IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INTERNET-OF-THINGS ATTACKS AND DEFENSES: RECENT ADVANCES AND CHALLENGES

Received January 4, 2021, accepted January 9, 2021, date of publication January 14, 2021, date of current version January 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3051602

Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network

SAURABH SINGH[1], A. S. M. SANWAR HOSEN[2], AND BYUNGUN YOON[1], (Senior Member, IEEE)

[1]Department of Industrial and Systems Engineering, Dongguk University, Seoul 04620, South Korea
[2]Division of Computer Science, Jeonbuk National University, Jeonju 54896, South Korea

Corresponding author: Byungun Yoon (postman3@dongguk.edu)

This work was supported in part by the National Research Foundation of Korea under Grant 2019R1A2C1085388, and in part by the Dongguk University Research Fund of 2020 under Grant S-2020-G0001-00050.

ABSTRACT Blockchain technology is becoming increasingly attractive to the next generation, as it is uniquely suited to the information era. Blockchain technology can also be applied to the Internet of Things (IoT). The advancement of IoT technology in various domains has led to substantial progress in distributed systems. Blockchain concept requires a decentralized data management system for storing and sharing the data and transactions in the network. This paper discusses the blockchain concept and relevant factors that provide a detailed analysis of potential security attacks and presents existing solutions that can be deployed as countermeasures to such attacks. This paper also includes blockchain security enhancement solutions by summarizing key points that can be exploited to develop various blockchain systems and security tools that counter security vulnerabilities. Finally, the paper discusses open issues relating to and future research directions of blockchain-IoT systems.

INDEX TERMS Blockchain, Internet of Things, threats and attacks, security.

I. INTRODUCTION

Blockchain technology, a distributed digital ledger technology that can be used to maintain continuously growing lists of data records and transactions securely, has recently taken the world by storm. The three main criteria related to blockchain identity and accessibility are public or less authorized, private or authorized, and consortium. The most important and unique factor of the blockchain concept is that the stored information is secured entirely within the blocks of the blockchain's transactions. Its decentralized consensus model has the three main features of consistency, aliveness, and fault tolerance [1]–[3].

Blockchain technology has been successfully applied in a wide variety of areas. When blockchain technology is implemented in the Internet of Things (IoT) domain to exchange and share network data, records, validation, and security service, there are a few relevant issues that are still being researched, with a particular focus on the security of cyber-physical systems in the IoT sector. Many authorized organizations are currently working to ensure proper interoperability, integrity, and privacy of the IoT network. These organizations are all working together using blockchain technology and cloud computing. The technology brings transparency, reliability, and proper governance to the IoT information system [4]–[7].

Blockchain technology is redefining data modeling, and governments have implemented blockchain in many IoT applications. It is mainly attractive for such applications due to its unprecedented ability to adapt as well as the segment, protect, and share IoT data and services. Blockchain technology is at the center of many current developments in the IoT industry. One reason for this is that many IoT services are vulnerable to attacks and challenges. Using blockchain technology can solve many of the issues with cyber-physical systems in the IoT sector. As the IoT industry is moving toward a network sensor model, sustainable smart cities, and the many components involved must be framed in consideration of certain benefits [8]–[12].

Moreover, blockchain enables different privacy-preserving models for IoT applications, such as data privacy, user privacy, location privacy, privacy-preserving aggregation, and

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

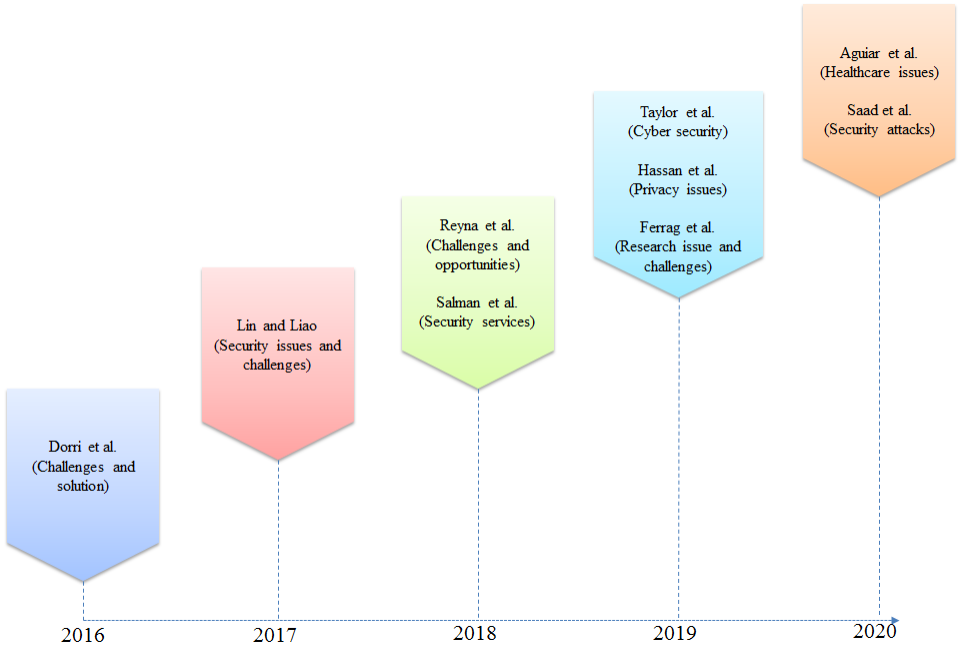


FIGURE 1. Roadmap of different literature on security issues, attacks, and solutions in blockchain technology between 2016 and 2020.

many others. Ferrag *et al.* [13] suggested many privacy-preserving schemes and presented a side-by-side comparison of different security and privacy approaches for Fog-based IoT applications. Dwivedi *et al.* [14] proposed a scheme of modified blockchain models in the medical sector that involves additional protection and privacy parameters based on advanced cryptographic primitives. This scheme uses lightweight digital signatures to guarantee that the information cannot be improperly modified, and a tamper-proof seal protects it. Privacy-preserving methods for IoT data in smart cities have been discussed by Shen *et al.* [15]. Support vector machine training is used with blockchain technology to enable it to handle smart city data. The blockchain techniques allow for secure and reliable IoT data between data providers, where each provider can encrypt the data instance locally using its private key.

In the move toward numerous beneficial features such as decentralization, persistence, anonymity, and auditability, security is a major concern. This paper provides an inclusive overview of blockchain parameters and security attacks in cyber-physical systems. It also presents some existing solutions and blockchain applications for various factors that can affect the blockchain system. Blockchain technology has attracted substantial industrial and academic attention due to its decentralization, persistence, anonymity, and auditing attributes. In this survey, we consider the implementation of blockchain technology in a wide range of applications and discuss a number of the challenges involved.

A. CONTRIBUTION

1) To the best of our knowledge, this is the first study of its kind to survey blockchain attacks in IoT networks and provide solutions for such attacks.
2) This review presents the essential background knowledge needed for blockchain and its elements, participants, and components along with their functionalities. The goal is to familiarize readers with the blockchain system. Moreover, this paper systematically presents and discusses the security limitations, vulnerabilities, challenges, and issues associated with blockchain technology, as well as security issues in blockchain enterprises.
3) This paper discusses the widespread security attacks on blockchain technologies and their vulnerabilities based on the results of many existing studies. Moreover, various applications and opportunities involved in blockchain technology are also discussed.
4) This survey presents existing security solutions for blockchain technology in different environments. Finally, this paper discusses some security tools that can address these security vulnerabilities. It also outlines some open questions and research challenges, and open requirements that could improve blockchain-IoT capability.

B. ROADMAP AND COMPARISON WITH RELATED SURVEY ARTICLE

Fig. 1 shows a roadmap of the various kinds of surveys related to blockchain technology presented from 2016 to 2020. Dorri *et al.* considered IoT security and privacy issues and vulnerabilities [S1]. The authors also provided a blockchain-based solution. Lin and Liao [S2] surveyed the blockchain security issues and challenges as well as the different kinds of attacks. They also briefly discussed other blockchain applications such as Bitcoin, Ethereum, and hyper ledger.

Reyna *et al.* surveyed blockchain technology with a focus on feature analysis and challenges, as well as the integration of blockchain and IoT through different identification and analysis methods. Applications based on blockchain-IoT are also discussed. However, there is limited research on security attacks, although a solution has been proposed by Reyna *et al.* [S3]. Salman *et al.* [S4] illustrated blockchain-based approaches for several security services, including resource provenance, confidentiality, authentication, integrity assurance, and privacy.

They also discussed some of the challenges and issues associated with blockchain-based security services, and provided insight into security services in current applications and techniques. Taylor *et al.* [S5] provided a systematic literature survey on blockchain cybersecurity, including research-type applications, and reported key qualitative/quantitative data. They also discussed future research directions in blockchain for IoT security, artificial intelligence (AI) data security, and the release of open-source software and datasets. Hassan *et al.* [S6] discussed privacy-preserving features in blockchain-based IoT systems. The authors focused on presenting the practical issues caused by privacy leakages in IoT operating systems, analyzing the implementation of privacy protection, and outlining the various issues associated with the privacy protection of blockchain-based IoT systems. Ferrag *et al.* [S7] discussed different application domains of blockchain–IoT, such as IoV, IoE, IoC, edge computing, and others. They reviewed the anonymity and privacy of the bitcoin system and provided a taxonomy with a side-by-side comparison of state-of-the-art privacy-preserving blockchain technology. Aguiar *et al.* [S8] surveyed blockchain-based strategies for healthcare applications. They analyzed the tools employed by industries in that area to construct blockchain networks. The paper also discussed privacy techniques and access control employed in healthcare records using case scenarios for monitoring patients in remote care environments. Saad *et al.* [S9] systematically explored the attack surface in terms of blockchain cryptographic construct, distributed architecture, and blockchain application context, while providing detailed solutions and opportunities.

This paper is organized as follows: Section II explains blockchain technology and its related factors. Section III provides details about blockchain security attacks, and section IV discusses the blockchain security issues. Section V discusses blockchain challenges, and Section VI surveys the different blockchain technology solutions for the challenges in various sectors. Section VII discusses open issues and potential future research directions. Finally, Section VIII concludes the paper.

II. BLOCKCHAIN FACTORS and ISSUES

This section discusses the key factors and issues related to blockchain implementation in smart networks, including existing solutions and recommendations.

A. ELEMENTS IN BLOCKCHAIN AND RELATED CONCERNS

1) DECENTRALIZATION

In blockchain technology, decentralization entails dispersing functions throughout a system rather than having all units connected with and controlled by a central authority; in other words, there is no central point of control, and this absence of centralized authority in a blockchain is what makes it more secure than other technologies. Each blockchain user, called a miner, is assigned a unique transaction account, and blocks are added once the miners are validated. The decentralized nature of the data records used in blockchain technology exemplifies its revolutionary quality; blockchain networks use consensus protocols to secure nodes. In this way, transactions are validated and data cannot be destroyed. While the decentralized nature of networks allows for peer-to-peer operations [16], it also poses major challenges to personal data privacy [17]. Gai *et al.* [18] surveyed some of these security and privacy issues, which include threats, malicious adversaries, and attacks in financial industries. Zyskind *et al.* [19] examined decentralized personal data management in the context of personal data privacy concerns.

2) CONSENSUS MODEL

Consensus refers to agreement among entities [20], and consensus models help decentralized networks make unanimous decisions. This allows for all records to be tracked from a single authority. Blockchain technology requires consensus algorithms to ensure that each next block is the only true version; that is, the algorithms ensure that all nodes agree that each new block added to the blockchain carries the same message. Consensus models guarantee against ''fork attacks'' and can even protect against malicious attacks [21]. The three main features of consensus models are as follows:

1) *Consistency*- this protocol is safe and consistent when all nodes produce the same output.
2) *Aliveness*- the consensus protocol guarantees aliveness if all participating nodes have produced a result.
3) *Fault tolerance*- the mechanism delivers fault tolerance for recovery from failure nodes.

3) TRANSPARENCY AND PRIVACY

The most appealing aspect of blockchain technology is the degree of privacy it offers, but this can create some confusion regarding transparency. Blockchain networks periodically (i.e., every 10 minutes) self-audit the digital value ecosystems that coordinate transactions; one set of these transactions is called a block, and this process results in two properties: transparency and impossibility of corruption. In a blockchain, the identity of the user is hidden behind a strong cipher, making it particularly difficult to link public addresses to individual users. The question thus arises of how blockchain can be regarded as truly transparent [22].

Blockchain is already regarded as a powerful technology [23]. It organizes interactions in such a way that greatly

TABLE 1. Comparison of related surveys.

Article	Year	Focused on	Security Attacks	Classification	Opportunities	Applications	Solutions	Security tools
[S1]	2016	Proposing a secure, private, and lightweight architecture for IoT based on blockchain technology	Yes	No	No	No	Yes	No
[S2]	2017	Introducing preliminaries of blockchain and security issues in blockchain	No	No	No	Yes	No	No
[S3]	2018	Investigating the challenges in IoT applications integrated with blockchain.	Yes	No	Yes	Yes	No	No
[S4]	2019	Blockchain-based solutions for security issues.	No	No	No	No	Yes	No
[S5]	2019	Blockchain applications in cybersecurity	No	No	No	Yes	No	No
[S6]	2019	Privacy issues caused by the integration of IoT with blockchain	Yes	Yes	No	No	No	No
[S7]	2019	Surveying existing blockchain protocols used with IoT	Yes	Yes	No	Yes	Yes	No
[S8]	2020	Applications of blockchain in the healthcare domain	No	No	No	No	Yes	No
[S9]	2020	Exploring the attack surface of the public blockchain	No	Yes	No	Yes	Yes	No
This Survey	2020	All of the above	Yes	Yes	Yes	Yes	Yes	Yes

improves reliability while also eliminating the business and political risks associated with managing processes through central entities, thus reducing the need for trust. Blockchain networks create platforms that can simultaneously run different applications from different companies, enabling seamless and efficient dialogue and the creation of audit trails through which everyone can verify that everything is being processed correctly.

