also defined by its persistency [7], [9], which is based on the following three conditions:

1) the technical interrelatedness of the system components;
2) the costs of adopting the new technology;
3) the positive network effects [17].

The coordination of actors' choices of a specific technology is particularly determined by the way how they understand and communicate the benefits received from the adoption of new technology, i.e., GPT [24]. The degree of diffused information points to the role of information and uncertainty in adoption, as it tackles potential coordination failures between innovation actors. Concerning coordination, large actors, such as large firms, public procurement organizations, or large public utilities, may play a leading role not only in the design and development of GPTs but also in the encouragement of complementary innovations by users in specific directions [24]. For instance, the procurement policy of the United States (US) Department of Defence and NASA during the 1950s and 1960s enabled the microelectronics technology to play a significant role in the electronics industry, while they also shouldered much of the risk through procurement assurances.

5) Reallocation of Resources: GPTs lead to "destructive creation," as resources are reallocated to develop the competencies necessary for the use of the new technology and to replace the

old capital goods with new assets that enable the exploitation of all the potentialities expressed by the GPT [11], [30].

Just after the emergence of a new GPT, a phase of experimentation is witnessed in which companies explore different methods to exploit these opportunities, facing strong uncertainties and the skills required to succeed on the market. This leads to a reduction in entry barriers. At the end of this process, a dominant standard is established and the industry can develop, while economies of scale are the main target, leading to industrial and geographical consolidation [21]. An example of this is the arrival of microelectronics and the Internet, which shifted economic power from the east coast of the US to Silicon Valley.

Several potential symptoms are caused by the reallocation of resources during the emergence of a GPT [17], such as the following:

1) a slowdown in productivity, due to learning effects and the allocation of productive resources to the development of the new compatible and complementary capital required to use the GPT;
2) an increase in the demand for skilled and qualified labor;
3) a rise in entries, exits and mergers;
4) an initial decline in stock prices due to the acceleration of the rate of obsolescence of old capital vintages caused by the adoption of the new GPT;
5) a change in the relative market shares of "young" companies;
6) a rise in the interest rate and a worsening of the trade balance due to asset reallocation and a reduction in output, pushing demand and consumption to search for foreign markets;
7) the transformation of the industrial geography.

6) Inclusive Democratization: Various studies, such as [28], [31], and [32], claim that technological progress, institutional change, and economic development paths are interwoven. Progress in democracy and innovation foster growth by improving the accumulation of social capital and by lowering income inequality, facilitating inclusivity, which emphasizes the role of institutions.

Papers [31] and [32] describe institutional change as a path-dependent process in which institutions are a function of technological developments and previous institutions. For instance, the first and second industrial revolutions were triggered by several GPTs, such as steam engine or electricity, which supported the development of social capital in European and North American countries and caused the emergence of further GPTs. Similarly, the work in [28] claims that recent democratisztion developments between the 1980s and the 1990s fostered a new techno-economic paradigm based on converging technologies, such as ICT.

It appears to be the case that the development of social capital, such as BoP, is also influenced by the emergence of new GPTs. In this context, scholars such as Coccia [8], Jovanovic and Rousseau [11], Graham and Iacopetta [25], and Coccia [28] point out the revolutionary role of GPTs as new forms or sources of energy (e.g., steam, electricity and engines), new forms of transportation (e.g., ships and railroads) or a combination of these (e.g., steam-powered rail engines) as well as ICT.

ICT, as inclusive innovation [33], could leverage BoP to improve living conditions by enabling the following:

1) the access of BoP buyers to goods and services;
2) the access of BoP producers to buyers of goods and services;
3) the demand for and creation of relevant goods and services for BoP consumers;
4) the generation of entrepreneurial opportunity;
5) an increase in overall skills, knowledge, and confidence.

In the same manner, Blockchain is referred to as a new-generation ICT that enables financial and social inclusion, which is especially necessary for improved social capital and BoP [18].

B. Blockchain-Specific GPT and Patentometric Studies

In a variety of studies in the literature, such as [3], [14]–[16], Blockchain is referred to either as a GPT or as an emerging multidisciplinary KET. Various GPTs are studied to understand their impact on civilization. Similarly, there is a critical need in the academic world to understand whether and to what extent Blockchain may become a new GPT [1].

Scholars such as Kane [1] and Davidson *et al*. [34] claim that Blockchain, which is a disruptive institutional innovation, may be considered as a GPT and not only as an ICT, as it is a technology that may create new forms of organizations. Blockchain may be viewed as an emerging GPT that shows a particular scope for improvement, which is a widely acknowledged characteristic of GPTs [2].

However, there is a lack of studies describing the features of a system that are required to label it as a DLT or Blockchain, so these terms are used interchangeably in the literature. Although the same approach was deployed in the scope of this article, particularly for simplicity reasons, it is also essential to clarify what is meant by Blockchain: Blockchain is a DLT-based special software that has shifted from being seen simply as a digital currency software to being viewed as a disruptive institutional technology [1]. It consists of a consecutive time-stamped chain of blocks in a decentralized fashion created through consensus and cryptographic mechanisms, which are stored by the nodes, that is, small servers, distributed across a P2P network.

Blockchain may be grouped into three categories [35]: Blockchain 1.0 ("Internet of Money"), Blockchain 2.0 ("Internet of Contracts"), and Blockchain 3.0 ("Internet of Governance"). Blockchain 1.0 refers to the currency applications of Blockchain, namely Bitcoin, and relies on a public ledger system for transactions that is considered to be explicitly Turing incomplete [1], [36], that is, a distributed database. Blockchain 2.0 refers to entire markets and economies by relying on executable codes and applications, such as Ethereum, not just transactions, and is considered to be Turing-complete, that is, distributed computing [1], [37]. Blockchain 3.0 involves complete diffusion and adoption throughout society, which would expectedly cover Turing-incomplete and Turing-complete structures.

Kane [1] claims that Blockchain displays the main characteristics of a GPT, although some may argue that it should not be counted as a GPT, while most of the literature refers to computers or the Internet as a GPT rather than this type of

computer software database. In this regard, it is important to highlight that many technologies, such as steam or electricity, which are considered to be GPTs or KETs, usually spawn newer GPTs, such as the railway or ICT [20]. In the same manner, the emergence of computers (GPT) or the Internet (GPT) triggered further innovations considered to be GPTs, such as the Internet of Things (IoT) [38], Artificial Intelligence (AI) [39], [40], or Blockchain, all of which are expected to converge with each other soon [41]. Thus, the IoT and AI are counted as GPTs even though they are based on other GPTs, such as electricity (GPT), computers (GPT), or the Internet (GPT), so the same may be expected of Blockchain.

Blockchain may be claimed to lower production costs in the neoclassical approach or lower transaction costs as institutional technology [1], [34]. Although Davidson *et al.* [34] refer to Blockchain as disruptive institutional technology, becoming a new GPT, Merediz-Solà and Bariviera [53] not only refer to technological innovations but also include marketing and institutional innovations, so GPTs can be classified not just as technological but also as process and institutional innovations [1], [42].

A GPT can only truly be identified historically, as the technology may differ from its first iteration, whereas patents offer information about the current state of a technology and more commonly about the past development of that technology [9], [19]. However, new technologies, such as Blockchain, are in the process of emerging, so the patent characteristics that have traditionally been collected are either not available or are rather small in number and thus prone to statistical error. Moreover, Blockchain was designed initially as an open-source technology [1], so few of the Blockchain innovations and improvements can be identified in patents. Despite these disadvantages, as there has been a strong increase in patent applications over recent years, Blockchain's path from a business process perspective might be understood now by investigating patent data [43].

C. Research Gap, Aim, and Objectives

The potentially pervasive nature of Blockchain and its increasing recognition as a GPT have also resulted in a desire in the academic world to investigate whether and to what extent Blockchain might be the next GPT and/or to what extent Blockchain already possesses the characteristics of a GPT. The fact that there are few Blockchain-related studies—such as [1]–[3] and [34], which discuss Blockchain as a potential GPT, and [12], [13], and [43] in the innovation management domain, which investigate Blockchain from an emerging technology perspective based on bibliometrics or a text-mining approach but without a GPT focus—points definitively to a research gap in the evaluation of Blockchain's potential as a new-generation GPT. In fact, to the best of our knowledge, only [2], [3], and [14], besides [1], investigate Blockchain from the GPT perspective and only [2] and [3] rely on patent analysis. Therefore, many Blockchain-related studies, such as [1], [12], [13], and [44], fail to conduct a patent data-based investigation, omitting extensive analysis of the topic. For instance, the work in [1] focuses on a survey of Blockchain applications based on information provided by the Internet to investigate Blockchain rather than using historical data, that is, patent data, as there is a lack of such historical data to analyze this new technology. However, the analysis in [1] might be misleading as the entire Blockchain ecosystem is exceptionally dynamic, with small groups of entrepreneurs and individuals who are motivated by the hype playing a significant role.