4) IDENTITY AND ACCESS

Blockchain is a secure distributed ledger technology (DLT) that has taken on a new role in recent years. Jacobovitz *et al.* [24] discussed the state of the art in blockchain technology, applications, and solutions regarding identity management. Taking identity and access control to the next level and investigating whether the use of blockchain technology improves the management of device ID comprises one of the priority security projects of Sentara Healthcare, and Virginia and North Carolina are connected via an integrated distribution system [25]. According to industry expert Jeremy Kirk, there are currently six ongoing projects addressing how blockchain could make it easier to manage identity: Hyperledger Independent, Civic, Sovran, Evernym, Alastria, and uPort.

The three main criteria related to blockchain identity and accessibility are public or less authorized, private or authorized, and consortium. Pilkington [26] presented the main distinction between public and private blockchain technologies and discussed the foundations and disruptive nature of blockchain technology. Public blockchains are completely open and allow anyone to join the network; they are designed to reduce intermediaries so that more participants can join. By contrast, private blockchains restrict network privileges; participants need permission to join and the access control mechanism can change.

5) OPEN SOURCE

With distributed and closed-source applications, users must trust the applications, and they cannot access any data from central sources. It is possible to launch decentralized closed-source applications and achieve desired results, but doing so would have catastrophic consequences. This is a major reason that participants prefer decentralized open-source applications, with relevant platforms including Ethereum, Bitcoin cash, Litecoin, and Dash. Sidechain-capable blockchain platforms provide powerful benefits developed by community members such as

1) flexible configurations: no risk in multi-block reorganization and enables rapid transactions,
2) confidential transactions: leveraging stability,
3) federated two-way peg: issuing multi-transferrable assets on single blockchains, and
4) multiple assets issuance: secured by a federation of parties with aligned incentives.

Open-source applications help users adopt new technologies. One of the main features of such applications, as emphasized by Buterin [23], is an open-source license model and government mechanism that enables changes in public ledger currency platforms or blockchain applications. Tech giant IBM has helped evolve open-source technologies by promoting projects such as Linux Foundation's Hyperledger Composer; regarding enterprise ecosystems, MentaGo provides a blockchain solution for financial systems and SXSW uses Hyperledger fabric and IBM [27], [28].

6) ANONYMIZATION

Anonymity is one of the most important elements (shown in Fig. 2) in blockchain technology for maintaining the privacy of transactions in networks, but ensuring anonymity is difficult because the blockchain ledger is public. Each user generates an address, and there is no mechanism for

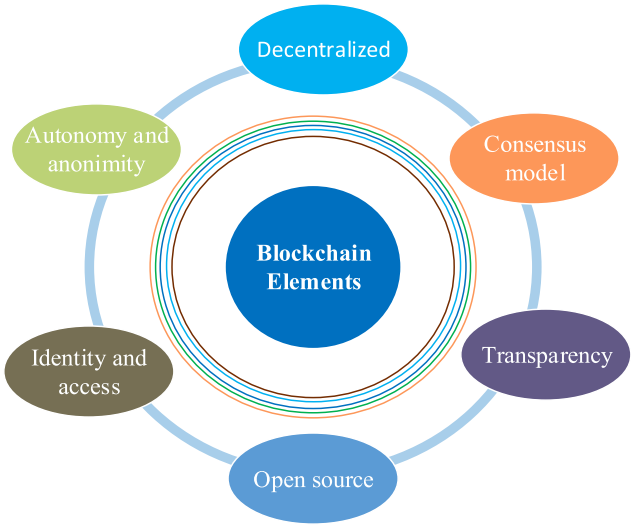


FIGURE 2. Blockchain elements.

keeping user information private. This is why Bitcoin is considered pseudo-anonymous: users can be linked with their public addresses, but it is not possible to learn their actual names or addresses [29]. Möser [30] presented an article on the anonymity of Bitcoin transactions in which a special Bitcoin mixing service was proposed that could complicate or confuse originating Bitcoin transaction addresses and thereby increase anonymity. The main security concern with blockchain is that public keys and transactions must not reveal real identities.

B. BLOCKCHAIN PARTICIPANTS AND RELATED CONCERN

Blockchain networks allow participants to reach consensus, and they also store data that can be accessed by all participants. Here, we discuss the different roles of blockchain network participants.

1) BLOCKCHAIN USERS

Users operate in blockchain networks, and their numbers have increased exponentially since 2011, according to Blockchain.info. This statistical portal also reported that the number of blockchain users was expected to reach 50 million by the end of 2020 [31]. There is a privacy issue facing blockchain users in the network.

2) BLOCKCHAIN REGULATOR

Achieving overall authority in business networks may require broad access to ledger contents. Kakavand *et al.* [32] presented an in-depth analysis of the current regulatory landscape of distribution technology, and Yeoh [33] discussed the regulatory issues involved with blockchain technology. He addressed the key regulatory challenges associated with innovative distributed blockchain technology across Europe and the United States.

3) BLOCKCHAIN DEVELOPER

Developers design both the applications and the smart contracts used by blockchain users. There are significant market opportunities for developers to cryptographically ensure the accuracies of the ledgers at the hearts of cryptocurrencies. Nordrum [34] presented a time frame for blockchain developers and described that developers have limited software tools with which to build secure blockchain ledgers.

4) CERTIFICATE AUTHORITY

This manages the heterogeneous certificates needed to run a permissioned blockchain using a trusted third party; Bitcoin and Ethereum are examples of permissioned blockchains. The authority authorizes the limited set of legitimate readers or writers [35]. The main issue in blockchain networks is trust. To address the issue of trust, blockchains distribute ledgers among many servers under different control authorities, but there is still a bootstrap problem associated with finding initial ledgers [36].

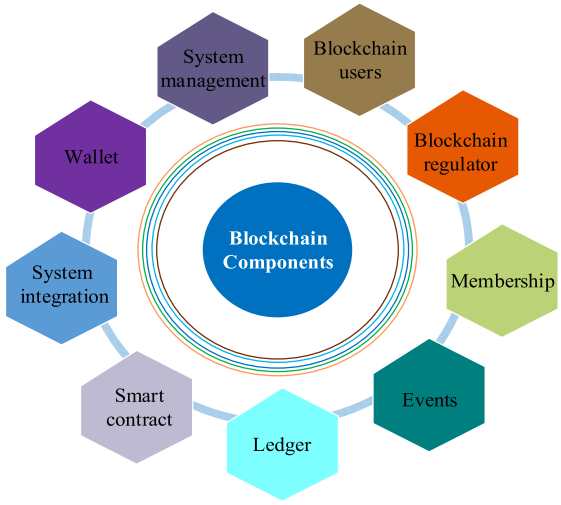


FIGURE 3. Blockchain components.

C. BLOCKCHAIN COMPONENTS

Fig. 3 shows many of the essential components of a blockchain. Detailed descriptions of each component are as follows:

Ledger: Contains the current world state of the blockchain transactions.

Smart Contract: Encapsulates the business network transactions into code. A transaction call causes the ledger state to be retrieved and set.

Consensus network: A set of data and processing peers that continually maintain the replicated ledger.

Membership: Manages identity and transactional certificates and other aspects of access rights.

Events: Generates notifications about important actions in the blockchain (such as new blocks) as well as notifications related to smart contracts with no event distribution.

System management: Provides the ability to create, change, and monitor blockchain components.

Wallet: Securely manages security credentials.

System Integration: Is responsible for integrating blockchains in a bidirectional manner with external systems.

D. SUMMARY AND INSIGHTS

Section II has discussed the security concerns and benefits of blockchain elements, such as decentralization, which pose major challenges for data privacy and transparency and lead to confusion in the network. In addition, the open-source and anonymous nature provide flexible configuration, confidentiality, and privacy in transactions. We have also discussed the security concerns of blockchain participants and components.

III. ATTACKS

In this section, we present different blockchain network applications and attacks as well as future opportunities in various sectors. For this subsection, we surveyed real blockchain attacks that commonly occur. We also referred to Li *et al.* [37], who discussed blockchain attacks and security risks. Here, we discuss some of these attacks in further detail.

1) Liveness Attack: Kiayias and Panagiotakos [38] stated that these attacks can delay the acknowledgment times of target transactions, and presented two examples of such attacks against Bitcoin and Ethereum. The liveness attack proceeds in three stages: preparation, transaction denial, and blockchain delay [39]. This attack delays the transaction confirmation time. In the preparation phase, the attacker tries to gain a potential advantage against honest players to build their private chain. Next is the transaction denial phase, in which the attacker attempts to delay the genuine block that contains the transaction, and when the attacker decides the delay is unconvincing, they proceed to the blockchain render phase, where they try to decrease the rate at which the chain transaction grows.

2) Double Spending Attacks: This problem is generated when one successful transaction is duplicated with the same funds; it represents a potential flaw in digital cash, as the same digital token can be spent two times when such an attack occurs. It is impossible to avoid double-spending, even though the blockchain consensus mechanism validates all transactions [40]. The authors of a research study by the Bank of Canada said that ''if a miner controls more than half of computational capacity amongst all miners, in theory, loses their power to control double spending incentives. A malicious miner can do this or dishonest who creates a larger arrival rate than the sum of all other legitimate or honest miners'' [41], [42]. Attacks related to double spending include race, Finney, 51%, and Vector 76 attacks.

3) 51% Vulnerability Attack: Blockchains rely on distributed consensus mechanisms to establish mutual trust. However, there is a 51% vulnerability in the consensus mechanism that an attacker can exploit to control the entire blockchain. Specifically, in a PoW-based blockchain, if a single minor hash function occupies more than 50% of the entire blockchain's total hash function, a 51% attack may be initiated. Thus, if the mining power is concentrated in several mining pools, unexpected situations can arise, such as a case in which a single pool controls more than half of all computing power. For example, in one real case, the mining pool ''ghash.io'' accounted for more than 42% of the total bitcoin mining power. The fact that a single mining pool represented such a high proportion was a serious concern, and many miners dropped out of the pool [43]. By starting a 51% attack, an attacker can arbitrarily manipulate and change blockchain information and perform the following actions [44], [45]:

1) reverse the transaction and initiate a double-spending attack
2) exclude and specify transaction orders
3) obstruct the general mining operations of other miners
4) impede the verification of normal transactions

4) Private Key Security Attack: A private key allows individuals to access funds and verify transactions; it is only created once and cannot be recovered if lost. Malicious actors perform a variety of actions to steal cryptocurrency by targeting key custodial services because cryptographic keys are particularly attractive targets. An attacker who has discovered vulnerability in an elliptic curve digital signature algorithm can recover a user's private key, and if a private key is stolen, it is difficult to track any related criminal activity and recover the relevant blockchain information [45]–[49]. FireEye Threat Intelligence has detected several prominent crimeware families with this functionality: Dridex, Terdot, IceID, SmokeLoader, BlackRubyRansomware, and Corebot.

5) Transaction Privacy Leakage: Because user behavior in blockchains is traceable, a blockchain system must take some measures to protect users' transaction privacy. However, some leakage of confidential information such as cryptographic keys can still occur, leading to the potential for people to commit real-world crimes. For instance, Bitcoin and Zcash use a one-time account to store received cryptograms, and users must also assign a secret key to each transaction. In this way, an attacker cannot infer whether the same transaction has involved a password violation by another person. Moreover, an attacker cannot infer the actual coin's linkage consumed by the transaction because the user can include several chaffcoins (called ''mixins'') when starting the transaction [50].

Wallet privacy leakage can also occur, where common bitcoin wallet operations leak some user information [51]; this leakage has been exploited in the past. Paul Fremantle *et al.* [52] proposed an architecture for IoT security and privacy that resolves the leakage issue.

6) Selfish Mining Attack: Selfish mining attacks are committed by some miners to waste legitimate miners' computing power or obtain unearned rewards. Such attackers attempt to fork the private chain by making the discovered block private [53], then self-employed miners try to maintain a longer private branch than the public branch to dig through this private chain and personally hold more newly found blocks; during this time, honest miners continue to dig in the

public chain [54]. As the public domain approaches the length of the private branch, the new block mined by the attacker is revealed, thus wasting honest miners' computing power and keeping them from earning what they should earn. As a result, the selfish miners gain a competitive advantage over real miners [55]. By further strengthening attackers' mining rights, these attacks undermine the intended decentralized nature of blockchain technology.

7) DAO Attack: Decentralized autonomous organizations (DAOs) have been used as venture capital funds for crypto and distributed spaces because the lack of centralized authority minimizes costs and provides investors with more control and access. The cost savings coding framework in the absence of central power was developed by the German startup Slock.it as an open-source platform for building smart locks, but it was fully deployed underneath and distributed to "The DAO," a member of the Ethereum community [56], [57].

Ethereum deployed DAO as a smart contract in 2016 on a crowdfunding platform. The DAO contract was assaulted after being deployed for 20 days. It had raised approximately US$120 million before the attack, and the attacker stole around $60 million, making it the largest attack on the Ethereum consensus model. In this case, the attacker exploited reentrant vulnerability. First, the attacker exposed a malicious smart contract with a callback function, including the DAO's withdrawal function call. Withdraw () sent Ether to the called party, and this also occurred in the form of a call. Therefore, the malicious smart contract's callback function was called again. In this way, an attacker was able to steal all the Ether from DAO. Smart contract vulnerabilities have been exploited in other cases as well [58].

8) BGP Hijacking Attack: The Border Gateway Protocol (BGP) is used to share routing information networks on the internet, which specify how IP packets are forwarded to their destinations. An attacker can intercept the blockchain network by manipulating the BGP, after which data can be routed and the traffic can be modified to the attacker's favor [56].

Apostolakiet al. [59] considered small- and large-level attacks targeting individual nodes or the whole network and their impacts on Bitcoin. Due to the increased concentrations of some of Bitcoin's mining pools, BGP hijacking represents a major vulnerability; an attacker can effectively divide the Bitcoin network and slow the block propagation speed. As stated by Dell SecureWorks in 2014, BGP hijacking intercepts connections to the Bitcoin mine's mine pool server [60].

9) Balance Attack: For a balance attack, an attacker simply introduces a delay between valid subgroups with the same mining power, then executes the transaction in one of these subgroups. Next, the attacker mines enough blocks in other subgroups to ensure that the subtree of the other subgroup is more important than the transaction subgroup. Even if a transaction is not committed, an attacker can create a block with such a transaction that has a high probability of exceeding the subtree that contains this transaction.

10) Sybil Attack: This attack destroys the reputation system in a computer security system by forging an identity in the peer-to-peer network. If nodes are required to prove their identities before joining the network, as is the case in permissioned or private blockchains, they will not be able to forge identities. Soska and Christin (2015) proposed the "Beaver" system, which protects users' privacy while resisting Sybil attacks by charging fees [61].

A. SUMMARY AND INSIGHTS

This section discusses different attacks on the blockchain network. We address the liveness attack, which delays the transaction confirmation time; double-spending attacks, which duplicate the transaction funds; 51% vulnerability attacks, where adversaries can exploit more than 50% in the consensus mechanism; and private Key security attacks, in which an attacker discovers a vulnerability in the elliptic curve digital signature used in encryption methods, privacy leakage, and self-mining. Other attacks are also explained in detail.

IV. BLOCKCHAIN SECURITY ISSUES

1) Transaction Malleability: During contracted transactions, the agreement does not immediately cover all the information in the hashed transaction; therefore, it is rare but possible for a node to change a transaction in the network in such a way that the hash is not validated. Christian Decker and Roger Wattenhofer defined transaction malleability as when transactions are intercepted, modified, and rebroadcast, thus leading the transaction legal entity to believe that the original transaction was not confirmed [62], [63].

2) Network Security: An eclipse attack occurs when an opponent controls pieces of network communication and logically divides the network to increase synchronization delay [61]; an example is a simple denial of service attack to improve selfish mining and double-spending [65], [66]. In eclipse attacks, an attacker selects and hides information from one or more participants, potentially by delaying the delivery of blocks to a node.

3) Privacy: Privacy and confidentiality are still major concerns with blockchain transactions because each node can access data from another node, and anyone viewing the blockchain can see all transactions [67]. Studies have suggested various ways to overcome this problem, but these methods are only practical for specific applications, and they do not cover all issues. Due to the enormous number of data transmissions, communications involving important data in the network might be attacked by some adversaries through attacks such as the man-in-the-middle (MitM) attack and the DoS/DDoS attack. IoT poses many unique privacy challenges, such as data privacy and tracking concerns for phones and cars. In addition, voice recognition is being integrated to allow devices to listen to conversations to actively transmit data to cloud storage for processing [68], [69].

4) Redundancy: Expensive duplication for the purpose of eliminating the arbitration that allows each node of the network to have a copy of every transaction. However, it is both financially and legally illogical to have redundant brokering; banks are not willing to perform every transaction with every

TABLE 2. Items available through criminal enterprises.

Category	Number of Items	Percentage (%)	Related Information and Title	Money Seized	Reference
Weed	3338	13.7	"From Seeds to Weed, Bitcoin Finds Home Where Commerce Goes Gray" (https://www.coindesk.com/bitcoin-atms-gray-areas)	$141.8 Billion	[74] [75]
Drugs	2194	9.0	"Blockchain in Action: Derailing Drug Abuse & Prescription Drug Fraud" (https://blockchain.wtf/2018/06/series/blockchain-in-action/derailing-drug-abuse/) "Tracing Illegal Activity Through the Bitcoin Blockchain To Combat Cryptocurrency" (https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/#18aa339b33a9)	$72 Billion	[76] [77]
Prescriptions	1784	7.3	"Bitcoin: Economics, Technology, and Governance" (https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213) "Blockchain Aims to Curb Prescription Drug Abuse" (https://hackernoon.com/blockchain-aims-to-curb-prescription-drug-abuse-47fc9cc66379)		[76] [78] [79] [80]
Benzodiazepines	1193	4.9	A class of psychoactive drugs	$3.6 Million	[79]
Cannabis	877	3.6	"Blockchain for Crime Prevention in the Legal Cannabis Space" (https://investingnews.com/innspired/blockchain-crime-prevention-legal-cannabis-space/)		[80] [81]
Hash	820	3.4	"The Future of Blockchain technology and cryptocurrencies" (https://skemman.is/bitstream/1946/30832/1/The%20future%20of%20blockchain%20technology%20and%20cryptocurrencies.pdf) "The Dark Side of Bitcoin" (https://blog.blockonomics.co/the-dark-side-of-bitcoin-illegal-activities-fraud-and-bitcoin-360e83408a32)		[82] [84]
Cocaine	630	2.6	"How the Feds Took Down the Silk Road Drug Wonderland" (https://www.wired.com/2013/11/silk-road/) "Heroin, Cocaine and LSD Sales Transactions Were Stopped Using Digital Currency BitCoin"		[83]
Pills	473	1.9	"Drug Dealers Are Using Bit Coins to Fund the Flooding-Fatal Fentanyl Waves in Foreign Countries" "From the Dark Side of Bitcoin: Misusing Cryptography" (https://99bitcoins.com/the-dark-side-of-bitcoin-misusing-cryptography/)	$10 million	[80] [84]

bank or complete other banks' transactions. Such duplication only increases costs while providing no conceivable benefits [70].

5) Regulatory Compliance: Blockchains exist regardless of the law, and government authorities do not necessarily change how they do their jobs in response to the existence of blockchains. Applying blockchain technology in the legal and financial sectors in non-Bitcoin currencies creates regulatory challenges, but infrastructure regulation is very similar to blockchain regulation [70]. Yeoh [33] discussed the key regulatory issues affecting the blockchain and innovation distributed technology that has been adopted across Europe and the United States.

6) Criminal Activity: Bitcoin-enabled third-party trading platforms allow users to purchase or sell a wide variety of products. These processes are anonymous, making it difficult to track user behavior and impose legitimate sanctions. Criminal activity involving Bitcoin frequently involves ransomware, underground markets, and money laundering [71]. Some underground markets that operate online trade as Tor hidden services use Bitcoin exchange currency, thus making blockchain availability uncertain because of criminal activity. Table 2 lists the top 10 item available categories [72].

7) Vulnerabilities in Smart Contracts: When a program is executed in a blockchain, a smart contract can have security vulnerabilities caused by a flaw in that program. For instance, the authors of one study found that "8,833 out of 19,366 Ethereum smart contracts are vulnerable" to bugs such as "(i) transaction-ordering dependence, (ii) timestamp dependence, (iii) mishandled exceptions, and (iv) reentrancy vulnerability" [71]. Table 3 presents the different vulnerabilities present in smart contracts as well as detailed causes of these vulnerabilities. Atzei *et al.* proposed a taxonomy of vulnerability and categorized the different types of vulnerabilities into levels that represent the vulnerabilities: solidity, Ethereum Virtual Machine (EVM), and blockchain [85]. The vulnerability causes contract issues with codifying, security, privacy, and system performance, including blockchain scalability.

Summary And Insights:

This section discusses the security issues associated with blockchain in terms of transaction malleability. This malleability is caused because information is not immediately covered in the hash transaction. This section also discusses the issues with network security where DoS attacks are possible, privacy and confidential effects due to MitM attacks,

TABLE 3. Smart contract vulnerabilities.

Vulnerability	Cause	Smart Contract	Level	Reference
Call to the unknown	Call to the unknown	Ethereum	Solidity	[85]
Gasless send	The recipient contract's fallback function *send* is invoked	Ethereum	Solidity	[86]
Field disclosure	Selfish miners published their private chain completely.	Bitcoin	Solidity	[87]
Exception disorder	Inconsistent in terms of exception handling while the call contract will not recognize errors that occur during execution.		Solidity	[88]
Reentrancy	A call that invokes back to itself through a chain of calls.	Ethereum	Solidity	[88]
Dangerous Delegate Call	DELEGATECALL opcode is identical to the standard message call	Wallet contract, Ethereum	Solidity	[88] [89]
Time stamp dependency	Vulnerability favoring a malicious miner by changing timestamp of StartTime, EndTime		Blockchain	[90]
Block number dependency	block.blockhash function associated with block.number as parameters for random number is being manipulated			[88]
Freezing ether	Freezing ether contract i.e., no transfer/send/call/suicide code within the current contract itself to transfer ether to other address	Wallet contracts		[88]
Immutable bug	Altered contract that cannot be patched.		EVM	[91]
Ether lost in transfer	Ether sent to an orphan address which did not belong to any particular contract or user	Cryptocurrency, Ethereum	EVM	[91]
Unpredictable state	User cannot predict the state of contract if he or she invokes the particular transaction		Blockchain	[85]
Randomness bug	Biasness behavior of malicious miner by arranging their blocks to influence the outcome		Blockchain	[91]

criminal activities involving unauthorized third parties, and smart contract vulnerabilities, as listed in Table 3, caused by flaws in programming codes.

V. OTHER CHALLENGES

1) Unclear Terminology: The limited talent pool available for blockchain technology has increased the needs (both real and perceived) for regulatory agencies to ask industry experts to explain the technology and any related concerns. These needs, along with all the potential consequences of false risk analysis and its tendency to underregulate, greatly increase the risk of capture by regulators [92], [93]. In fact, even just the terms ''DTL'' and ''blockchain'' are confusing. In short, there is a general lack of technical understanding among consumers, business firms, and authorities [10], [94], [95], including in areas such as

1) the blockchain job market,
2) DTL,
3) smart contracts that require that the business logic nature in ledgers be automatically executed,
4) knowing where to look to find the necessary talent, and
5) investing in blockchain jobs regardless of the demand for new talent.

2) Risk of Adoption: Even if there are expected economic benefits, the adoption and implementation costs of DLT/blockchain for existing projects can quickly become substantial. This is particularly true for existing customers with IT systems or processes that have been written to comply with current standards, which may require costly redesigns [96]. The operational costs associated with adopting DLT/blockchain remain unclear. Still, in the short term, certain back-office processes cannot be easily removed or replaced with DLT/blockchain solutions [97], [98]. For the development of blockchain in the capital market, industry participants must consider four immediate actions:

1) evaluating the business impact and planning for the long term,
2) participating in the relevant consortium and working with regulators,
3) identifying and capturing internal ledger opportunities, and
4) implementing post-trade and manual processes (required).

3) Economic Impact: in many cases, it is unclear whether blockchain will be an improvement over centralized systems in terms of performance, throughput, scalability, security, and privacy [99]. In addition, DTL faces challenges involving economic scaling, high transaction costs, and long verification times. Besides, until a proof of concept is tried and tested, there may be uncertainty about which use cases are viable and realistic. If DTL/blockchain is not widely adopted, it will

not be easy to clearly assess its broader economic impacts over the medium to long term [100]. Three areas in particular require further investigation:

1) organizational incentives and costs,
2) market environment (how cryptocurrencies are affected by demand and competitors), and
3) decision-making processes.

4) Lack of Technical Clarity: Given the ledger's decentralized nature and its function as a constant record, establishing clear governance rules is important for both authorized and unauthorized ledgers [101]–[106]. Part of the likely challenge with this governance is the result of selecting a ledger outside the contract that defines the participants' use conditions and responsibilities. Further, as part of off-ledger contracts and depending on the user's status, certain rights may not be automatically granted to the ledger user. This involves establishing procedures for specific aspects of governance, such as user identity verification, as well as establishing processes for disputing arbitration and applicable laws. It is also necessary to select a method of error correction for when incorrect data need to be added to the ledger or a transaction needs to be canceled. Specifically, with anonymous users, all approaches should focus on regulatory compliance as it relates to customer knowledge and anti-money laundering processes.

5) Regulation Uncertainty: Understanding how blockchain affects specific regulations in a wide range of regulatory environments is an important element of the development and deployment of any DLT solutions. In 2016, the company Deloitte and the Smart Contracts Alliance highlighted regulatory standpoints, approval, functions, and impacts regarding blockchain technology [99], [107]. New technology standards can be decisive, particularly with respect to the tightly regulated financial sector. According to Lamarque *et al.* [108], approximately 80% of blockchain technology focuses on business processes, while the remaining 20% focuses on technology. This imbalanced focus on the finance sector poses significant challenges for regulators attempting to decide when to intervene [109].