Filippova in [3] asserts that Blockchain does represent an emerging GPT following an investigation of GPT characteristics, namely pervasiveness, innovation-spawning effects, and scope for improvement, while Filippova *et al.* in [2] claim that Blockchain deserves attention as an emerging GPT as it already possesses scope for improvement, which is a widely acknowledged feature of a GPT. However, this article took a different approach to the topic, claiming that Blockchain has not yet become a GPT, though it already shows some GPT characteristics. Moreover, this article has a wider scope as it is based on six different GPT characteristics, while [2] and [3] have a smaller focus concerning the GPT characteristics. For instance, prevalence is not considered in either study, although many scholars, such as [7], [9], and [17], already point to this characteristic. A methodological comparison between [2], [3] and this article shows that [2] and [3] are solely based on quantitative data, which may provide restrictive results, whereas this article aimed to increase the reliability and validity of the results derived from quantitative analysis with expert opinion.

Thus, the investigation of Blockchain concerning its potential as a GPT requires the most comprehensive approach possible, which was realized in the scope of this article, so it differs from other studies from the conceptual and methodological perspectives. This approach is becoming more important, as some studies, such as [14], claim Blockchain to be a disruptive institutional technology; however, this is not based on an empirical investigation.

At first glance, the work [3] and this article seem to follow similar approaches, although this article tackles some critical weaknesses of [3]. For instance, comparing Blockchain's generality index with ICT appears to be very vague, while patent data already show that Blockchain is strongly related to ICT. On the other hand, in the scope of Blockchain's technological improvement characteristics, Filippova in [3] claims that the detailed investigation of patent contents is not covered, while this parameter is extensively investigated with heatmap analysis supported by expert opinion in this article. This approach certainly provides a deeper insight into Blockchain's GPT characteristics.

Davidson *et al*. in [14] claim that Blockchain may be also counted as an institutional technology, as it is more than just a new-generation GPT. However, GPTs can be classified not just as technological but also as process and institutional innovations [42], so this distinction might not necessarily be correct. Moreover, this article assumed Blockchain to be widely deployed in our society, which demanded an empirical investigation. In comparison with [14], this article relied on patent data supported by expert opinion to investigate these assumptions empirically. For instance, the involvement of experts in the analysis of the heatmap of Blockchain patent data enabled a deeper investigation of Blockchain's technological improvement capability.

The work in [2] follows the quantitative approach based on data from patents and the media to investigate Blockchain's scope for improvement. However, the GPT analysis of any innovation cannot be restricted to only a single GPT parameter. Moreover, the work in [2] claims that the evolution of the total number of Blockchain patents serves as an indicator of the scope for improvement of technology. However, it does not provide any information on how particular fields of Blockchain technology are being addressed by innovation actors. For instance, the work in [2] is missing any insights into how Blockchain patents that address the R&D aspect are categorized, which was addressed by this article.

Studies such as [12], [13], and [44] investigate Blockchain-related academic studies using a bibliometric method but at a higher level, which are difficult to align with Blockchain's GPT characteristics. For instance, it is not possible to investigate whether Blockchain displays spawning characteristics as it is unclear whether the current research efforts aim to improve the technology or to work in related fields.

This article addressed this gap by deploying a mixed-method approach, consisting of patentometrics and semi-structured interviews, to examine Blockchain as a potential GPT. While investigating the GPT characteristics holistically, all the identified GPT characteristics were covered, without excluding any country- or sector-specific focus. Moreover, this article is the first academic work to study the Blockchain domain from a GPT perspective based on patentometric analysis, while contributing to the academic world by reviewing all the GPT parameters of relevant scholars.

Investigating Blockchain from a GPT perspective could challenge the existing organizational theories fundamentally [45], including organizational ecology, institutional theory, transaction cost economics, resource dependence, and network theory.

As mentioned earlier, Blockchain studies lack a data-based investigation of Blockchain's GPT characteristics, so that this article comprehensively investigates the topic with a patentometrics based extensive patent analysis. Based on the literature reviews in the GPT- and Blockchain-related domains (see Section II and Fig. 1). This article aimed to answer the following research questions:

RO1: Does Blockchain display pervasiveness characteristics and, if so, to what extent?
RO2: Does Blockchain display technological improvement capability characteristics and, if so, to what extent?
RO3: Does Blockchain display technological spawning capability characteristics and, if so, to what extent?
RO4: Does Blockchain display prevalence characteristics and, if so, to what extent?
RO5: Does Blockchain display reallocation of resources characteristics and, if so, to what extent?
RO6: Does Blockchain display inclusivity and democratization characteristics and, if so, to what extent?

III. Research Design

This article used a mixed-method approach to offer a deep and broad understanding of the subject by considering all the relevant GPT characteristics without reducing the focus to a single country or sector. The mixed-method approach is also suitable for this article as it increases the reliability and validity of the results. The patent data provided quantitative and comprehensive results, and the semi-structured interviews with experts deepened the interpretation of and validated the findings [46]. This sequential mixed-method approach [47], [48] began with patentometrics, followed by the interview method, which perfectly complemented the results retrieved from the patentometrics (see Fig. 2).

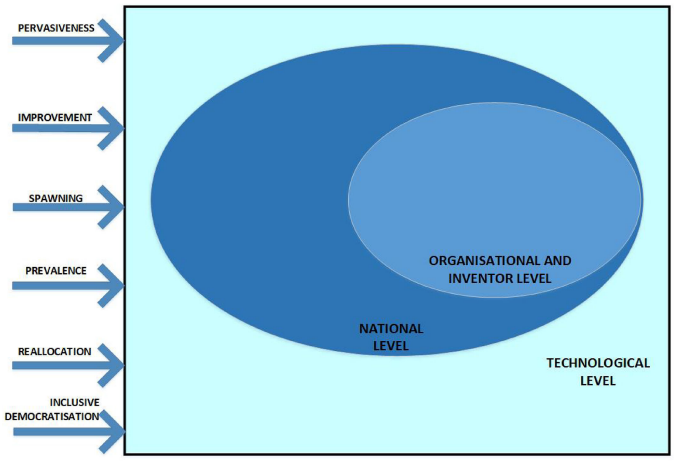


Fig. 1. Research framework.

A. Quantitative Method: Patentometrics

Patentometrics is composed of the following five stages:
1) database selection;
2) data search;
3) data optimization;
4) data analysis;
5) visualization—followed by the interpretation of results for the patent dataset [49].

To access the right set of patent codes and lexical search terms, the research and innovation areas in the Blockchain domain were grouped based on the literature and the qualitative examination of the sample patent data.

During the data collection process, 249 Blockchain-relevant terms were used; the following list of keywords shows some of the ones used to collect and create the dataset:

Blockchain OR Bitcoin OR Cryptocurrency OR "Distributed Ledger" OR "Smart Contract" OR "Zero-Knowledge Proof" OR Ethereum OR Hyperledger.

As a result, nearly 2500 Blockchain-related patents were examined. The total number of patenting organizations in relation to the number of organizations patenting for the first time in the Blockchain domain and the number of forward citations based on the number of distinct technological classes (IPCs) were investigated. Furthermore, Blockchain's proximity to other groups of GPTs and its impact on the innovation and management landscape were investigated.

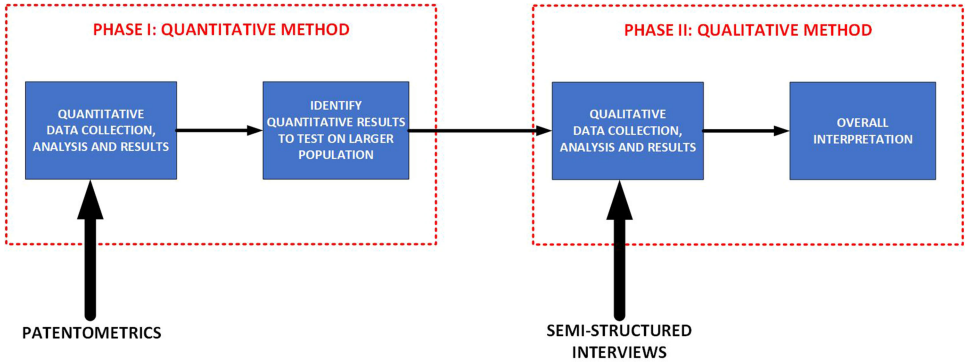


Fig. 2. Sequential exploratory design.

TABLE II
LIST OF INTERVIEWEES

Interviewee	Age	Highest Level of Education	Position in Organisation	Year of Experience
X1	55	BSc	Blockchain consultant	3
X2	45	MSc	CEO of a Blockchain-related company	4
X3	35	PhD	Academic undertaking Blockchain research	3
X4	39	MSc	Blockchain developer	4
X5	38	MSc	Blockchain consultant	4

B. Qualitative Method: Semi-Structured Interviews

In the qualitative stage of this research, semi-structured interviews were implemented to increase the reliability and validity of the results. Hence, information from the interviewees was used to support the analysis performed in the quantitative stage and to increase the depth of the study. Accordingly, the sample selection was designed to gather a variety of types of information from the relevant experts.

The interviewees were recruited from industry and academia based on the criterion that they were actively engaged individuals with at least one year of experience in Blockchain field. The experts are currently either working in a leading strategic position in their organization or working on an ICT-related function that gives them information and knowledge on Blockchain technology [21]. In such a way, it was possible to generate comprehensive knowledge and critical insights from various organizations. On average, the interviews took between 45 and 60 minutes and contained open-ended questions about GPT-related parameters of Blockchain. The experts participated in the semi-structured interviews in two ways: either 1) they were shown the results of the quantitative analysis and asked for their confirmation and further comments; or 2) they were asked open-ended questions to extend and illustrate cases, such as "Can you provide use case(s) of Blockchain in which you might consider Blockchain as a GPT?" or "Do you observe or expect a paradigm shift in the economy triggered by Blockchain technology?" As shown in Table II, five experts, consisting of one Blockchain developer, two independent Blockchain consultants, the CEO of a Blockchain company and one academic, the author of several studies, were included in the study.