1) Regulatory bodies need to develop better understandings of ledger activity.
2) Regulatory uncertainty generates platform, price, and novelty risks.
3) Regulators must ensure that innovation is not suppressed while simultaneously protecting the end-user privileges.

6) Interoperable Implementations: To realize all the benefits of DLT/blockchain, ledgers must be able to exchange information with other ledgers and existing IT systems, and it is unclear whether large companies are prepared to reorganize their existing operating procedures in both the short and medium terms [101]–[103], [110]–[113]. One author emphasized the potential risk of inconsistent developments in technology, which can lead to fragmented markets [97]. Some authors have promoted enabling seamless interactions between blockchain technology and legacy systems. Meijer and Carlo [113] highlighted some implementation standards:

1) intensified conversation
2) concern about interoperability and competition in fragmented blockchains
3) common interoperability standards for different protocols, applications, and systems in areas such as cryptographic standards, interoperability standards, scalability parameters, and regulatory standards

7) Maintaining Data Privacy: Organizations should be cautious about the integrity and security of the data stored in ledgers, including both transaction data and data on the ledger's own activity [101], [103], [116], [115]. Organizations need to ensure that only people with the appropriate permissions can access the data and that any access complies with general data protection laws [114], [115]. Lamarque [109] argued that regulatory and legal intervention may be necessary to ensure that DLT/blockchain implementations can have meaningful and specific impacts.

8) Ensuring Encryption: While blockchains can provide encryption opportunities, such as having multiple copies of a book in the event of a cyberattack or computer failure, the development of access and management rights to multiple nodes represents a potential security risk, as there must be ''backdoors'' through which the system can be attacked [98]. Confidence in systems, verifying other users' integrity in the distributed general ledger, and consistent transaction security are some of the key challenges in increasing DLT/blockchain adoption [116], [117]. Some authors have suggested that nodes in distributed ledgers need to be able to view transaction data, even though IDT can be effectively encrypted in DLT/blockchain to validate the data. This presents a potential data privacy protection issue in certain cases of permissionless ledgers.

9) Energy-Intensive: DLT/blockchain has attracted substantial interest from technology firms, financial institutions, and other user communities. One issue with such technologies is that the ledgers are significantly more energy-intensive than centralized legacy systems [98], [101], [118]; Bitcoin blockchains, for instance, are highly energy-intensive [119]. Bitcoin uses PoW, or the number of CPU cycles a system has devoted to mining, and this is likely to represent a significant problem for future scaling that can be planned for and managed. Lamarque [108] explained that blockchain systems require considerably more energy to run than centralized ledger systems for a number of reasons:

1) more network nodes requiring unpredictable energy needs
2) many stakeholders with different approaches to blockchain technologies
3) server-side management demand
4) the need for effective cost-estimation mechanisms

10) Ambiguous Smart Contract Execution through Blockchain: There is a lack of clarity regarding whether smart contracts have been fulfilled and whether their terms

can be expressed, which can limit the terms to the binary determination of whether or not the contract has been fulfilled [120]. Charles Brennan and William Lunn described how the Ethereum hack was implemented in DLT/blockchain and revealed certain flaws in smart contracts [117]. Many of the challenges associated with smart contracts stem from the lack of clarity and diverse definitions in the contracts themselves, rather than the use of DLT or blockchain technology.

Summary And Insights:

This section has discussed some more fundamental challenges that may be encountered when dealing with blockchain technology, such as the unclear terminology that is still prevalent in some regulatory agencies. Some technical understandings are clear, such as risk adoption in the capital market industry and the economic impact in many cases, yet blockchain remains unclear in terms of performance, scalability throughput, and security. In addition, there is a lack of technical clarity with clear rules from the government, and the common interoperability implementation standard and maintaining data privacy are also big challenges.

VI. EXISTING BLOCKCHAIN TECHNOLOGY SOLUTIONS

This chapter discusses some existing blockchain solutions that have been proposed in different sectors. This survey focuses on the basic theory, key attributes, features, and limitations of existing studies on blockchain solutions.

A. HEALTH CARE

Linn and Koo [121] identified simple yet robust uses of blockchain for storing patients' health data; these systems allow each patient's entire health history to be stored on an individual blockchain. The data are primarily stored in data lakes that allow for simple querying, advanced analytics, and machine learning [122]–[130]. Data lakes are simple tools for warehousing many types of data; each user's blockchain serves as an index catalog that contains a unique user identification number and an encrypted link along with timestamps to indicate the latest data modifications.

Alhadhrami *et al.* [131] also discussed how blockchains could be used in the health care sector to maintain, validate, and store data, primarily data involving consortium blockchains. These are permissible blockchains in which both the node owner and the miners have access control. Consortium blockchains work on the theory of consensus for an optimum number of validations to ensure data accuracy.

Patel [132] discussed the development of a cross-domain image-sharing blockchain network that allows for the sharing of patients' medical and radiological images based on a consensus blockchain. The author's system sought consensus among very few trusted institutions to maintain a more meticulous consensus in which less effort is needed to manage the complex security and privacy module.

There has always been a trade-off associated with using the ISN (image sharing network) developed by the Radiological Society of South America and using the proposed image sharing blockchain where the ISN uses a central authority or clearinghouse to maintain many types of incoming and outgoing access. It is also a strict network for following the average concurrency and security protocol. However, this image-sharing blockchain is an open network that can be much more vulnerable to forced attacks; the only way to secure each node's URL endpoint is to guarantee the secrecy of the private keys used to access the blockchain. Therefore, we concluded from that study that there can be several proper use cases for sharing highly sensitive data in decentralized environments. However, the security model that relies on the nodes still appears to be quite complex, based on the Federal Policies and motions of the GDPR policies.

Mettler [133] reported that there are three basic sectors of blockchain health care technology: smart health care management, user-oriented medical research, and the prevention of drug counterfeiting. In the industry of smart health care management, the author discussed the Gem Health Network, which gives providers detailed views of their patients' current medical statuses. Medical record analysis of this type leads to the creation of an ecosystem that can elucidate even the past records of a patient by transparently reducing all merit costs. Moreover, medical experts can keep track of stakeholders' activities, such as visits to physicians and health centers, to follow their treatment tracks. Such systems can contribute to insurance claims being settled faster, and the same would happen if patients were to grant insurance companies access to their relevant records.

Liang *et al.* [134] discussed the growing demand for health care devices and wearable technology along with the challenges associated with storing and maintaining patients' records; blockchain is a far more secure and optimized way of maintaining these records. The wearable devices are linked to a cloud database or network wherein all the user's data are stored. Because vast amounts of data are stored in this way, they are stored in batches in a Merkle tree, thus allowing for efficient data processing. Table 4 summarizes the existing research solutions that have been proposed for smart health care environments using blockchain technology.

Tanwar *et al.* [135] have suggested how blockchain technology led to improve transactions involving medical records in healthcare 4.0 applications. The significant advantage of using blockchain in healthcare is that it can reform the interoperability of healthcare databases, accessibility to patient medical records, prescription databases, and device tracking. Moreover, the authors have proposed an access control policy algorithm for improving medical data accessibility between healthcare providers.

Tripathi *et al.* [136] proposed a new approach for a smart healthcare system named S2HS to provide intrinsic security and integrity of the system. In this paper, two-level blockchain mechanisms are used for internal and external entities of the healthcare system. This mechanism provides isolation among different entities with consistency and transparent flow in a secured and privacy-preserved manner.

Kumar *et al.* [137] performed the simulation and implementation of a novel healthcare design using the

TABLE 4. Healthcare solutions for blockchain systems.

Reference	Proposed Scheme	Basic Theory	Attributes	Other Features	Limitations
Linn and Koo, 2017 [121]	Secure way of storing and exchanging health care data using blockchain	Secure storage of many types of medical data helpful for in-depth research	Efficiency, authenticity, availability	Provides latest accurate data for many types of health care research	Storage and data throughput, interoperability, lack of data privacy
Alhadhrami et al., 2017 [131]	Different kinds of blockchains for validating and storing health care data	Pros and cons of different blockchains for health care data	Availability, efficiency, validity, privacy	Provides optimum number of validations for maintaining accuracy	Lack of technical details, ambiguous proposed scheme
Patel, 2018 [132]	Cross-domain image-sharing blockchain system	Using the consensus of trusted organization by considering GDPR policies	Authority, privacy	Designed for extreme level of privacy and security of medical images	Lack of relevant merits for large-scale implementation. No experimental results.
Mettler, 2016 [133]	Addresses the basic sectors of blockchain technology	Usage of Blockchain sectors and its effectiveness	Effectiveness, cost saving	Looking for past details to solve the problem in the easiest way	Unclear methodology
Liang et al. 2017 [134]	Maintaining electronic health records using blockchain	User-centric system where user has all rights for sharing information	Privacy, robustness, integrity	More responsibility for the user	Limited health data sharing. Scalability issue.
Tanwar et al. 2020, [135]	Blockchain-based EHR system for health application 4.0 version	Utilizing the blockchain concept and implementing permission-based HER system with the use of chaincode concept.	Latency, Throughput, round trip time	Improving current limitations of healthcare system such as efficiency and security	Required Test bed environment, limited rounds
Tripathi et al. 2020, [136]	Proposes a blockchain-based SHS framework to provide intrinsic security and integrity	Applying two level blockchain mechanism, i.e., private blockchain for internal entities and public blockchain for internal use in health care ecosystem	Privacy-preserved healthcare system	Enable patient centric system, promotes patient mediated communication	No experimental performance
Kumar et al. 2020, [137]	Smart healthcare design, simulation, and implementation using healthcare 4.0 process	Explore optimization algorithm and improve the performance of blockchain-based decentralization system	Performance improvement, data redundancy,	Easy data maintenance	Implementation on different blockchain networks with different tools and techniques

healthcare 4.0 process. This work has explored an optimization algorithm that improves the performance of the healthcare system. The proposed method integrated the simulation-optimization process with the proposed approach and improved the performance of industry 4.0 networks and the overall system.

B. TRANSACTION SECTORS

Oh and Shong [138] provided a survey report on how blockchain technology can be used in the financial sector and how it is gaining popularity. They also defined many use cases. Blockchain in the financial industry is not substantially more technically significant than the predefined databases, but the blockchain is far superior in terms of data storage reliability. In the present structure with central authorization, if at any point a database fails, then the entire system fails, and the data can be improperly accessed and modified. However, in blockchain, such scenarios are rare because transaction data are always safe: there is no single point of failure in blockchain. The authors also provided a comparative analysis of public, private, and consortium blockchains.

Turner *et al.* [139] discussed how Bitcoin is being leveraged for malicious activities and crimes online. The biggest advantage of Bitcoin is the anonymity of transactions; all personally identifiable information is hidden in the transactions. Bitcoin users have previously been tracked through careful analysis of transaction patterns (for instance, where stolen public keys are being used). However, the issue that persists here is the usage of dark wallets or Bitcoin Fog, wherein a huge set of transactions involving a single piggy bank is released to a destination address at once. Piggy banking blockchain transactions are often maximally anonymous because it is impossible to track the recipient of the transaction. Moreover, if piggy banking is used with the Tor browsers, then the entire transaction is completely anonymous, and tracking is impossible.

Yoo [140] described the use of blockchain in financial systems where most transactions were previously centrally regulated. Previously, decentralized blockchain technology was only used in certain areas, but its use has since expanded exponentially in the financial industry; areas such as smart contracts, settlement, remittances, and securities have all come to use blockchain on some level. The R3CEV Consortium of Korea, which comprises 16 different banks, has laid the foundation of certificate authority to authenticate transactions. Moreover, transfers of funds that were previously conducted across banks through gradual gold transfers have now been reduced and partially replaced by cryptocurrency

TABLE 5. Blockchain solutions in transaction sector.

Reference	Proposed Scheme	Basic Theory	Attributes	Other Features	Limitations
Oh and Shong, 2018 [138]	Evaluation of suitability of different blockchains for finance sectors using case study	Performance-based study by using comparative analysis	Robustness, efficiency	Feasibility study for different financial institutions	Not applied to all financial institutions
Turner et al., 2018 [139]	Use of blockchain for illicit activity and how to identify it	Good technology can be used in bad ways	Robustness, effectiveness	Pattern-based behavior during transactions	Bitcoin address and IP address limited
Yoo, 2017 [140]	Development of decentralized financial system based on blockchain	Evaluate the effectiveness of blockchain	Privacy, security, efficiency	Good recommendations for finance sectors	Limited to Korean financial sector

TABLE 6. Blockchain solutions for privacy and security.

Reference	Proposed Scheme	Basic Theory	Attributes	Other Features	Limitations
Joshi et al., 2018 [141]	Summarizes the issues related to privacy and security of blockchain	Case studies for validation and recommendation	Privacy, security, effectiveness, efficiency	Optimum traceability	Lack of blockchain tools distribution and permissions
Kshetri et al., 2017 [142]	Comparison between cloud and blockchain for privacy and security	Identify the pros and cons of cloud versus blockchain	Integrity, efficiency, privacy, security	Less storage required for blockchain than cloud	----------
Singh et al., 2019 [143]	Secure and efficient smart home architecture based on blockchain and cloud computing	Transaction handling and security analysis in smart home network	Privacy, security, confidentiality, integrity, scalability	Anomaly packet detection, high throughput, low latency	Handling limited security attacks and high execution time

transfers across institutions. Private distributed ledgers track many types of transactions between trusted authorities. The author also clearly described how the Korean banking sector could incorporate blockchain technology to increase the security and privacy of customer transactions. Table 5 summarizes the existing blockchain research solutions in the transaction sector.