During the study, it was possible to determine that the experts provided consistent information and that, in the last interview, a saturation point was reached, so the information provided was similar and repetitive. Thus, as the qualitative method was a supportive step in this article, our results were finalized based on these five experts' opinions. Considering the reliability of the results, all the experts confirmed the accuracy of the quantitative results regarding the validity of information gathered in the scope of GPTs and Blockchain, enabling the results of the quantitative investigation to become more related and deeper.

The semi-structured interviews were interpreted with the NVivo qualitative data analysis software in five steps:

1) organization of the data;
2) disassembling the data into groups;
3) reassembling the data by regrouping them according to GPT characteristics;
4) induction of meaning from the reorganized data;
5) deriving of conclusions from the data with a special focus on Blockchain.

IV. RESULTS AND DISCUSSION

This section consists of the illustrative outputs retrieved from the mixed-method analysis to investigate the extent to which Blockchain shows GPT characteristics. The discussion section is divided into six sections in line with the GPT characteristic parameters shown in Table I. The investigation of Blockchain from a GPT perspective requires a holistic approach to the research objective so that all the identified GPT characteristics are covered without excluding a country- or sector-specific focus.

A. Pervasiveness

GPTs, such as Blockchain, disrupt different segments across the entire economy, particularly the ones that are based on database [1]. Although the work in [1] claims that Blockchain applications are concentrated on Blockchain 2.0, that is, the "Internet of Contracts," many interviewees claimed that Blockchain as the "Internet of Money" has a higher probability of transforming itself into a GPT, as they observed that many Blockchain developers are concentrating on corresponding topics. It is also important to note that [1] does not introduce a clear definition of Blockchain categories, so there is an arbitrary approach concerning the allocation of Blockchain applications to these categories. Furthermore, the interviewees pointed to the most

TABLE III
NUMBER OF TECHNOLOGY TERMS BY YEAR

Year	Number of Terms (New)	Number of Terms (Existing)	Number of Terms (Total)
2014	0	0	0
2015	18	0	18
2016	32	6	38
2017	124	28	152
2018	298	120	418
2019	96	170	266

significant application fields of the "Internet of Money", namely identity solutions; logistics; energy; mobility; and healthcare.

Interviewee X2 further claimed that the digital revolution, particularly fuelled by social media platforms, is expected to disrupt the existing traditional institutions. For instance, Facebook already connects 2.4 billion users worldwide, so it may easily transform itself into the "Internet of Money" platform as it is currently experimenting with Libra. Furthermore, another pervasive social media platform, WhatsApp, with 1.5 billion users, could be converted into the "Internet of Money" platform supported by Blockchain features.

X2 also emphasized the role and impact of policymakers as they can recognize an element existing in the online world, for example, electronic signatures, as if it exists in the physical world by law. For instance, two unique "Internet of Money" concepts, namely Initial Coin Offerings (ICOs) and Security Token Offerings (STOs), also depend on corresponding policies, as recent US regulations have proven. Initially, cryptocurrencies such as Ethereum or Bitcoin received considerable attention from US investors, which was unfortunately negatively affected by the recent decision of the Internal Revenue Service concerning the taxation of cryptocurrencies. Furthermore, the US Government prohibits Blockchain-related institutions located in other countries from selling securities, including ICO or STO tokens, to US citizens.

In the scope of the "Internet of Money," digital identity solutions are also expected to benefit strongly from Blockchain. Considering Blockchain's unique security features, it could provide the best storage medium for such highly sensitive data. For instance, the biometric data of BoP citizens could be stored securely on Blockchain, so BoP can be included in the civilized world. Thus, the unbanked people of BoP are currently highly emphasized by the Blockchain community.

However, interviewee X1 pointed out two main reasons for the slow diffusion of Blockchain technology: 1) Blockchain does not enable the realization of a product as it needs to be integrated with other products or solutions; and 2) Blockchain alone is not at Technology Readiness Level (TRL) 9, the TRL indicating the maturity level of technology.

Table III indicates that the number of Blockchain terms increased dramatically, from almost 0 in 2014 to 418 in 2018, as newer technology terms have been increasingly introduced. Dabbagh *et al*. in [13] also confirm the publication and citation trends of Blockchain papers, stating that the number of Blockchain articles has been growing dramatically since 2013. Blockchain technology is obviously spreading to other technology fields.

TABLE IV
PATENTS VERSUS TECHNOLOGY TERMS

Patent Class	Number of Records
G06F001730	524
H04L002906	333
G06Q002038	292
G06Q002006	248
G06F002162	132
G06F002164	125
G06F002160	110
G06Q004004	110
G06Q002002	98
H04L002908	92
G06F002110	79
G06Q001006	62
G06F002131	52
G06Q001008	52
G06Q002010	50
Other	2385

Fig. 3 shows the patents scores for each patent classification. In 2015, there were no patent applications, particularly because Blockchain was a very new technology; in 2018, Blockchain patents had already achieved a level of approximately 1400 in 10 different categories. This is also confirmed by the citation trends of Blockchain papers, which have been increasing since their initial publication in 2014 [13].

The patents shown in Table III, Fig. 3, and Table IV point to three main patent categories: G06Q; G06F; and H04L. G06Q deals with payment mechanisms, whereas G06F and H04L address security concerns for data transmission and storage. It seems that the Blockchain community is currently concentrating on the development of topics related to the "Internet of Money." Interestingly, G06Q patents also cover payment mechanisms, which enable the involvement of intermediaries, such as notaries, trusted third parties, stocks and commodities. This development confirms the statements of interviewees that highlighted the changing business models of various traditional institutions in society.

Fig. 4 shows the direction of ten major countries in Blockchain landscape concerning their R&D efforts. None of the actors exhibits similar orientations in terms of R&D activities, demonstrating Blockchain's pervasive characteristics. It appears that the US actors are more focused on data processing, specially adapted for specific functions, such as information retrieval, database structures or file system structures, while China is engaged in communication control and protocol. Moreover, South Korea is strongly concentrated on payment protocols, that is, the "Internet of Money."

In conclusion, it is clear that Blockchain already possesses pervasive characteristics as it is applied to a range of sectors, a fact that is also underlined by Vitalik Buterin, the founder of the Ethereum platform [1].

B. Technological Improvement Capabilities

In line with [1] and [2], most of the interviewees claimed that Blockchain code is available to the public as open-source software, so anyone may access the original Blockchain code

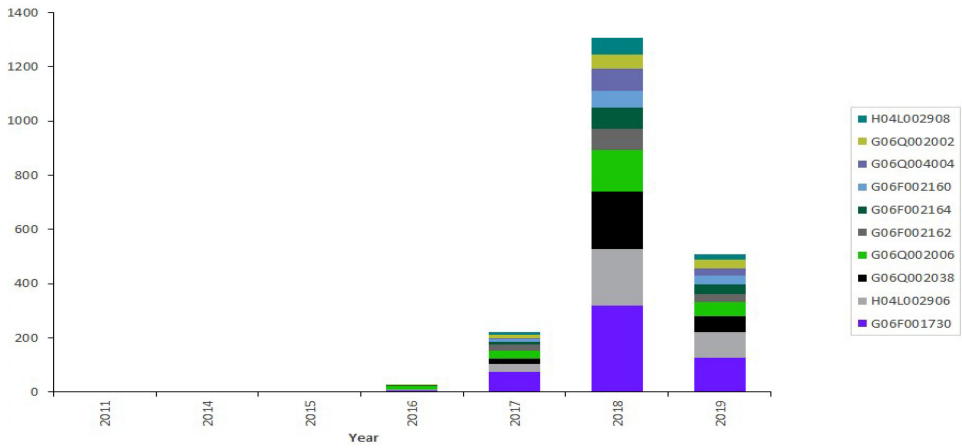


Fig. 3. Technology terms versus year.

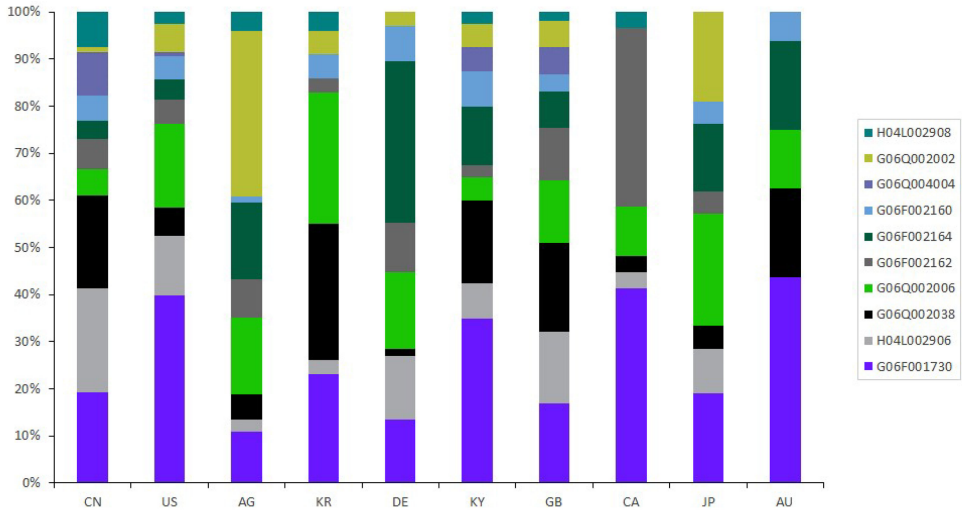


Fig. 4. Technology terms versus location.

and create applications, which points to Blockchain's technological improvement characteristics [1]. This also applies to soft and hard forks. Hard or soft forks occur when Blockchain's existing code is changed and the older version, Bitcoin, remains on the network, while the new version, Bitcoin Cash or Bitcoin Gold, is created to eliminate the existing malfunctions of the system. Blockchain's adoption is convenient from a cost consideration perspective [9], only if it shows continuous technological advancement, particularly in security, scalability and usability [50].

In this regard, Blockchain's technological improvement characteristics may be investigated in Fig. 5, which depicts a heatmap based on the analysis of Blockchain patents. The analysis shown in Fig. 5 has been realized with VOSviewer, which generates maps using VOS mapping, while the distance between items depends on their similarity or relatedness. Thus, if the distance between the two terms is smaller, it implies greater relatedness between them. Furthermore, the font size of terms is dependent on their frequency of occurrence in patents.

The majority of academic work is dedicated to computer science, engineering, and telecommunications domains [12], [13]. This is confirmed in Fig. 5, which was investigated with the support of Blockchain experts to create Table V. Table V consists of six clusters, namely value management; asset management; tracking; technology; documentation and certification; and governance and interaction. Cluster 1 deals with value management, including value storage, value security, value transmission, and value processing. Various use cases are patented in this cluster, such as the IoT, aviation, sustainability, three-dimensional applications and energy, making it one of the most fundamental blocks. Cluster 2 covers asset management, including topics such as the verification of digital asset ownership, its exchange based on tokens and the secure, efficient transfer of entities. However, it seems that Blockchain actors concentrate less on Cluster 2. Cluster 3 is focused on the tracking of values besides storage and exchange as well as on microtransactions. Interviewee X2 claimed that Blockchain needs to be improved in the context of microtransactions. Cluster 3 also covers topics

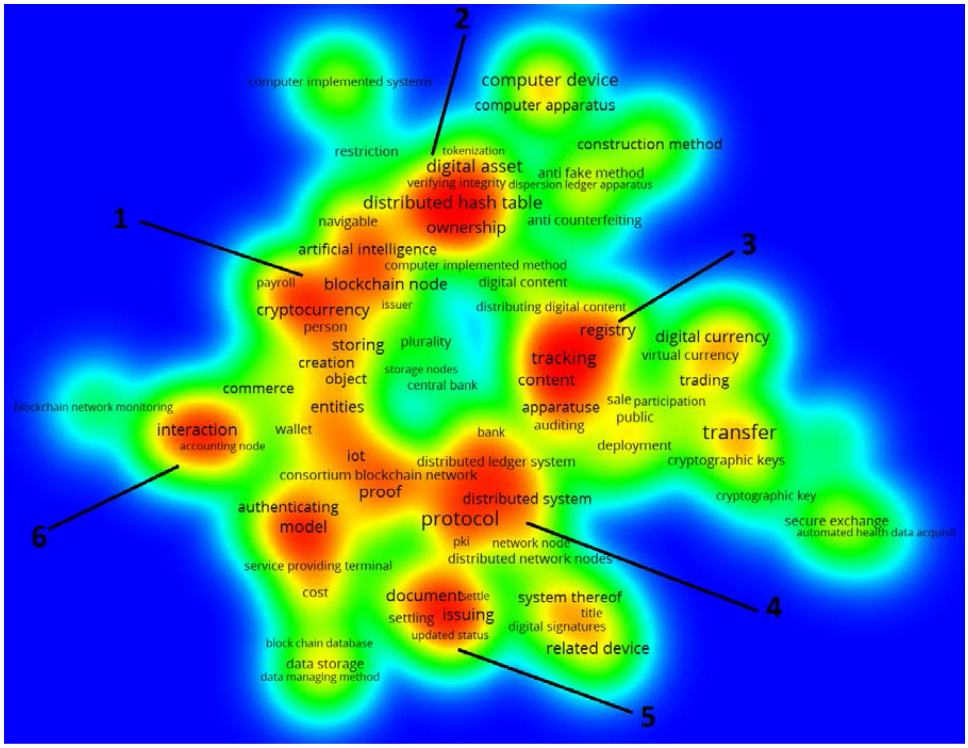


Fig. 5. Heatmap based on blockchain patents.

related to the enhancement of the Blockchain platform to store and exchange transaction data in a distributed computing network. Cluster 4 is particularly related to improving Blockchain technology, such as new types of Blockchain consensus methods and new types of Blockchain approaches. Cluster 5 deals with Blockchain-based document management, whereas Cluster 6 covers governance and interaction on the Blockchain platform and is particularly related to the enhancements required for Blockchain.

In conclusion, Blockchain actors are either working on the improvement of weaknesses in the Blockchain technology, in line with [50], or trying to position themselves as competitively as possible to benefit from the Blockchain hype.

C. Technological Spawning Capabilities

As mentioned earlier in Section II-B, Blockchain is also referred to as a KET [15] and [16] pointing to Blockchain's spawning capabilities. To exemplify this, interviewee X1 claimed that database technology might be considered to be a GPT as well, as it is responsible for 80%–90% of ICT deployments, including Internet (GPT) or Global System for Mobile Communications networks (GPT), with critical consequences for our civilization. For instance, the Internet was enabled by the Domain Name System (DNS), which is a database-related technology. The transformation of Arpanet to the Internet was only possible through the spawning of database technology to the Internet, that is, the DNS. Thus, X1 strongly associated this concept with Blockchain and database technologies, whereby Blockchain is expected to be integrated into the Internet by solving its shortcomings and thus spawn through further pervasion in our society.

However, in line with several other scholars, including [51] and [52], interviewee X2 claimed that Blockchain can be used as an integral part of the IoT, as it lacks micropayment mechanisms, which are one of the main problems of the IoT. However, the inefficient Blockchain architecture restricts money transactions on Blockchain which hinders the realization of micropayments. IOTA's Tangle, that is, "Blockchain without Blocks and the Chain," tackles this inefficiency, introduces a new way of reaching consensus and has the potential to enable the integration of IoT and Blockchain. Tangle is expected to enable faster payment mechanisms solely dedicated to IoT applications. Conditional on the current problems of Blockchain technology being solved successfully, it could spread successfully to other sectors, particularly in parallel with the diffusion of IoT technology. Furthermore, Blockchain could play a significant role in the IoT context concerning 1) Blockchains and smart contracts for the IoT and 2) IoT security, in which decentralization, peer-to-peer realizations, keeping a log of sequential transactions and traceability are important factors to be considered [44].

The analysis of Blockchain-related patents may provide valuable insights into the innovation-spawning effects of Blockchain, although Blockchain is still in its premature stage.

Table VI indicates that the number of R&D personnel increased from almost 0 in 2014 to approximately 1800 in 2018, as there is increasingly a shift of human resources to Blockchain-related R&D.

Table VII outlines 10 major actors with patent scores ranging between 50 and 250, whereas the "Other" bar consists of around