C. BLOCKCHAIN FOR PRIVACY AND SECURITY

Joshi *et al.* [141] discussed the huge expansion of blockchain technology with an emphasis on the privacy and the security of the vast amounts of data involved. Blockchain transactions in the financial sector tend to be highly secure and authorized by either the central commission (in private blockchains) or the consortium of regulating stakeholders (in consensus blockchains). In the health care field, patients' medical data stored in central databases can be vulnerable to leaks, whereas blockchain architectures provide patients with full discretion over their data.

Kshetri *et al.* [142] compared how a cloud service and a blockchain operate in terms of data security and privacy. In cloud storage, it is very clear that data are not being permissioned, causing vulnerability; data are also managed and accessed by central authorities, and a rogue regulating authority can cause massive damage involving data leakage to unauthorized entities. By contrast, in blockchains, data are stored in peer-to-peer networks, and users have complete discretion over their data, thus guaranteeing complete data security and privacy.

Singh *et al.* considered the fundamental issues with smart home applications and presented a secure and efficient smart home architecture with which to overcome these challenges [143]. The proposed system also fulfills the security goals of protecting communication, scalability, ensuring the system's efficiency, and protecting against a variety of attacks. The proposed architecture incorporates blockchain and cloud computing technology in a holistic solution. Our proposed model uses the Multivariate Correlation Analysis (MCA) technique to analyze the network traffic and identify the correlation between traffic features to ensure the security of smart home local networks. The anomaly detection algorithm is presented for the detection and mitigation of DoS/DDoS attacks.

Table 6 summarizes the existing blockchain research solutions for privacy and security.

D. BLOCKCHAIN-IoT PRIVACY PRESERVING APPROACH

Yang *et al.* identified the three ways through which the location of blockchain addresses could be disclosed that raise the potential risk of privacy infringement. Therefore, the authors have proposed a novel blockchain solution to preserve the worker's position and increase the success rate of assigned work [144].

Kuo *et al.* [145] focused on developing a hierarchical approach to inherit the privacy-preserving benefits and retain blockchain adoption services concerning research networks-of-networks. Therefore, the authors have proposed

TABLE 7. Blockchain for privacy preserving scheme.

Reference	Proposed Scheme	Basic Theory	Attributes	Other Features	Limitations
Yang et al [144]	Blockchain-based location, privacy-preserving crowd- sensing system	Preserve the worker's location and increase the success rate of assigned work	Prevent re-identification, location privacy	Efficiency, security	Uploaded data can be re-used by malicious worker, quality evaluation problem
Kuo et al. [145]	Privacy-preserving model learning on the blockchain on a networks-of-networks	Implementation of hierarchical privacy-preserving model on blockchain and evaluate it on three healthcare/genomic datasets	Improve predictive correctness of datasets, improve decision support system	Learning iteration, reduce execution time,	Topology, evaluation of large number of data, advance privacy concern
Gai et al [146]	Energy trading with user's privacy using blockchain in smart grid	Differential privacy, neighboring energy trading, privacy preserving	Efficiency, user's privacy	----------	----------
Qui et al. [147]	Location privacy approach based on blockchain	Location-based service, K-anonymity	Efficiency, privacy, security	Good response time, and scalability performance increased	This method is more suitable for snapshot theory

a framework to combine model learning with blockchain-based model dissemination and with a hierarchical consensus algorithm to develop an example implementation of a hierarchical chain that improves predictive correctness for small training datasets.

Gai *et al.* [146] discussed the privacy concern caused by attackers, which use data mining algorithms to violate a user's privacy when the user group is located nearby geographically. The authors proposed a module for constructing a smart contract called the black-box module. This module allows for the regular operation of energy trading transactions per demand for privacy preservation in design objectives.

Qui *et al.* overviewed the shortcomings of two existing privacy-preserving schemes and proposed a location privacy protection method using blockchain technology. The proposed method does not require a third-party anonymizing server, instead satisfying the principle of k-anonymity privacy protection [147].

Table 7 summarizes the existing blockchain research solutions for privacy-preserving.

E. SECURITY VULNERABILITY AND TOOLS

Blockchain smart contracts offer security and privacy, but their vulnerabilities must be further understood. Here, we discuss some security tools to provide the body of knowledge necessary for creating secure blockchain software. The decentralized nature of blockchain technology carries historic immutability recognized by industries aiming to apply it in their business processes, particularly in IoT. IoT's major security issue is knowing and controlling who is connecting in huge networks without breaching privacy regulations [148].

Blockchain technology is recognized as safe in its design, but built-in applications may be vulnerable in real circumstances. For example, smart contracts have been affected financially by various unfortunate incidents and attacks. In one case, in June 2016, a reentrancy problem in split DAO caused a loss of approximately $40 million [85], and $32 million was taken by attackers in 2017 [149]. These high-profile cases show that even experienced developers can leave a system seriously vulnerable to attackers aiming to exploit security bugs in smart contracts. Table 8 presents a matrix of security tools covering the most serious vulnerabilities; as shown in the table, most of these tools address more than vulnerability. The visibility check is omitted because it is only covered by smart checks [90].

Summary And Insights:

Many existing solutions in different sectors have been discussed in this section. In the healthcare sector, various proposed schemes based on storing healthcare data improve efficiency, availability, integrity, effectiveness, and other features, while each scheme has certain limitations. Moreover, this section has also discussed the existing scheme in the transaction sector to evaluate the finance sector by using blockchain to identify illicit activity and develop a financial system. A blockchain scheme based on privacy and security is also discussed, which provides optimal traceability and anomaly packet detection.

F. ATTACK SOLUTIONS

1) LIVENESS ATTACK

To combat the active liveness attack, Conflux's consensus protocol essentially encodes two different block generation strategies proposed by Li *et al.* [150]. One is the optimal strategy that allows quick confirmation and the other is the conservative strategy that guarantees the progress of consensus. Conflux is a scalable and decentralized system with high

TABLE 8. Tools and vulnerability.

Security tool	Interface	ReEntrancy	Timestamp dependency	Mishandled exceptions	Immutable Bugs	Gas costly patterns	Blockhash usage
Oyente	Command line	✓	✓	✓	✓	……	……
Remix	Command line	✓	✓	✓	……	✓	✓
Gasper		……	……	……	……	✓	……
Securify	User interface	✓	……	✓	……	------	……
S. Analysis		……	……	✓	……	------	……
Smartcheck	User interface	✓	✓	✓	✓	✓	……
Mythril	Command line	✓	……	✓	✓	------	……

throughput and fast confirmation in the blockchain system. It uses a novel adaptive weight mechanism to combine these two strategies to an integrated consensus protocol.

2) DOUBLE SPENDING ATTACKS

To address the double-spending attack, Nicolas and Wang [151] have proposed the MSP (Multistage Secure Pool) framework which allows the pool to authenticate the transactions. The proposed framework includes four stages to overcome this attack are 1) detection stage, 2) confirmation stage, 3) Forwarding stage, and 4) broadcast stage. In addition, Begum *et al.* [152] provide a set of solutions against double-spending attacks after showing the limitation of this attack.

3) 51% VULNERABILITY ATTACK

To combat the 51% attack, Sayeed and Macro-Gisbert [153] have focused on crypto-coin with low hashing power to analyze 51% attack, revealing the weakness in the consensus protocol which makes this attack happen. The authors define the hash rate problem and provide five security mechanisms against 51% attack. A recent work that has been done to address the 51% attack includes defensive mining, implementing a ''Permapoint'' finality arbitration system to limit chain re-organization [154].

4) PRIVATE KEY SECURITY ATTACK

Pal *et al.* [155] have proposed public key infrastructure used in the blockchain technology to authenticate the entities to counter a key security attack. This technique ensures the integrity of the blockchain network. A group key management is discussed to secure group communication to achieve confidentiality in the network.

5) TRANSACTION PRIVACY LEAKAGE

The work proposed by Bhushan and Sharma [156] presented the overall view of security loopholes, carrying out of transactions and suggested secure transaction methodology scheme. The scheme uses a homomorphic cryptosystem, ring signature, and many other security measures to decrease the overall impact of threats to improve the reliability in the transactional process in the network.

6) SELFISH MINING ATTACK

Saad *et al.* [157] have discussed the vulnerability of self-mining and proposed a solution to counter this attack. To counter the attack, the authors leverage an honest mining practice to devise the notation of truth state for blocks during self-mining fork and also allocate self-confirmation height to each transaction. Nicolas et al [158] have done a comprehensive overview of self-mining attack and their countermeasure schemes.

7) DAO ATTACK

Ghaleb *et al.* addressed the DAO insider attack in RPL IoT network. To mitigate this attack, the authors have proposed a scheme by conducting experiments using the Contiki tool, a low-power-designed tool for resource-constrained devices [159].

8) BGP HIJACKING ATTACK

Xang *et al.* [160] proposed a BGPCoin scheme, which is a trustworthy blockchain-based internet resource solution. The scheme develops the smart contract to perform and supervise resource assignment on temper resistant Etherium blockchain. BGPCoin scheme poses a credible BGP security solution on the Etherium blockchain and smart contract programming.

9) SYBIL ATTACK

To prevent Sybil attacks in blockchain networks, Swathi *et al.* [161] have proposed a scheme to restrict the Sybil attack by monitoring other nodes' behavior and checking for the nodes which are forwarding the blocks of only a particular user.

G. COUNTERMEASURE

Although blockchain systems can be used very reliably, security mechanisms must be implemented at every point in the network. The blockchain user's private key address needs

to be highly coded to make the information more secure. Blockchain network designers need to be aware of potential network attacks before implementation. Attack self-detection software must be built into the system.

This section describes existing countermeasures and detection algorithms available for technologies within the blockchain that can be used to ensure privacy and security. For a comprehensive overview of this topic, this paper extracted some existing research papers and internet resources from scientific databases. Here is a summary of state-of-the-art solutions applied to blockchain environments that address security threats and provide strong privacy.

1) QUANTITATIVE FRAMEWORK

Application: The quantitative framework is made up of two sections. While one is a blockchain simulator, another segment has a security model plan [162]. The stimulator takes after the activity of blockchain frameworks. The consensus protocol and the network are the input parameters.

Impact: The quantitative system yields a high basic procedure to check the assaults. By doing so, the framework helps build the security of the blockchain system.

2) OYENTE

Application: Oyente is built in a way that can detect bugs in Ethereum based contracts. This technology is designed to evaluate the bytecode of blockchain smart contracts on Ethereum [163]. The Ethereum blockchain system stores the EVM bytecode of smart contracts.

Impact: Oyente is very convenient to deploy on a system. It detects bugs that may be present in a system.

3) HAWK

Application: The framework is used to develop the privacy of smart contracts. The Hawk framework can allow developers to write codeless private smart contracts to enhance the security system.

Impact: Since using hawk, the developer divides a system into two main parts, financial transactions are not explicitly stored in the blockchain network system [162]. The private part stores non-public data. Financial transaction information is stored in the private part. Code and information that does not require privacy can be found in the public section [164]. Hawk protects the personal information records on a blockchain system because it uses the private smart contract that automatically generates an effective cryptographic model.

4) TOWN CRIER

Application: Town crier works by recovering data demands from clients and gather information from HTTP websites [165]. A carefully marked blockchain message got back to the client contract by the Town crier.

Impact: Town crier provides security when requesting information from clients. Strong security which is a robust model for the blockchain smart contract is provided by a local announcer/town crier.

5) LIGHTNING NETWORK

Application The Lightning network generates double-signed transaction receipts. The transaction is said to be valid after the parties involved in the transaction have signed it to accept the new check [165].

Impact: This Lightning network helps two individuals to conduct transactions between themselves without interference from a third-party miner. Double signing ensures transaction security for the parties involved.

6) SEGWIT

Application: Segwit is one of the sidechain features that runs in parallel with the main Blockchain network [166]. Signature data moves from the main Blockchain system to the extended sidechain.

Impact: By using the sidechain, more blockchain space is freed and more transactions are executed [167]. The signature data is placed in the parallel side chain in the form of a Merkle tree. With this placement, the overall block size limit has increased without interfering with the block size. Data diversification improves network security.

7) INTEGRATION OF BLOCKCHAIN WITH ARTIFICIAL INTELLIGENCE (AI)

Application: Artificial intelligence is building a machine in a way that can perform tasks that require intelligence.

Impact: Machine learning can be used by security personnel to detect anomalous behavior in the network and prevent attacks on the system [165].

8) TENDERMINT

Tendermint proposed the concept of blocking, in which security is provided by a modified reconciliation protocol based on share confirmation. Each block must be cryptographically signed by certifiers in the Tendermint consensus protocol, where certifiers are simply users who confirm their interest in the security of the system by closing their funds with the help of a bonding transaction [168].

However, some cryptographic works have been done to improve the blockchain network. For example, Wang *et al.* [169] have proposed a secure and efficient protocol using Elliptic Curve Cryptography (ECC) to solve the identity authentication issue in the smart grid. Moreover, Song *et al.* [170] have worked on security and privacy concerns for smart agriculture systems by proposing a data aggregation scheme with a flexible property that utilizes ElGamal cryptosystem. Zhang *et al.* [171] have suggested a distributed Covert Channel of the packet ordering enhancement model based on data compression to enhance the unknowability of the data. Some more work has studied the applications of providing security techniques to enhance the blockchain network system [50], [172]–[176].