TABLE V
INTERPRETATION OF THE HEATMAP

ID	Cluster Name	Key Words Identified	Interpretation
1	Value Management	Artificial Intelligence, Blockchain Node, Cryptocurrency, Storage	• The following fields are expected to be influenced by Blockchain technology: (1) genetics; (2) e-commerce; (3) gambling; (4) aviation; (5) sustainability; (6) creativity; (7) security; (8) energy; (9) finance management; (10) asset management; (11) 3D applications; (12) social media; (13) sports management; (14) gaming; (15) business operations, including accounting, HR, marketing and knowledge management; (16) healthcare; and (17) smart cities, including autonomous objects and the IoT. • The fields mentioned may be grouped into two categories, namely near-term and far-term use case categories. • To provide an example of a near-term use case scenario, a Blockchain-based payment system in aircraft (Patent Code US20180293555A1) may be counted as an interesting deployment of Blockchain technology. It appears that Blockchain will spread to such fields as well. • Another interesting near-term category is creativity, which deals with various topics, such as the monetising of intellectual property (Patent Code US20190130507A1), rewarding mechanisms concerning story creation (Patent Code KR20190113075A). • When it comes to the far-term use case category, the convergence of Blockchain and AI seems to be very promising, so categories such as (1) smart cities, including autonomous objects and the IoT, (2) healthcare or (3) energy management are expected to emerge. Thus, Blockchain enables distributed computing. • For instance, in the case of autonomous objects, Blockchain and AI are expected to be deployed to manage moveable autonomous devices (Patent Code CA2961357A1).
2	Asset Management	Digital Assets, Distributed Hash Table, Ownership	• Cluster 2 is focused more on topics related to the verification of digital asset ownership, exchange based on tokens and secure, efficient transfer of entities. These topics deal with the improvement of Blockchain technology.
3	Tracking	Registry, Tracking, Content	• There are various areas in which Blockchain technology may be deployed to trace value. This includes areas such as (1) finance; (2) virtual reality; (3) asset management; (4) various business functions, including document management and manufacturing; (5) tracing IoT data; (6) e-commerce; (7) security; and (8) healthcare. • One of the best examples of Blockchain's deployment is the track-driver-behaviour-to-prevent-drowsy-driving prevention method (Patent Code KR20190128479A). • Another example is the Blockchain-based tracing of energy consumption, water consumption, water quality, greenhouse gas emissions and air emissions (Patent Code US20190311443). • It appears that Blockchain's deployment will also occur in the digital world, as demonstrated by virtual reality (Patent Code KR102044008B1), which enables identity authentication and management.
4	Technology	Protocol, Distributed System, Network Node, Proof	• Cluster 4 deals with managing transactions of value data through Blockchain while covering topics including (1) secure data transactions (2) using infrastructure technologies, such as wireless telecommunication systems (Patent Code US20180048738A1). It also deals with updating the Blockchain network protocol. • Furthermore, it covers topics related to data storage in the distributed computing environment, that is, cloud computing (Patent Code WO2019152750A1), including various consensus mechanisms for Distributed Ledger Technologies. • Moreover, in the case of the IoT, a Blockchain-based sustainability protocol for IoT Sensors (Patent Code US20190122086A1) is described.
5	Documentation and Certification	Document, Issuing, Settling	• While some patents describe how to certify an electronic document, others deal with Blockchain-based signatures, such as signing PDF-based documents or due diligence in mortgage documents. • There are some specific use cases besides generic document management cases. For instance, in the case of identity management, Blockchain-based digital identity management and permission control mechanisms are described. • When it comes to certification-related patents, a mechanism is an interesting case as it describes how to manage lifelong learner events via Blockchain.
6	Governance and Interaction	Interaction, Accounting Node	• This cluster is focused on securing value using Blockchain, covering topics such as securing and disseminating time-sensitive information (Patent Code AU2017212801B2) or managing Blockchain access to user profile information (Patent Code US10129269B1). • Regarding the transmission of Blockchain data, it deals with how to reduce Blockchain transaction delays (Patent Code US20190114626A1) or cross-chain interactions in Blockchain systems (Patent Code US20190253263A1). • Concerning processing value data, several concepts are proposed, such as distributed reputational databases (Patent Code US20190052722A1) or new methods for Blockchain management (Patent Code US20180308072A1). • There are various fields in which Blockchain-based governance and interactions may play a role. • For instance, in the case of the IoT, they are patents that describe how object reconciliation for interaction in a Blockchain environment (Patent Code US10192073B2) may be realised. • Another Blockchain-based patent describes a gaming platform system for the interactive participation of players with a Bitcoin-based award mechanism (Patent Code WO2015117029A1).

TABLE VI
INVESTORS' TREND

Year	New People	Existing People
2014	0	0
2015	17	0
2016	50	0
2017	332	0
2018	1609	134
2019	648	198

TABLE VII
PATENTS VERSUS ORGANIZATIONS

Organisation	Number of Records
NChain	270
IBM	154
Alibaba	150
Mastercard	138
Coinplug	70
Huawei	62
Walmart	58
Pingan	51
Intel	49
China Unicom	48
Other	3909

3800 patents. This confirms the widely distributed Blockchain-related R&D landscape, as there is certainly a high number of actors with a low number of patent scores.

Furthermore, Table VIII outlines that the major Blockchain actors are highly concentrated on "Internet of Money"-related topics, particularly payment mechanisms, data storage and data transmission, and they are either shifting their existing R&D capacity or increasing their R&D capacity by hiring new inventors. For instance, NChain is fairly focused on payment mechanisms (115 patents), whereas IBM is dealing with data storage (92 patents). Furthermore, it appears that IBM is working on some niche topics, including healthcare and traffic, that is, future promising IoT use cases, pointing to Blockchain's technology-spawning characteristics.

In conclusion, there is obviously the reallocation of assets and entries of new actors, such as organizations or inventors, in the innovation process, which points to the arrival of a new GPT, that is, Blockchain.

D. Prevalence

The key point regarding prevalence is that different actors in the innovation landscape understand and communicate a set of beliefs concerning the wide applicability of the GPT [9]. Despite the widespread acceptance of Blockchain's potential, it is still seen by a majority of people as a niche technology, so few people utilize its services [1]. This requires strong coordination between a broad set of actors, particularly entrepreneurs, who need to be persuaded to attempt to make technological advances in a highly uncertain environment [7].

Interviewee X2 pointed to Facebook's Libra, which is in principle a stablecoin. Just after the introduction of Libra, the US Congress invited Zuckerberg to testify to his Libra project, while Germany and France declared Libra to be a national security risk. X2 claimed that US policymakers are extremely concerned about the risk that, following the introduction of Libra, the US would lose the ability to dominate the global economy economically. In return, China, which competes with the US, declared its support for Blockchain technology, banned any negative news related to Bitcoin and revealed plans to introduce a Chinese national cryptocurrency. Furthermore, members of the Chinese Communist Party are required to transfer and register all of their daily activities to Blockchain. Thus, as proven by various government-supported projects, the interviewees claimed that strong policies are essential to promote the implementation of Blockchain so that it may become a GPT. The role of policymakers is also described by [1], who claims that centralized traditional institutions in competition with Blockchain may stifle its development through regulations, which would certainly threaten the positive benefits that it offers to society and the economy.

The interviewees also confirmed the importance of the common perception of stakeholders in the Blockchain landscape, as Blockchain's wide deployment and recognition may be effectively hindered by a poor reputation among stakeholders. For instance, a dramatic depreciation of Bitcoin's value would cause investors to lose money, which in return would reduce their motivation for investing in Blockchain and related technologies. Another event with equally negative consequences would be either slandering or deterring actors from Blockchain, as has occurred in the US with new legislation regarding taxing cryptocurrencies.

Table IX shows how each country is performing in the Blockchain landscape, including the most significant actors. Several countries have started to shift their R&D capacities to work on Blockchain technology, while private organizations, such as Huawei, IBM, Mastercard, Walmart, Samsung, Siemens, NEC, British Telecom and Alibaba, are also active in the Blockchain field.

China and the US are outcompeting other countries in terms of patent scores. X1 pointed to two main megatrends, namely the sharing economy and big data, and claimed that both countries are focusing on Blockchain as they are aware of the change in the global economy from traditional business models to a new type of business models, as proven by AirBnb, Uber, and so on. Thus, they have started to prepare their economies for this paradigm shift to strengthen their position in the global economy.

The number of Blockchain-related patent scores in relation to the number of researchers is higher in the US (1350 patents) than in China (1880 patents). In other words, the intensity of Blockchain-related R&D efforts is greater in the US than in other countries, including China. Thus, one may conclude that the US is more focused on Blockchain than other countries.

On the other hand, the number of Blockchain-related organizations is much higher in China than in other countries, including the US. The work in [13] provides an overview of the top funding agencies of Blockchain studies, and the majority of these institutions originate from China. Moreover, the majority of studies in the Blockchain field originate from China [12].

TABLE VIII
PATENTS CLASSIFICATION VERSUS MAJOR ACTORS

Ranking	Organisation	Patent Class	Patent Score (per Patent Class)	Description
1	NChain	G06Q	115	Payment Mechanisms
		H04L	107	Data Storage
		G06F	54	Data Transmission
		H04W	8	Wireless Communication Networks
2	IBM	H04L	92	Data Storage
		G06Q	66	Payment Mechanisms
		G06F	73	Data Transmission
		H04W	6	Wireless Communication Networks
		A63F	5	Games
		G16H	1	Healthcare Informatics
		G08G	1	Traffic Control
3	Alibaba	G06Q	39	Payment Mechanisms
		H04L	39	Data Storage
		G06F	28	Data Transmission
4	Mastercard	G06Q	39	Payment Mechanisms
		H04L	39	Data Storage
		G06F	28	Data Transmission
5	Coinplug	G06Q	39	Payment Mechanisms
		H04L	23	Data Storage
		G06F	16	Data Transmission
		H04W	3	Wireless Communication Networks

TABLE IX
LIST OF COUNTRIES AND SELECTED ORGANIZATIONS

Country	Number of Blockchain Patents (per Country)	Actors in the Particular Country	Number of Blockchain-Patents (per Organisation)
China	1880	Huawei Technologies Company Ltd.	59
		Pingan Sci & Technology Shenzhen Co Ltd	49
		China Unicom Group Co Ltd	47
US	1350	International Business Machines Corp	135
		Mastercard Inc	130
		Walmart Stores Inc	58
South Korea	199	Coinplug Inc	70
		Samsung Sds Co Ltd	17
		Samsung Electronics Co Ltd	11
Germany	162	Siemens Aktiengesellschaft	39
		Bundesdruckerei Gmbh	34
		NEC Corp	13
UK	105	British Telecommunications Plc	27
		R3 Ltd	7
		Alibaba Group Holding Ltd	6
		International Business Machines Corp	6
		Technicolor Sa	5
		Alcatel-Lucent	3
		Gemalto	3
		Ingenico Group Sa	3
		Maim E	3

Thus, Blockchain-related R&D activities are more pervasive in China, whereas R&D activities are more concentrated in the US, led by large organizations such as IBM, Mastercard, and Walmart, each from a different sector. However, interestingly, Switzerland plays a significant role in the Blockchain-related academic world, with its two leading journals, Sensors and Sustainability, but this is not reflected in Blockchain patents, as shown in Table IX. This occurrence confirms the open-source characteristics of Blockchain [12]. Furthermore, although Ireland is the country with the most citations per article in the field of Bitcoin, which functions as a proxy for the average scientific importance or quality of the academic work in the country, it is not identified in the list of countries with the most Blockchain patents [53].