TABLE 9. Solving secirity issues through blockchain characteristics.

Characteristics / Issues	Smart contract	Transparent And verifiable	Decentra-lization	Anonymity	Efficiency	Persistency	Resiliency	Digital ledger
Data privacy	Yes	No	No	Yes	No	No	No	No
Access control	Yes	Yes	Yes	No	Yes	No	No	No
Single point failure	No	No	Yes	No	Yes	No	Yes	No
Third-party	No	No	Yes	No	Yes	No	Yes	No
Integrity of data	Yes	No	Yes	No	No	Yes	No	No
Availability	No	No	Yes	No	Yes	No	No	No
Immutability	Yes	No	No	No	No	Yes	No	Yes
Eavesdropping	No	No	No	Yes	No	No	No	No
Trust	No	Yes	Yes	No	No	Yes	No	No
Botnet attacks	No	No	Yes	No	No		Yes	Yes

VII. OPEN ISSUES AND RESEARCH DIRECTION

To complete our overview, we outline some open questions and research challenges, along with available requirements to improve blockchain-IoT capability. Table 9 summarizes some key blockchain characteristics that solve the security issues.

1) Vulnerability: Despite offering a robust approach for IoT security, blockchain systems are also vulnerable. The consensus mechanism based on the miner's hash power has disappeared, thus allowing attackers to host the blockchain. Likewise, it is possible for attackers to compromise blockchain accounts by exploiting private keys with limited randomness. Users need to define effective mechanisms to ensure transactions' privacy and avoid competitive attacks, leading to double spending during transactions.

2) Resiliency against combined attack: Many security solutions and applications have been discussed and proposed for blockchain-IoT, and each of them has been designed to handle certain security issues and threats. The main question involves developing a framework that can be resilient against many combined attacks with consideration of the implementation feasibility of the proposed solutions.

3) Policies for zero-day attacks: A zero-day attack is a software module technique that occurs when there is a lack of countermeasures against such vulnerability. It is difficult to identify the possibility of such attacks, and any device can be compromised by one. Most of the related suspicious activities are recognized during the development stage, but some of them are recognized during testing operations. When a vulnerability is exploited, the liabilities should be addressed by a security patch from the software distributers. A non-homogeneous Markov model is defined using an attack graph that incorporates time-dependent covariates to predict zero-day attacks.

4) Blockchain specific infrastructure: Storing the data on the blockchain database means storing information on the IoT nodes in the network that cannot be deleted. This means information is imposed on the miner nodes, which imposes huge costs on a decentralized network. Specifically, we can understand that storage-limited IoT devices may not store large blockchains that grow as blocks are added to the blockchain. It is also known that IoT devices store data on blockchains that are not useful for their transactions. Therefore, fining equipment that supports the distributed storage of large-scale blockchain-specific blockchains becomes a difficult problem. In addition, address management and basic communication protocols play important roles in the blockchain infrastructure. In particular, the reliability between devices with abundant computing resources must be established in the blockchain infrastructure. Further, the application programming interface should be as user-friendly as possible.

5) Security requirements: Considering blockchain-IoT, it is of the utmost importance for the specific condition which aims to facilitate security parameters, attack countermeasures, privacy, and trust. Blockchain-IoT must satisfy certain security requirements, illustrated as follows:

- *Secure key exchange:* It is considered as an important role in a cryptographic mechanism to secure end-to-end communications. It is a pillar of attack prevention in the network. It should be guaranteed that a key must be securely shared over the network.
- *Resource-exhausted attack resilient:* Resource exhaustion attacks are security exploitations of the targeted system or network that should be prevented. The attack can be exploited through the excessive key operation, or when many transactions occur in the network and there is abundant validation from the miners. Such attacks may cause a shutdown of the entire network.
- *Resource utilization:* The utilization of memory and power can save the operation up to a longer duration. The novel network architecture can utilize the resources well for each function in a blockchain transaction system. Some other facilities like fog computing, edge-crowd modeling, osmotic computing, and other distributed concepts can improve resource utilization and security facilities.
- *Performance trade-off:* Apart from the cryptographic requirement for providing security and efficiency, one should not ignore or compromise the system's

performance and handle the implementation overhead during parallel operation.

- *Insider threat management:* It prevents threat, combating, detecting, and monitoring of employees. Non-compromising models are required to detect and prevent false alarms in the aspects of the blockchain system.

6) Open Questions:

- How many blockchains can secure the IoT environment?
- What are the smart contract vulnerabilities, and how do smart contracts respond in the face of changing IoT environmental conditions?
- In what cases can blockchain be used in IoT networks?
- How safe will blockchain technology remain in the future age of quantum computing?
- How can the issue of latency in block creation in blockchain and cryptographic processes be addressed without compromising privacy?

VIII. CONCLUSION

The blockchain paradigm is changing the IT industry. Blockchain can bring together companies, governments, and even countries. Blockchain technology is widely recognized and highly valued due to its decentralized nature and peer-to-peer characteristics. The main takeaway of this review paper is that the authors have thoroughly analyzed several attacks on blockchain and the security issues of blockchain with some real-world examples. Moreover, this paper discussed the various security issues, challenges, vulnerabilities, and attacks that impede the increased adoption of blockchain technology while exploring these challenges in a variety of aspects. We also explained other blockchain applications and benefits, and we discussed many related opportunities at the business level. Finally, we summarized existing security solutions for different environments and open research issues.

REFERENCES

[1] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, pp. 1–17, 2019.

[3] X. Jiang, M. Liu, C. Yang, Y. Liu, and R. Wang, "A blockchain-based authentication protocol for WLAN mesh security access," *Comput., Mater. Continua*, vol. 58, no. 1, pp. 45–59, 2019.

[4] Z. Deng, Y. Ren, Y. Liu, X. Yin, Z. Shen, and H. Kim, "Blockchain-based trusted electronic records preservation in cloud storage," *Comput., Mater. Continua*, vol. 58, no. 1, pp. 135–151, 2019.

[5] R. Song, Y. Song, Z. Liu, M. Tang, and K. Zhou, "GaiaWorld: A novel blockchain system based on competitive PoS consensus mechanism," *Comput., Mater. Continua*, vol. 60, no. 3, pp. 973–987, 2019.

[6] G. Sun, S. Bin, M. Jiang, N. Cao, Z. Zheng, H. Zhao, D. Wang, and L. Xu, "Research on public opinion propagation model in social network based on blockchain," *Comput., Mater. Continua*, vol. 60, no. 3, pp. 1015–1027, 2019.

[7] C. Li, G. Xu, Y. Chen, H. Ahmad, and J. Li, "A new anti-quantum proxy blind signature for blockchain-enabled Internet of Things," *Comput., Mater. Continua*, vol. 61, no. 2, pp. 711–726, 2019.

[8] W. Wang and C. Su, "CCBRSN: A system with high embedding capacity for covert communication in Bitcoin," in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*. Cham, Switzerland: Springer, 2020, pp. 324–337.

[9] Z. Lejun, Z. Zhijie, W. Weizheng, W. Rasheed, Z. Chunhui, K. Seokhoon, and C. Huiling, "A covert communication method using special bitcoin addresses generated by vanitygen," *Comput., Mater. Continua*, vol. 65, no. 1, pp. 597–616, 2020.

[10] S. Li, F. Liu, J. Liang, Z. Cai, and Z. Liang, "Optimization of face recognition system based on azure IoT edg," *Comput., Mater. Continua*, vol. 61, no. 3, pp. 1377–1389, 2019.

[11] D.-Y. Kim, S. Dong Min, and S. Kim, "A DPN (delegated proof of node) mechanism for secure data transmission in IoT services," *Comput., Mater. Continua*, vol. 60, no. 1, pp. 1–14, 2019.

[12] L. Xu, C. Xu, Z. Liu, Y. Wang, and J. Wang, "Enabling comparable search over encrypted data for IoT with privacy-preserving," *Comput., Mater. Continua*, vol. 60, no. 2, pp. 675–690, 2019.

[13] M. A. Ferrag, A. Derhab, L. Maglaras, M. Mukherjee, and H. Janicke, "Privacy-preserving schemes for fog-based IoT applications: Threat models, solutions, and challenges," in *Proc. Int. Conf. Smart Commun. Netw. Technol. (SaCoNeT)*, Oct. 2018, pp. 37–42.

[14] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019.

[15] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[16] (2019). *What is Block Decentralization*. [Online]. Available: https://lisk.io/academy/Blockchain-basics/benefits-of-Blockchain/what-is-decentralization

[17] (2015). *Obama Announces Legislation Protecting Personal Data, Student Digital Privacy*. [Online]. Available: https://www.rt.com/usa/221919-obama-privacy-student-consumer/

[18] K. Gai, M. Qiu, X. Sun, and H. Zhao, "Security and privacy issues: A survey on FinTech," in *Proc. Int. Conf. Smart Comput. Commun.*, 2016, pp. 236–247.

[19] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.

[20] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 31, 2016, pp. 1–4.

[21] 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, pp. 1–5.

[22] P. D. Filippi, "The interplay between decentralization and privacy: The case of blockchain technologies," *J. Peer Prod.*, no. 7, pp. 1–19, Sep. 2016.

[23] J. L. D. L. Rosa, V. Torres-Padrosa, A. el-Fakdi, D. Gibovic, O. Hornyák, L. Maicher, and F. Miralles, "A survey of Blockchain technologies for open innovation," in *Proc. 4th Annu. World Open Innov. Conf.*, 2017, pp. 14–15.

[24] O. Jacobovitz, "Blockchain for identity management," Lynne William Frankel Center Comput. Sci., Dept. Comput. Sci., Ben-Gurion Univ., Be'er Sheva, Isreal, Tech. Rep., 2016.

[25] (2018). *ID and Access Management: The Next Steps*. [Online]. Available: https://www.bankinfosecurity.com/interviews/id-access-management-next-steps-i-3904

[26] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, vol. 11. Cheltenham, U.K.: Edward Elgar Publishing, 2016, pp. 225–253.

[27] *Blockchain Developers*. Accessed: Dec. 2020. [Online]. Available: https://www.ibm.com/blogs/Blockchain/category/Blockchain-developers/Blockchain-open-source/

[28] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, Oct. 2016.

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

[30] M. Möser, "Anonymity of bitcoin transactions," in *Proc. Munster Bitcoin Conf. (MBC)*, 2013, pp. 1–10.

[31] (2021). *Number of Blockchain Wallet Users Worldwide From November 2011 to January 11, 2021*. [Online]. Available: https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/
[32] H. Kakavand, N. K. D. Sevres, and B. Chilton, "The Blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies," *Available SSRN*, vol. 2849251, pp. 1–27, Jan. 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id
[33] Y. Peter, "Regulatory issues in blockchain technology," *J. Financial Regulation Compliance*, vol. 25, no. 2, pp. 96–208, 2017.
[34] A. Nordrum, "Is it time to become a blockchain developer," *IEEE Spectr.*, vol. 54, no. 9, p. 21, Aug. 2017.
[35] K. Wüst and A. Gervais, "Do you need a blockchain?" in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Zug, Switzerland, 2018, pp. 45–54, doi: 10.1109/CVCBT.2018.00011.
[36] C. Sullivan and E. Burger, "E-residency and blockchain," *Comput. Law Secur. Rev.*, vol. 33, no. 4, pp. 470–481, Aug. 2017.
[37] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 9604, pp. 106–125, Jun. 2016.
[38] A. Kiayias and G. Panagiotakos, "On trees, chains and fast transactions in the blockchain," in *Proc. Int. Conf. Cryptol. Inf. Secur. Latin Amer.*, in Lecture Notes in Computer Science (LNCS), vol. 11368. Cham, Switzerland: Springer, 2019, pp. 327–351, doi: 10.1007/978-3-030-25283-0_18.
[39] S. W. Kim. (May 24, 2018). *Safety and Liveness—Blockchain in the Point of View of FLP Impossibility*. Accessed: 2020. [Online]. Available: https://medium.com/codechain/safety-and-liveness-blockchain-in-the-point-of-view-of-flp-impossibility-182e33927ce6
[40] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, pp. 1–32, Jun. 2015.
[41] G. O. Karame, E. Androulaki, and S. Capkun, "Two Bitcoins at the price of one? Double-spending attacks on fast payments in Bitcoin," in *Proc. Conf. Comput. Commun. Secur.*, 2012, pp. 1–17.
[42] M. Rosenfeld, "Analysis of hashrate-based double spending," 2014, *arXiv:1402.2009*. [Online]. Available: http://arxiv.org/abs/1402.2009
[43] N. Hajdarbegovic, *Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack*. New York, NY, USA: CoinDesk, 2014.
[44] J. L. Zhao, S. Fan, and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," *Financial Innov.*, vol. 2, no. 1, pp. 1–7, Dec. 2016.
[45] J. Frankenfield, *51% Attack*. New York, NY, USA: Investopedia, 2019.
[46] H. Mayer, "ECDSA security in bitcoin and ethereum: A research survey," *CoinFaabrik*, pp. 1–10, Jun. 2016. [Online]. Available: https://www.semanticscholar.org/paper/ECDSA-Security-in-Bitcoin-and-Ethereum-%3A-a-Research-Mayer/434a117a2717cdbf78035365d8bab2b0a3410be9?p2df
[47] A. Bryk, *Blockchain Attack Vectors: Vulnerabilities of the Most Secure Technology*. Dnipro, Ukraine: Apriorit, 2018.
[48] B. Bordel, R. Alcarria, M. Martin, and A. Sanchez-Picot, "Trust provision in the Internet of Things using transversal blockchain networks," *Intell. Automat. Soft Comput.*, vol. 25, no. 1, pp. 155–170, 2019.
[49] A. Badshah, A. Ghani, M. Ahsan Qureshi, and S. Shamshirband, "Smart security framework for educational institutions using Internet of Things (IoT)," *Comput., Mater. Continua*, vol. 61, no. 1, pp. 81–101, 2019.
[50] A. S. M. S. Hosen, S. Singh, V. Mariappan, M. Kaur, and G. H. Cho, "A secure and privacy preserving partial deterministic RWP model to reduce overlapping in IoT sensing environment," *IEEE Access*, vol. 7, pp. 39702–39716, 2019.
[51] J. Barcelo, "User privacy in the public bitcoin Blockchain," *J. Latex Class Files*, vol. 6, no. 1, pp. 1–4, 2007.
[52] P. Fremantle, B. Aziz, and T. Kirkham, "Enhancing IoT security and privacy with distributed ledgers—A position paper," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, 2017, pp. 1–7.
[53] Y. Tang, Q. Zou, J. Chen, K. Li, C. A. Kamhoua, K. Kwiat, and L. Njilla, "ChainFS: Blockchain-secured cloud storage," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 987–990.
[54] S. Solat and M. Potop-Butucaru, "Zeroblock: Preventing selfish mining in bitcoin," Sorbonne Universities, UPMC Universities, Paris, France, Tech. Rep. hal-01310088v1, 2016, pp. 1–17. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01310088v1
[55] (2018). *What is Selfish Mining*. Tokens. Accessed: 018. [Online]. Available: https://www.tokens24.com/cryptopedia/mining/what-is-selfish-mining
[56] (2016). *Understanding the DAO Attack*. CoinDesk. [Online]. Available: https://www.coindesk.com/understanding-dao-hack-journalists/
[57] P. Daian, "Analysis of the DAO exploit," *Hacking, Distrib.*, vol. 6, Jul. 2016. Accessed: Dec. 2020. [Online]. Available: https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/
[58] Phil Daian. *Analysis of the DAO Exploit*. Accessed: Dec. 2020. [Online]. Available: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/
[59] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 375–392.
[60] J. Stewart. (May 2014). *BGP Hijacking for Cryptocurrency Profit*. Accessed: 2021. [Online]. Available: https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit
[61] K. Soska, A. Kwon, N. Christin, and S. Devadas, "Beaver: A decentralized anonymous marketplace with secure reputation," *IACR Cryptol. ePrint Arch.*, vol. 2016, pp. 464–479, 2016.
[62] D. Christian and D. Wattenhofer, "Bitcoin transaction malleability and MtGox," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2014, pp. 313–326.
[63] U. Rajput, F. Abbas, R. Hussain, H. Eun, and H. Oh, "A simple yet efficient approach to combat transaction malleability in bitcoin," in *Proc. Int. Workshop Inf. Secur. Appl.*, 2014, pp. 27–37.
[64] K. Wust, "Security of blockchain technologies," M.S. thesis, Dept. Comput. Sci., ETH Zürich, Zürich, Switzerland, 2016, pp. 1–59.
[65] C. DeCusatis, M. Zimmermann, and A. Sager, "Identity-based network security for commercial blockchain services," in *Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2018, pp. 474–477.
[66] P. K. Sharma, S.-Y. Moon, and J.-H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, 2017.
[67] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. (2014). *Enabling Blockchain Innovations With Pegged Sidechains*. [Online]. Available: http://www.opensciencereview.com/papers/123/enablingBlockchain-innovations-with-pegged-sidechains
[68] S. Wenbo, W. Jiaqi, Z. Jinxiu, W. YuPeng, and D. Choi, "A novel privacy-preserving multi-attribute reverse auction scheme with bidder anonymity using multi-server homomorphic computation," *Intell. Automat. Soft Comput.*, vol. 25, no. 1, pp. 171–181, 2019.
[69] I. You, C. Choi, V. Sharma, I. Woungang, and B. K. Bhargava, "Guest editorial: Advances in security and privacy technologies for forthcoming smart systems, services, computing, and networks," *Intell. Automat. Soft Comput.*, vol. 25, no. 1, pp. 117–119, 2019.
[70] C. Mann and D. Loebenberger, "Two-factor authentication for the bitcoin protocol," *Int. J. Inf. Secur.*, vol. 16, no. 2, pp. 213–226, Apr. 2017.
[71] J. McKendrick. (2017). *9 Reasons to be Cautious With Blockchain*. [Online]. Available: https://www.zdnet.com/article/9-reasons-to-be-cautious-with-Blockchain/
[72] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *Proc. 22nd Int. Conf. World Wide Web*, 2013, pp. 213–224.
[73] S. Mire. (2018). *Blockchain for Cannabis: 6 Possible Use Cases*. [Online]. Available: https://www.disruptordaily.com/Blockchain-use-cases-cannabis/
[74] B. Reutzel. (2016). *From Seeds to Weed, Bitcoin Finds Home Where Commerce Goes Gray*. [Online]. Available: https://www.coindesk.com/bitcoin-atms-gray-areas
[75] J. Martin. (2018). *Blockchain in Action: Derailing Drug Abuse & Prescription Drug Fraud*. [Online]. Available: https://Blockchain.wtf/2018/06/series/Blockchain-in-action/derailing-drug-abuse/
[76] R. Wolfson. (2018). *Tracing Illegal Activity Through the Bitcoin Blockchain to Combat Cryptocurrency*. [Online]. Available: https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-Blockchain-to-combat-cryptocurrency-related-crimes/#3beb9fa333a9
[77] M. Powell, "Bitcoin: Economics, technology, and governance," *CFA Dig.*, vol. 45, no. 7, pp. 213–238, Jul. 2015.
[78] C. Wire. (2018). *Blockchain Technology Can Prevent Prescription Drug Abuse*. [Online]. Available: https://www.coinwire.com/Blockchain-technology-can-prevent-prescription-drug-abuse
[79] R. Jackson. *Blockchain Aims to Curb Prescription Drug Abuse*. Accessed: Nov. 2020. [Online]. Available: https://hackernoon.com/Blockchain-aims-to-curb-prescription-drug-abuse-47fc9cc66379

[80] (2018). *Blockchain for Crime Prevention in the Legal Cannabis Space*. [Online]. Available: https://investingnews.com/innspired/Blockchain-crime-prevention-legal-cannabis-space/

[81] P. Godsiff, "Bitcoin: Bubble or blockchain," in *Agent and Multi-Agent Systems: Technologies and Applications*. Cham, Switzerland: Springer, 2015, pp. 191–203, doi: 10.1007/978-3-319-19728-9_16.

[82] E. Hreinsson and S. Blöndal, "The future of Blockchain technology and cryptocurrencies," Ph.D. dissertation, 2018.

[83] K. Zetter. (2018). *How the Federal Government Defeated the Silk Road Drug Wonderland*. [Online]. Available: https://www.wired.com/2013/11/silk-road/

[84] M. A. Niloy. (2018). *From the Dark Side of Bitcoin: Misusing Cryptography*. [Online]. Available: https://99bitcoins.com/the-dark-side-of-bitcoin-misusing-cryptography/

[85] A. Nicola, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SOK)," in *Proc. Int. Conf. Princ. Secur. Trust*, 2017, pp. 164–186.

[86] M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," 2017, *arXiv:1710.06372*. [Online]. Available: http://arxiv.org/abs/1710.06372

[87] J. H. Mosakheil. *Security Threats Classification in Blockchains*. Accessed: 2020. [Online]. Available: https://repository.stcloudstate.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1093&context=msia_etds

[88] B. Jiang, Y. Liu, and W. K. Chan, "ContractFuzzer: Fuzzing smart contracts for vulnerability detection," in *Proc. 33rd ACM/IEEE Int. Conf. Automated Softw. Eng.*, Sep. 2018, pp. 259–269.

[89] (2018). *Introduction to Smart Contracts*. [Online]. Available: http://solidity.readthedocs.io/en/v0.4.21/introduction-tosmart-contracts.html

[90] A. Dika, "Ethereum smart contracts: Security vulnerabilities and security tools," M.S. thesis, Dept. Comput. Sci., NTNU, Trondheim, Norway, 2017, pp. 1–97.

[91] J. H. Mosakheil, "Security threats classification in blockchains," Culminating Projects Inf. Assurance, St. Cloud State Univ., St Cloud, MN, USA, Tech. Rep. 5-2018, 2018, vol. 48, pp. 1–142.

[92] *The Lack of Blockchain Talent is Becoming an Industry Concern*. Accessed: 2020. [Online]. Available: https://www.coindesk.com/Blockchain-hiring-difficulties-becoming-industry-concern

[93] A. Walch, "The path of the blockchain lexicon (and the law)," *Rev. Banking Financial Law*, vol. 36, pp. 713–765, Sep. 2017. [Online]. Available: https://ssrn.com/abstract=2940335

[94] (2020). *SWIFT on Distributed Ledger Technologies*. [Online]. Available: http://www.ameda.org.eg/files/SWIFT_DLTs_position_paper_FINAL1804.pdf

[95] *ISITC Europe and Oasis to Define Technical Standards for Blockchain*. Accessed: 2020. [Online]. Available: https://www.bankingtech.com/2016/10/isitc-europe-and-oasis-to-define-technical-standards-for-Blockchain/

[96] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov. Rev.*, vol. 2, pp. 1–16, Jun. 2016.

[97] H. Kakavand, N. K. De Sevres, and B. Chilton, "The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies," *SSRN Electron. J.*, pp. 1–27, 2017.

[98] K. Buehler, D. Chiarella, H. Heidegger, M. Lemerle, A. Lal, and J. Moon, "Beyond the hype: Blockchains in capital markets," in *Proc. McKinsey Working Papers Corporate Investment Banking*, no. 12, 2015, pp. 1–32.

[99] V. Grewal-Car and S. Marshall, *Blockchain: Enigma. Paradox. Opportunity*. London, U.K.: Deloitte LLP, 2016, pp. 1–27.

[100] (2018). *Understanding Blockchain Risks, Controls and Validation*. PWC. [Online]. Available: http://usblogs.pwc.com/emerging-technology/Blockchain-validation-infographic/

[101] *Report: The Distributed Ledger Technology Applied to Securities Markets*, ESMA (European Securities and Markets Authority), Paris, France, 2017, pp. 1–37.

[102] M. Michael and S. Mills, "The missing links in the chains? Mutual distributed ledger (aka blockchain) standards," *Long Finance, SSRN Electron. J.*, pp. 1–75, 2016. [Online]. Available: https://ssrn.com/abstract=3676283

[103] *Distributed Ledgers, Smart Contracts, Business Standards and ISO 20022*, SWIFT, SWIFT (Society for Worldwide Interbank Financial Telecommunications) Institute, La Hulpe, Belgium, 2016.

[104] S. Bogart and K. Riche, *Blockchain Report: Welcome to the Internet of Value*. New York, NY, USA: Needham Company LLC, 2015, pp. 1–57.

[105] W. He, S. Guo, Y. Liang, R. Ma, X. Qiu, and L. Shi, "QoS-aware and resource-efficient dynamic slicing mechanism for Internet of Things," *Comput., Mater. Continua*, vol. 61, no. 3, pp. 1345–1364, 2019.

[106] *Blockchain Healthcare 2016 Report: Promise & Pitfalls*, Tierion, Mountain View, CA, USA, 2016, pp. 1–8.

[107] *Blockchain Technology: How Banks are Building a Real-Time Global Payment Network*, Accenture Digital, Dublin, Ireland, 2016, pp. 1–12.

[108] M. Lamarque, "The Blockchain revolution: New opportunities in equity markets," Doctoral dissertation, Sloan School Manage., Massachusetts Inst. Technol., Cambridge, MA, USA, 2016, pp. 1–88.

[109] D. Broby and T. Karkkainen, "FINTECH in Scotland: Building a digital future for the financial sector," in *Center for Financial Regulation and Innovation*. Glasgow, U.K.: SSRN, 2016, pp. 1–31.

[110] D. Mills, K. Wang, B. Malone, A. Ravi, J. Marquardt, C. Chen, A. Badev, T. Brezinski, L. Fahy, K. Liao, V. Kargenian, M. Ellithorpe, W. Ng, and M. Baird, "Distributed ledger technology in payments, clearing, and settlement," in *Proc. FEDS Working Paper*, 2016, pp. 1–36.

[111] A. A. M. Jamel and B. Akay, "A Survey and systematic categorization of parallel K-means and Fuzzy-c-Means algorithms," *Comput. Syst. Sci. Eng.*, vol. 34, no. 5, pp. 259–281, 2019.

[112] A. Morrison, *Blockchain and Smart Contract Automation: Introduction and Forecast*. London, U.K.: PWC, 2016.

[113] D. Meijer and R. W. Carlo, *Blockchain and Standards: First Things First*. London, U.K.: FinExtra, 2016.