Interviewee X2 also pointed to the so-called hash power concerning the competition between China and the US. Currently,

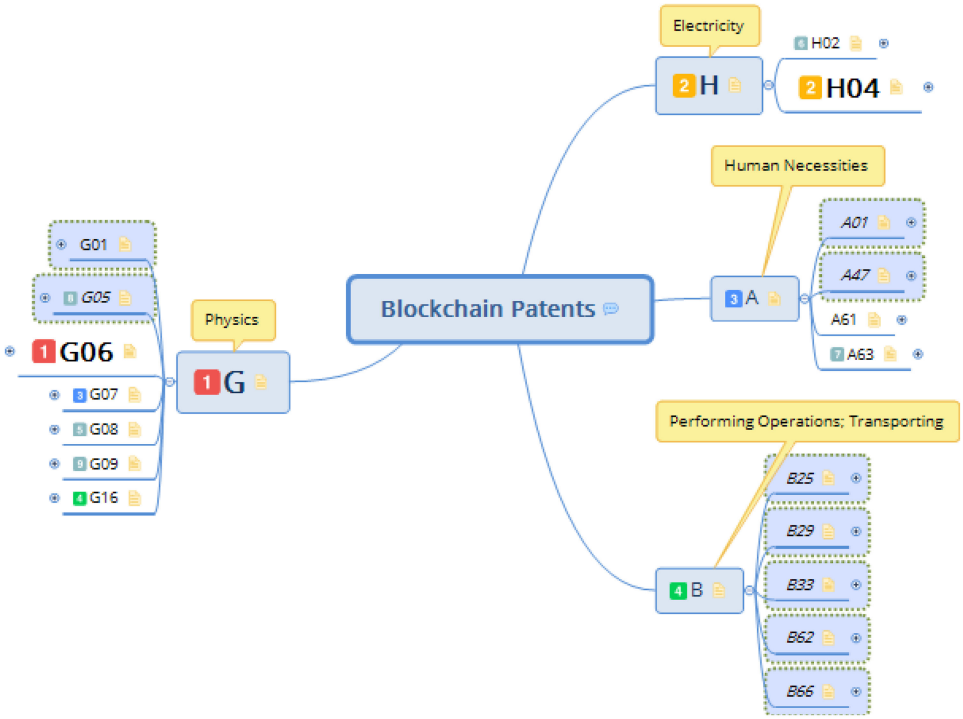


Fig. 6. Overview of blockchain patents.

Chinese mining pools control more than 70% of the Bitcoin network's collective hash power and therefore have an immense influence on the Blockchain landscape. Hash power is highly related to the Proof-of-Work consensus mechanism, which is the fundament of Blockchain, including Bitcoin. Moreover, it is important to mention that 50% of cryptocurrency projects and the majority of miners are based in China, whereas 90% of Blockchain calculations are simply concentrated in the nine groups of Chinese organizations.

Table V also shows that South Korea (199 patents) is following the US and China, particularly due to the R&D efforts of companies such as Samsung, which recently created a secure area for Blockchain applications on mobile phones. Germany, which occupies the fourth place with 162 patents, is largely led by companies located in Berlin. In the German ecosystem, Siemens (39 patents) is mainly concentrated on IoT applications, whereas Bundesdruckerei (34 patents) deals with personalization solutions, such as IDs or passports. As mentioned earlier, it is more secure to keep personalized information on Blockchain instead of one centralized server. Germany is followed by the UK with 105 patents, while, interestingly, the Chinese Alibaba (6 patents) also has some patent applications in the UK. Furthermore, R3 Ltd is located in the UK; this is a consortium consisting of various actors from the financial sector. They aim to develop a Blockchain platform, namely the Corda Platform, which may be compared to IBM's Hyperledger.

In conclusion, it can be argued that prevalence can already be observed in the Blockchain landscape, particularly in China and the US. This situation is also reflected in academic studies, in which the US and China are recognized as the two leading countries with the most publications in the Blockchain field [12].

E. Reallocation of Resources

The introduction of GPTs usually follows an S-shaped diffusion pattern while resources are reallocated, causing an economic slowdown. Innovation actors are initially unable to exploit the potential of a GPT and require some time to adjust before they can start to benefit from it [1]. In that context, Jovanovic and Rousseau in [11] claim that the introduction of new technologies to the market is usually accompanied by the emergence of new actors, who are ready to take more risks than other existing actors. Thus, during the GPT adoption, "younger" actors, who have been established for less than 25 years, are expected to perform better than "older" actors. In this scope, interviewee X3 pointed to the dominance of "younger" actors based on the validation in Crunchbase, which is a database consisting of information on public and private companies on a global scale. Only 20 out of 5261 organizations were established before 1995.

Table X depicts the companies with the highest Blockchain patent scores. IBM is the only company that has been in existence for more than 100 years; the majority of companies were established within a 25-year time frame, that is, "younger" companies (e.g., Mastercard in 2006, Alibaba in 1999, and CoinPlug in 2013). Thus, the larger portion of "younger" companies indicates that the "reallocation of resources" characteristic is already observable in the Blockchain landscape. However, it needs to be emphasized that large companies aiming to keep their monopoly

TABLE X
COMPANIES WITH THE MOST BLOCKCHAIN PATENTS

Company Name	Patent Score
NChain Holdings	270
IBM	154
Alibaba	150
Mastercard	138
Coinplug	70

on Blockchain might underinvest in R&D and therefore threaten younger companies [1], necessitating strong Blockchain-related policies.

F. Inclusive Democratization

The work in [31] briefly claims that technological development influences the institutional structure by changing the material setting in which it operates. In this scope, Blockchain as the "Internet of Governance" could enable democratic institutions and countries to coordinate their economic and scientific subsystems efficiently to increase their future technological and social progress. This would also extend from the sphere of politics to that of society, in which every citizen is expected to participate, enabling a condition of political and economic stability.

The study in [28] claims that many democracies need to consider how to bring out the value of people and to increase the education of human capital, that is, the intangible capital accumulation, which would also exert a positive impact on technology production and the competitive advantage of countries. In this scope, X3 claimed that Blockchain could tackle the distribution of disaggregated power, currently controlled by the so-called "power elites" associated with many democracies, which is also capable of marshalling forces against innovation. Thus, Blockchain offers a new method of institutional coordination for a new type of collaborative network, which is more distributed, participatory, citizen-centric and inclusive [54].

As mentioned earlier in Section II-A6, inclusivity is highly related to BoP, which has the poorest population of the world and suffers from scarcity resulting from barriers to the flow of goods, information and money. The study in [55] claims that Blockchain could allow BoP to improve living conditions by enabling financial inclusion. In this context, the study in [56] outlines that BoP has been using basic mobile phones to benefit from this new paradigm shift, enabled by ICT particularly, and exemplifies this with M-PESA, which is a mobile money service offered by Safaricom with approximately 14 million subscribers in Kenya. Conversely, some interviewees, such as X1, doubted whether Blockchain may be deployed pervasively in BoP countries so that it may act similarly to electricity (GPT), which has been playing an inclusive role in developing countries. Moreover, interviewee X1 asserted that our civilization's dependency on electricity is much greater than that on Blockchain, particularly considering BoP.

Fig. 6 presents an overview of Blockchain patents in mind map format. The fonts of the patent classes are in proportion to the patent scores. Moreover, Fig. 6 shows that actors are currently concentrating on G06 and H04, while G06 is related to computer technology and communication technologies. In other words, Blockchain seems to be highly related to the ICT domain, which is in line with scholars such as Ozdagoglu *et al*. [12], Dabbagh *et al*. [13], and Kamran *et al*. [44], who show that the majority of academic work is dedicated to the ICT domain, whereas other authors refer to Blockchain not just as an ICT innovation but also as an inclusive institutional technology [1].

G. Discussion and Implications

The findings of this article point to the critical need that Blockchain can only become a GPT if efficient policies are introduced that enable an effective innovation landscape and smooth coordination among Blockchain actors and tackle information asymmetry, along with strong leadership.

Although Blockchain shows some GPT characteristics, it should be highlighted that there are currently certain factors influencing Blockchain's progress toward becoming a GPT, which are as follows.

1) With cryptocurrencies, such as Bitcoin, Blockchain has proven to be pervasive [1]. This is also expected to happen with other features of Blockchain, such as smart contracts or Decentralized Autonomous Organisation (DAO) as well, which calls for Blockchain specific policies.
2) Patent data show that Blockchain actors have already started to address several technological shortcomings of Blockchain [50], such as the speed of transactions or the rise in energy consumption. However, the existing Blockchain-specific information asymmetry needs to be addressed by policymakers to strengthen the competence of actors in the Blockchain field so that Blockchain's adoption may be accelerated.
3) Countries such as China and the US seem to be highly focused on Blockchain, which are already dominating the world in many perspectives. On the other hand, patent data also points to inefficient innovation landscape in many countries which calls for strong Blockchain specific policies aligned with national strategies.
4) Currently, there is a market shift in favor of "younger" companies, such as Mastercard or Alibaba, which were established in the last twenty-five years period. We might expect to witness another Blockchain-enabled "Google" or "Facebook" in the near future, which has either just established or is not existing in the market yet. However, large companies aiming to keep their dominance in the market might change the current trend of Blockchain and therefore threaten younger companies.
5) As a disruptive institutional technology, Blockchain is expected to enable inclusive democratization, which will lead to disintermediation, decentralization and disruption of existing policy frameworks. This requires Blockchain-specific policies which aim to enable appropriate leadership to utilise Blockchain for good purposes.

In this scope, Table XI outlines the critical implications derived from this article which is particularly important for leaders from "Industry", "State" and "Academia".

TABLE XI
CRITICAL IMPLICATIONS

Industry	1. Industrial actors are highly concentrated on the development of "Internet of Money"-related topics, particularly the various payment mechanisms and security concerns related to data transmission and storage. This points to the changing business models of various traditional institutions. 2. Industrial actors should concentrate on the most significant application fields of "Internet of Money": (1) Identity Solutions, (2) Logistics, (3) Energy, (4) Mobility and (5) Healthcare. 3. The software industry should prioritise Blockchain-based social media payment solutions in their strategy. This is as Blockchain is expected to play a critical role in this context as part of the "Internet of Money." 4. Industrial actors should work on micro-payment mechanisms while Blockchain can be used as an integral part of IoT. This is one of the main problems of IoT. 5. The industrial actors can provide solutions for the unbanked people of BoP, as Blockchain can securely store the biometric data. 6. Industrial actors can focus on following fields as given by patent data, particularly from value management perspective: (1) genetics; (2) e-commerce; (3) gambling; (4) aviation; (5) sustainability; (6) creativity; (7) security; (8) energy; (9) finance management; (10) asset management; (11) 3D applications; (12) social media; (13) sports management; (14) gaming; (15) business operations, including accounting, HR, marketing and knowledge management; (16) healthcare; and (17) smart cities. Particularly the convergence of Blockchain and AI seems to be very promising, e.g. management of moveable autonomous devices. 7. From value tracing perspective, fields such as (1) finance; (2) virtual reality; (3) asset management; (4) various business functions, including document management and manufacturing; (5) tracing IoT data; (6) e-commerce; (7) security; and (8) healthcare, could be interesting fields for industrial actors.
State	1. From "Internet of Money" perspective, the integration between the digital world and the physical world should be enabled by law, e.g. Initial Coin Offering (ICO) and Security Token Offering (STO), where Blockchain is expected to become critical technology. 2. Blockchain's pervasion in our society is highly impacted by the fiscal policies which require special attention. 3. To tackle missing collaborations between industry, academia and the state, Blockchain specific innovation policies should be introduced. 4. Governments should promote the implementation of Blockchain as centralised traditional institutions in competition with Blockchain may stifle its development. This would certainly threaten the positive benefits that it offers society and the economy. 5. To enable distributed hash power in the global Blockchain field, international cooperation should be enabled so than the global hash power doesn't depend on a single country such as China. 6. Blockchain is expected to cause disintermediation, decentralisation and disruption of existing societal structures. This calls for Blockchain specific policies with the main focus on Blockchain as "Internet of Governance".
Academia	1. Academia should clearly define Blockchain and its categories as there is currently a rather arbitrary approach in this context. 2. Considering Blockchain as a potential GPT and given its open-source characteristics, academic institutions should support the education of citizens in the Blockchain context. This is as anyone can access the original Blockchain code and create their applications. 3. Academic institutions need to investigate the collaborative innovation processes and activities based on smart contracts and DAOs. This is so then the proper policies may be introduced to enable collaborative innovation. 4. Policymakers should introduce policies to leverage BoP to a higher level to contribute to the achievement of SDGs. 5. Blockchain patents are currently concentrated on (1) Value Management, (2) Asset Management, (3) Tracking, (4) Technology, (5) Documentation and Certification and (6) Governance and Interaction, which asks for particular attention by the academic actors.

V. CONCLUSION

The pervasive nature of Blockchain, in addition to its potential for changing production processes and creating new technologies, has raised the question of whether Blockchain will be the next GPT. In this regard, this article aimed to understand the extent to which Blockchain may be considered as a GPT. This research differs from previous studies as it investigates approximately 2500 Blockchain-related patents according to six GPT characteristics, specifically pervasiveness, improvement capabilities, spawning capabilities, prevalence, reallocation of resources and inclusive democratisation, as identified during the literature review (see Section II-A). In this context, a mixed method, consisting of patentometrics and semi-structured interviews, was deployed to establish whether Blockchain may be considered to be a next-generation GPT.

By systematically examining the Blockchain-related patent data with a mixed method approach, this article has found preliminary evidence that Blockchain is a GPT, although the evidence is limited in terms of scope, coverage, and timing.

The contributions of this article are threefold:

1) a comprehensive list of GPT relevant parameters based on the work of GPT-related scholars;

2) a methodological examination of Blockchain, that is, a mixed-method approach investigating Blockchain from a GPT perspective based on Blockchain-related patents with Blockchain-related word thresholds;
3) practical contributions to the Blockchain field made by outlining Blockchain from the perspective of GPT-relevant parameters.

The important findings of this article are as follows:

1) Blockchain shows pervasive characteristics and is spread over various industrial fields;
2) Blockchain is capable of further improvement, while actors in Blockchain landscape are tackling the problems of Blockchain technology that are hindering its rapid adoption;
3) Blockchain facilitates and encourages the creation of new innovations, showing technological spawning capabilities;
4) several countries with strong R&D capability, particularly China and the US, are showing the prevalence of Blockchain technology;
5) the Blockchain landscape demonstrates reallocation of resources characteristics, while disrupted market conditions enable the emergence of new actors with distributed innovation network characteristics;
6) as disruptive institutional technology, Blockchain has the potential to enable inclusive democratisation, thanks to its financial and social inclusion characteristics.

This article was likely to be of great interest to a broad spectrum of stakeholders, such as scholars and policymakers, who will be confronted with the associated benefits as well as the potential challenges raised by the appearance of Blockchain. The main implication of this article is that China and the US have the potential to influence the future development of Blockchain technology, while their competition is directly influenced by their so-called hash power. Chinese mining pools already control more than 70% of the Bitcoin network's collective hash power. Thus, China already has a significant influence on Blockchain, particularly in security-related topics. In conclusion, the competition between China and the US in the Blockchain field will define whether and to what extent Blockchain may become a GPT in the future.

Moreover, there are critical implications from a policy makers' perspective:

1) industrial actors should concentrate on the most significant application fields of the "Internet of Money":
   a) identity solutions;
   b) logistics;
   c) energy;
   d) mobility;
   e) healthcare;
2) the biometric data of BoP citizens may be securely stored on Blockchain, so BoP might be included in the civilized world and, in this context, industrial actors could provide solutions for the unbanked people of BoP;
3) integration between the digital world and the physical world should be enabled by law, for example Initial Coin Offerings (ICOs) and Security Token Offerings (STOs), in which Blockchain is expected to become critical technology;
4) governments should promote the implementation of Blockchain, as centralized traditional institutions in competition with Blockchain may stifle its development, which would certainly threaten the positive benefits that it offers to society and the economy;
5) considering Blockchain as a potential GPT with open-source characteristics, academic institutions should support the education of citizens in the Blockchain context, as anyone may access the original Blockchain code and create applications.

This article was subject to the usual limitations of studies attempting to investigate the characteristics of emerging technologies based on patents:

1) despite many advantages, patent data have several limitations, as not all innovative activity is reflected in the patent system; and 2) a given patent class, which is assigned by patent examiners, does not correspond to a technological field. Thus, future studies aiming to investigate the GPT characteristics of Blockchain technology should consider additional data sources, such as academic journals.

ACKNOWLEDGMENT

The authors would like to thank to Blockchain experts for their contributions in this article. The contributions in this article by Dr. S. Ozcan was prepared within the framework of the Basic Research Program of the National Research University Higher School of Economics.

REFERENCES

[1] E. Kane, "Is blockchain a general purpose technology?" 2017, doi: 10.2139/ssrn.2932585.
[2] E. Filippova, A. Scharl, and P. Filippov, "Blockchain: An empirical investigation of its scope for improvement," in *Proc. Int. Conf. Blockchain*, 2019, pp. 1–17.
[3] E. Filippova, "Empirical evidence and economic implications of blockchain as a general purpose technology," in *Proc. IEEE Technol. Eng. Manage. Conf.*, 2019, pp. 1–8.
[4] T. F. Bresnahan and M. Trajtenberg, "General purpose technologies 'Engines of growth'?" *J. Econometrics*, vol. 65, no. 1, pp. 83–108, 1995.
[5] M. Coccia, "General purpose technologies in dynamic systems: visual representation and analyses of complex drivers," CNR-IRCRES, Moncalieri, Italy, Working Paper 201705, 2017.
[6] E. Helpman and M. Trajtenberg, "A time to sow and a time to reap: Growth based on general purpose technologies," Nat. Bureau Econ. Res., Cambridge, MA, USA, Working Paper no. 4854, 1994.
[7] K. I. Carlaw and R. G. Lipsey, "Productivity, technology and economic growth: what is the relationship?" *J. Econ. Surv.*, vol. 17, no. 3, pp. 457–495, 2003.
[8] M. Coccia, "General sources of general purpose technologies in complex societies: Theory of global leadership-driven innovation, warfare and human development," *Technol. Soc.*, vol. 42, pp. 199–226, 2015.
[9] J. Youtie, M. Iacopetta, and S. Graham, "Assessing the nature of nanotechnology: Can we uncover an emerging general purpose technology?" *J. Technol. Transfer*, vol. 33, no. 3, pp. 315–329, 2008.
[10] E. Calvano, "Destructive creation," Stockholm School Econ., Stockholm, Sweden, SSE/EFI Working Paper Series in Economics and Finance, no. 653, 2006.
[11] B. Jovanovic and P. L. Rousseau, "General purpose technologies," in *Handbook of Economic Growth*. New York, NY, USA: Elsevier, 2005, pp. 1181–1224.