[114] Euro Banking Association, "Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios: An exploration for transaction banking and payments professionals," in *Proc. EBAWGEAP (Euro Banking Assoc. Working Group Electron. Alternative Payments)*, 2015, pp. 1–25.

[115] M. Mainelli and A. Milne, "The impact and potential of Blockchain on the securities transaction lifecycle," in *Proc. SWIFT Inst. Working Paper*, 2015, pp. 1–81.

[116] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[117] C. Brennan and W. Lunn, *Blockchain: The Trust Disrupter*. London, U.K.: Credit Suisse, 2016, pp. 1–135.

[118] *How Blockchains Could Change the World*, McKinsey & Company, New York, NY, USA, 2016, pp. 1–10.

[119] S. Deetman, "Bitcoin could consume as much electricity as Denmark by 2020," Leiden Univ., Leiden, The Netherlands, Tech. Rep., 2016. Accessed: 2020. [Online]. Available: http://motherboard.vice.com/read/bitcoincould-consume-as-much-electricity-as-denmark-by-2020

[120] M. Mainelli and B. Manson, *Chain Reaction: How Blockchain Technology Might Transform Wholesale Insurance*. London, U.K.: Z/Yen Group, Long Finance Report, 2016, pp. 1–60.

[121] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *Proc. ONC/NIST Use Blockchain Healthcare Res. Workshop*, 2016, pp. 1–10.

[122] Y. Sun, Y. Yuan, Q. Wang, L. Wang, E. Li, and L. Qiao, "Research on the signal reconstruction of the phased array structural health monitoring based using the basis pursuit algorithm," *Comput., Mater. Continua*, vol. 58, no. 2, pp. 409–420, 2019.

[123] K. Kaur and K. Kaur, "Failure prediction, lead time estimation and health degree assessment for hard disk drives using voting based decision trees," *Comput., Mater. Continua*, vol. 60, no. 3, pp. 913–946, 2019.

[124] M. Luo, K. Wang, Z. Cai, A. Liu, Y. Li, and C. Fong Cheang, "Using imbalanced triangle synthetic data for machine learning anomaly detection," *Comput., Mater. Continua*, vol. 58, no. 1, pp. 15–26, 2019.

[125] J. Qiu, Y. Liu, Y. Chai, Y. Si, S. Su, L. Wang, and Y. Wu, "Dependency-based local attention approach to neural machine translation," *Comput., Mater. Continua*, vol. 59, no. 2, pp. 547–562, 2019.

[126] K. M. Hamdia, H. Ghasemi, X. Zhuang, N. Alajlan, and T. Rabczuk, "Computational machine learning representation for the flexoelectricity effect in truncated pyramid structures," *Comput., Mater. Continua*, vol. 59, no. 1, pp. 79–87, 2019.

[127] F. Xu, X. Zhang, Z. Xin, and A. Yang, "Investigation on the chinese text sentiment analysis based on convolutional neural networks in deep learning," *Comput., Mater. Continua*, vol. 58, no. 3, pp. 697–709, 2019.

[128] A. Maamar and K. Benahmed., "A hybrid model for anomalies detection in AMI system combining K-means clustering and deep neural network," *Comput., Mater. Continua*, vol. 60, no. 1, pp. 15–39, 2019.
[129] Z. Xu, Q. Zhou, and Z. Yan, "Special section on recent advances in artificial intelligence for smart manufacturing—Part II intelligent automation & soft computing," *Intell. Automat. Soft Comput.*, vol. 25, no. 4, pp. 787–788, 2019.
[130] X. Wu, C. Luo, Q. Zhang, J. Zhou, H. Yang, and Y. Li, "Text detection and recognition for natural scene images using deep convolutional neural networks," *Comput., Mater. Continua*, vol. 61, no. 1, pp. 289–300, 2019.
[131] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)*, Nov. 2017, pp. 1–4.
[132] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informat. J.*, vol. 25, pp. 1398–1411, Dec. 2019.
[133] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3.
[134] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.
[135] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.
[136] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS-A blockchain based approach for smart healthcare system," in *Healthcare*, vol. 8, no. 1. Amsterdam, The Netherlands: Elsevier, Mar. 2020, Art. no. 100391
[137] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes," *IEEE Access*, vol. 8, pp. 118433–118471, 2020.
[138] J. Oh and I. Shong, "A case study on business model innovations using blockchain: Focusing on financial institutions," *Asia Pacific J. Innov. Entrepreneurship*, vol. 11, no. 3, pp. 335–344, Dec. 2017.
[139] A. Turner and A. S. M. Irwin, "Bitcoin transactions: A digital discovery of illicit activity on the blockchain," *J. Financial Crime*, vol. 25, no. 1, pp. 109–130, Jan. 2018.
[140] S. Yoo, "Blockchain based financial case analysis and its implications," *Asia Pacific J. Innov. Entrepreneurship*, vol. 11, no. 3, pp. 312–321, Dec. 2017.
[141] 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.
[142] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommun. Policy*, vol. 41, no. 10, pp. 1027–1038, Nov. 2017.
[143] S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, pp. 1–18, 2019.
[144] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019.
[145] T.-T. Kuo, J. Kim, and R. A. Gabriel, "Privacy-preserving model learning on a blockchain network-of-networks," *J. Amer. Med. Inform. Assoc.*, vol. 27, no. 3, pp. 343–354, Mar. 2020.
[146] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3548–3558, Jun. 2019.
[147] Y. Qiu, Y. Liu, X. Li, and J. Chen, "A novel location privacy-preserving approach based on blockchain," *Sensors*, vol. 20, no. 12, p. 3519, Jun. 2020.
[148] R. M. Parizi, A. Dehghantanha, K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contracts security testing on Blockchains," in *Proc. 28th Annu. Int. Conf. Comput. Sci. Softw. Eng.*, 2018, pp. 103–113.
[149] 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)*, Mar. 2018, pp. 19–25.
[150] L. Chenxin, L. Peilun, Z. Dong, Y. Zhe, W. Ming, Y. Guang, X. Wei, L. Fan, and C. Y. Andrew, "A decentralized blockchain with high throughput and fast confirmation," in *Proc. USENIX Annu. Tech. Conf. (USENIX ATC)*, 2020, pp. 515–528.
[151] K. Nicolas and Y. Wang, "A novel double spending attack countermeasure in blockchain," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2019, pp. 383–388.
[152] A. Begum, A. H. Tareq, M. Sultana, M. K. Sohel, T. Rahman, and A. H. Sarwar, "Blockchain attacks, analysis and a model to solve double spending attack," *Int. J. Mach. Learn. Comput.*, vol. 10, no. 2, pp. 1–6, 2020.
[153] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, p. 1788, Apr. 2019.
[154] L. Odera. (2020). *Ethereum Classic & IOHK Team Up to Find Solutions to Prevent 51% Attacks On The Blockchain*. Accessed: Dec. 20, 2020. [Online]. Available: https://bitcoinexchangeguide.com/ethereum-classic-iohk-team-up-to-find-solutions-to-prevent-51-attacks-on-the-blockchain/
[155] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key management for blockchain technology," in *ICT Express*. Amsterdam, The Netherlands: Elsevier, Aug. 2019, pp. 1–5, doi: 10.1016/j.icte.2019.08.002.
[156] B. Bhushan and N. Sharma, "Transaction privacy preservations for blockchain technology," in *Proc. Int. Conf. Innov. Comput. Commun.*, Singapore: Springer, Jul. 2020, pp. 377–393.
[157] M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, "Countering selfish mining in blockchains," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 360–364.
[158] K. Nicolas, Y. Wang, and G. C. Giakos, "Comprehensive overview of selfish mining and double spending attack countermeasures," in *Proc. IEEE 40th Sarnoff Symp.*, Sep. 2019, pp. 1–6.
[159] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO insider attack in RPL's Internet of Things networks," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 68–71, Jan. 2019.
[160] Q. Xing, B. Wang, and X. Wang, "POSTER: BGPCoin: A trustworthy blockchain-based resource management solution for BGP security," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 2591–2593.
[161] P. Swathi, C. Modi, and D. Patel, "Preventing sybil attack in blockchain using distributed behavior monitoring of miners," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–6.
[162] L. Er-Rajy, A. El Kiram My, M. El Ghazouani, and O. Achbarou, "Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures," *J. Internet Banking Commerce*, vol. 22, no. 3, pp. 1–29, 2017.
[163] Karame, G. and E. Androulaki, *Bitcoin and Blockchain Security*. Norwood, MA, USA: Artech House, 2016.
[164] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 5, pp. 840–852, Sep. 2018.
[165] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems," in *Proc. Int. Symp. Rules Rule Markup Lang. Semantic Web*, Cham, Switzerland: Springer, Jul. 2016, pp. 167–183.
[166] A. Kiayias, and G. Panagiotakos, "Speed-security tradeoffs in blockchain protocols," *IACR Cryptol. ePrint Arch.*, vol. 2015, pp. 1–27, Dec. 2015.
[167] C. Cachin, "Blockchains and consensus protocols: Snake oil warning," in *Proc. 13th Eur. Dependable Comput. Conf. (EDCC)*, Sep. 2017, pp. 1–2.
[168] K. Jae. (Jul. 8, 2018). *Tendermint: Consensus Without Mining*. Accessed: 2020. [Online]. Available: https://tendermint.com/static/docs/tendermint.pdf
[169] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," in *Peer-to-Peer Networking and Applications*. Springer, Aug. 2020, pp. 1–13.
[170] J. Song, Q. Zhong, W. Wang, C. Su, Z. Tan, and Y. Liu, "FPDP: Flexible privacy-preserving data publishing scheme for smart agriculture," *IEEE Sensors J.*, early access, Aug. 18, 2020, doi: 10.1109/JSEN.2020.3017695.
[171] Z. Lejun, H. Tianwen, H. Xiaoyan, Z. Zhijie, W. Weizheng, G. Donghai, Z. Chunhui, and K. Seokhoon, "A distributed covert channel of the packet ordering enhancement model based on data compression," *Comput., Mater. Continua*, vol. 64, no. 3, pp. 2013–2030, 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.

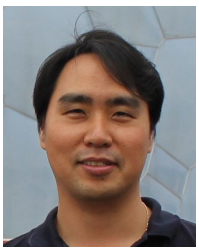
[173] S. More, J. Singla, S. Verma, Kavita, U. Ghosh, J. J. P. C. Rodrigues, A. S. M. S. Hosen, and I.-H. Ra, "Security assured CNN-based model for reconstruction of medical images on the Internet of healthcare things," *IEEE Access*, vol. 8, pp. 126333–126346, 2020.
[174] A. S. M. S. Hosen, S. Singh, P. K. Sharma, U. Ghosh, J. Wang, I.-H. Ra, and G. H. Cho, "Blockchain-based transaction validation protocol for a secure distributed IoT network," *IEEE Access*, vol. 8, pp. 117266–117277, 2020.
[175] A. S. M. S. Hosen, S. Singh, P. K. Sharma, M. S. Rahman, I.-H. Ra, G. H. Cho, and D. Puthal, "A QoS-aware data collection protocol for LLNs in fog-enabled Internet of Things," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 430–444, Mar. 2020.
[176] I. Batra, S. Verma, A. Malik, U. Ghosh, J. J. Rodrigues, G. N. Nguyen, A. S. M. Hosen, and V. Mariappan, "Hybrid logical security framework for privacy preservation in the green Internet of Things," *Sustainability*, vol. 12, no. 14, pp. 1–15, 2020.

OVERVIEW REFERENCES

[S1] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: challenges and solutions," 2016, *arXiv:1608.05187*. [Online]. Available: https://arxiv.org/abs/1608.05187
[S2] I. Lin, and T. Liao, "A survey of blockchain security issues and challenges," *IJ Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.
[S3] 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.
[S4] 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, 4th Quart., 2018.
[S5] P. Taylor, T. Dargahi, A. Dehghantanha, R. Parizi, and K. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, 2019.
[S6] M. Hassan, M. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512-529, Aug. 2019.
[S7] M. 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.
[S8] E. De Aguiar, B. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–27, 2020.
[S9] 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.

SAURABH SINGH received the Ph.D. degree from Jeonbuk National University, Jeonju, South Korea, carrying out his research in the field of ubiquitous security. He was a Postdoctoral Researcher with Kunsan National University, South Korea. He currently joined as an Assistant Professor with Dongguk University, Seoul, South Korea. He has published many SCI/SCIE journals and conference papers. His research interests include blockchain technology, cloud computing and security, the IoT, deep learning, and cryptography. He received the Best Paper Award from KIPS and CUTE Conference, in 2016.

A. S. M. SANWAR HOSEN received the Ph.D. degree in computer science and engineering from Jeonbuk National University (JBNU), Jeonju, South Korea. He worked as a Postdoctoral Researcher with the School of Computer, Information and Communication Engineering, Kunsan National University. He is currently working as a Research Assistant Professor with the Division of JBNU. He has published several articles in journals and international conferences. His research interests include wireless sensor networks, the Internet of Things, network security, data distribution services, fog-cloud computing, artificial intelligence, blockchain, and green IT. He serves as a reviewer for several reputed journals.



BYUNGUN YOON (Senior Member, IEEE) is currently a Professor with the Department of Industrial and Systems Engineering, Dongguk University. His theme of study has involved blockchain technology, patent analysis, new technology development methodology, and visualization algorithms. His current research interests include enhancing technology road mapping, research and development quality, and product designing with data mining techniques.