[12] G. Ozdagoglu, M. Damar, and A. Ozdagoglu, "The state of the art in blockchain research (2013–2018): Scientometrics of the related papers in web of science and scopus," in *Digital Business Strategies in Blockchain Ecosystems*. Cham, Switzerland: Springer, 2020, pp. 569–599.
[13] M. Dabbagh, M. Sookhak, and N. Sohrabi Safa, "The evolution of blockchain: A bibliometric study," *IEEE Access*, vol. 7, pp. 19212–19221, 2019.
[14] S. Davidson, P. De Filippi, and J. Potts, "Blockchains and the economic institutions of capitalism," *J. Institutional Econ.*, vol. 14, no. 4, pp. 639–658, 2018.
[15] M. Isaja and A. Calà, "Blockchain as a key enabling technology for decentralized cyber-physical production systems".
[16] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1421–1428, Sep. 2018.
[17] U. Cantner and S. Vannuccini, "A new view of general purpose technologies," *Jena Econ. Res. Papers*, Friedrich Schiller University Jena and Max Planck Institute of Economics, Jena, 2012.
[18] J. P. Conley, "Blockchain as a decentralized mechanism for financial inclusion and economic mobility," Dept. Econ., Vanderbilt Univ., Nashville, TN, USA, Working Paper, 2019.
[19] R. G. Lipsey, K. Carlaw, and C. T. Bekar, "Economic transformations: general purpose technologies and long-term economic growth," New York, NY, USA: Oxford Univ. Press, 2005.
[20] B. J. van der Kooij, "How did the general purpose technology 'electricity'contribute to the second industrial revolution (I): The power engines," 2017.
[21] A. Laino, "General purpose technologies: characteristics and impact on economic growth," *Int. J. Academic Res. Bus. Social Sci.*, vol. 9, no. 2, pp. 734–748, 2019.
[22] P. A. David, "The dynamo and the computer: An historical perspective on the modern productivity," *Amer. Econ. Rev.*, vol. 80, no. 2, pp. 355–361, 1990.
[23] P. A. David and G. Wright, "General purpose technologies and productivity surges: Historical reflections on the future of the ICT revolution," *Econ. Hist.*, 2005, Art. no. 502002.
[24] G. Thoma, "Striving for a large market: evidence from a general purpose technology in action," *Ind. Corporate Change*, vol. 18, no. 1, pp. 107–138, 2008.
[25] S. J. Graham and M. Iacopetta, "Nanotechnology and the emergence of a general purpose technology," *Ann. Econ. Statist.*, vol. 115, pp. 25–55, 2009.
[26] A. Rainer and R. Strohmaier, "Modeling the diffusion of general purpose technologies in an evolutionary multi-sector framework," *Empirica*, vol. 41, no. 3, pp. 425–444, 2014.
[27] M. Coccia, "A theory of the general causes of long waves: War, general purpose technologies, and economic change," *Technol. Forecast. Soc. Change*, vol. 128, pp. 287–295, 2018.
[28] M. Coccia, "Democratization is the driving force for technological and economic change," *Technol. Forecast. Soc. Change*, vol. 77, no. 2, pp. 248–264, 2010.
[29] L. Schultz and F. Joutz, "Methods for identifying emerging general purpose technologies: A case study of nanotechnologies," *Scientometrics*, vol. 85, no. 1, pp. 155–170, 2010.
[30] N. Rosenberg and M. Trajtenberg, "A general-purpose technology at work: The Corliss steam engine in the late-nineteenth-century United States," *J. Econ. Hist.*, vol. 64, no. 1, pp. 61–99, 2004.
[31] M. Coccia, "Effects of the institutional change based on democratization on origin and diffusion of technological innovation," Nat. Res. Council Italy, Rome, Italy, Working Paper, 2020.
[32] M. Coccia, "The Fishbone diagram to identify, systematize and analyze the sources of general purpose technologies," *J. Social Administ. Sci.*, vol. 4, no. 4, pp. 291–303, 2018.
[33] M. Tarafdar, R. Singh, and P. Anekal, "Impact of ICT-enabled product and process innovations at the bottom of the pyramid: A market separations perspective," *J. Inf. Technol.*, vol. 28, no. 4, pp. 279–295, 2013.
[34] S. Davidson, P. de Filippi, and J. Pot, "Economics of blockchain," in *Proc. Public Choice Conf.*, 2016.
[35] M. Swan, *Blockchain: Blueprint for a New Economy*. New York, NY, USA: O'Reilly Media Inc., 2015.
[36] C. Ehmke, F. Blum, and V. Gruhn, "Properties of decentralized consensus technology–why not every blockchain is a blockchain," 2019, *arXiv:1907.09289*.
[37] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *Proc. 17th Int. Symp. INFOTEHJAHORINA*, 2018, pp. 1–6.
[38] T. Abbate, F. Cesaroni, M. C. Cinici, and M. Villari, "Exploiting internet-of-things: Platforms and business models," in *Governing Business Systems*. Cham, Switzerland: Springer, 2018, pp. 101–118.
[39] A. Goldfarb, B. Taska, and F. Teodoridis, "Could machine learning be a general-purpose technology? Evidence from online job postings," 2019, doi: 10.2139/ssrn.3468822.
[40] J. Klinger, J. C. Mateos-Garcia, and K. Stathoulopoulos, "Deep learning, deep change? Mapping the development of the artificial intelligence general purpose technology, "2018.
[41] M. Swan, "Blockchain for business: Next-generation enterprise artificial intelligence systems," in *Advances in Computers*. New York, NY, USA: Elsevier, 2018, pp. 121–162.
[42] C. Freeman and L. Soete, *The Economics of Industrial Innovation*, 3rd ed. London, U.K.: Cassell, 1997.
[43] B. Bruens and M. G. Moehrle, "Understanding the diffusion of the blockchain technology: A patent-based Analysis using the tf-lag-idf for Term Novelty Evaluation," in *Proc. Portland Int. Conf. Manage. Eng. Technol.*, 2018, pp. 1–7.
[44] M. Kamran, H. U. Khan, W. Nisar, M. Farooq, and S.-U. Rehman, "Blockchain and internet of things: A bibliometric study," *Comput. Elect. Eng.*, vol. 81, 2020, Art. no. 106525.
[45] M.-D. L. Seidel, "Questioning centralised organisations in a time of distributed trust," *J. Manage. Inquiry*, vol. 27, no. 1, pp. 40–44, 2018.
[46] U. D. Jogulu and J. Pansiri, "Mixed methods: A research design for management doctoral dissertations," *Manage. Res. Rev.*, vol. 34, pp. 687–701, 2011.
[47] N. V. Ivankova, J. W. Creswell, and S. L. Stick, "Using mixed-methods sequential explanatory design: From theory to practice," *Field Methods*, vol. 18, no. 1, pp. 3–20, 2006.
[48] C. Teddlie and A. Tashakkori, "Mixed methods research," in *The Sage Handbook of Qualitative Research*. New York, NY, USA: SAGE, 2011.
[49] S. Ozcan and N. Islam, "Patent information retrieval: Approaching a method and analysing nanotechnology patent collaborations," *Scientometrics*, vol. 111, no. 2, pp. 941–970, 2017.
[50] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, 2016, Art. no. e0163477.
[51] W. Viriyasitavata, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *J. Ind. Inf. Integration*, vol. 15, pp. 21–28, 2019.
[52] S. Sanju, S. Sankaran, and K. Achuthan, "Energy comparison of blockchain platforms for Internet of Things," in *Proc. IEEE Int. Symp. Smart Electron. Syst.*, 2018, pp. 235–238.
[53] I. Merediz-Solà and A. F. Bariviera, "A bibliometric analysis of Bitcoin scientific production," *Res. Int. Bus. Finance*, vol. 50, pp. 294–305, 2019.
[54] S. Unalan and S. Ozcan, "Democratising systems of innovations based on Blockchain platform technologies," *J. Enterprise Inf. Manage.*, 2020, doi: 10.1108/JEIM-07-2018-0147.
[55] M. Swan, "Anticipating the economic benefits of blockchain," *Technol. Innov. Manage. Rev.*, vol. 7, no. 10, pp. 6–13, 2017.
[56] K. P. Donovan, "Mobile money, more freedom? The impact of M-PESA's network power on development as freedom," *Int. J. Commun.*, vol. 6, no. 23, pp. 2647–2669, 2012.