A Project Report

on

Blockchain Security

Submitted in partial fulfillment of the requirement for the award of the degree of

Btech CSE Core Sec-2

Under The Supervision of Ms. Poonam
Designation Assistant Professor

Submitted By
Lucky
20SCSE1010400

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING GALGOTIAS UNIVERSITY, GREATER NOIDA INDIA

CERTIFICATE

The Final Project Viva-Voce examination of Aman Kumar has been held on_____ and his work is recommended for the award ofB.Tech-CSE.

Signatureof Examiner(s) Signature ofSupervisor(s)

Signature ofProjectCoordinator Signature ofDean

Date: 24 Decembe r 2021
Place: Greater Noida

12/2021

A Review of Blockchain Technology and Its Applications in the Business Environment

GALGOTIS UNIVERSITY, GREATER NOIDA

DEPARTMENT OF COMPUTER SCIENCE AND TECHNOLOGY

Abstract

Blockchain is the technology that can lead to significant changes in our business environment and will have great impact on the next few decades. It can change the way we perceive business processes, and can transform our economy. Blockchain is a decentralized and distributed ledger technology that aims to ensure transparency, data security and integrity, since it cannot be tampered or forged.

Most of the current research related to Blockchain Technology is focusing on

its application for cryptocurrencies, such as Bitcoin and only a limited number of research is targeted at exploring the utilization of Blockchain Technology in other environments or sectors. Blockchain Technology is more than just cryptocurrency, and it can have several applications in government, finance and banking industry, accounting and Business Process Management. Therefore, this study attempts to investigate and explore its opportunities and challenges for the current or future applications of Blockchain Technology. Thus, a large number of published studies were carefully reviewed and analyzed based on their contributions to the Blockchain's body of knowledge.

Key words: Blockchain Technology, Ledger, Applications, Business

I. Introduction

Blockchain technology is a revolutionary computer protocol used for digital recording and storing information on multiple computers or multiple nodes. One of the most important elements of Blockchain is the so-called "Ledger", which is similar to a relational database Walport (2016). A Blockchain is a list of encrypted digital record or transaction, called a block. Each block is then "chained" to the next block, in a linear, chronological order, using a cryptographic signature (Bogart & Rice 2015). The blocks contain a copy of the last transactions since the last block was added (Bogart & Rice 2015). Thus, the shared block, or ledger, is linked to all participants who use their computers in a network to validate or confirm transactions, removing the need for a thirdparty, (Christidis, & Devetsikiotis, 2016; Porru, et. al., 2017).

Blockchain is used to secure and distribute data in a new and unique way. The elimination of a central instance in the distributed network implies a radical shift to direct transactions between non-intermediaries or intermediary services (Tapscott & Tapscott 2016). Thus, Blockchain can only be updated by consensus between participants in the system and a transaction can never be altered or deleted, (Fanning & Centers 2016). Its distributed database cannot be hacked, manipulated or disrupted in the same way as a traditional, centralized database with a user-controlled access system.

In other words, the data is immutable and once it has been written to a Blockchain, nobody, not even a system administrator, can modify or delete it from the ledger. Since, each data block is time stamped and linked in a chronological order via a cryptographic signature Walport (2016). Blockchain Technology can be applied almost in any type of transaction, involving value, such as money, goods, land ownership, medical records or even votes.

Blockchain does not require data migration in a project; all relevant transaction data will be stored on the ledger and status will be then derived from it. Since, Blockchain is a distributed system without a central control point or authority (Glaser& Bezzenberger 2015; Tapscott & Tapscott 2016) and it is not regulated by a single control center as there might be with a system administration, there's no single point of failure. Hence, in an enterprise, theoretically, there would be no need for an IT professional to monitor security on a blockchain database.

Despite these possibilities, it's important to emphasize that Blockchain is a very new technology. As a result, there are only a small number of instances in which the technology has been applied Aru (2017). A proven example, could be the Bitcoins which is the most successful implementation of the Blockchain Technology, and has confirmed to be a viable solution in creating trust in a trust-less ecosystem without central authority.

The methods of this this paper were mainly: data collection and grounded theory. Data collection and ground theory was done in different ways. For instance, the paper thoroughly searched all published works found in the exiting literature, books, academic journals, presentations, conferences, technical reports, searching several databases using keywords.

The objective of this study is to present a review of the Blockchain Technology and its current or future practical applications. Thus, in the next section we present a systematic literature review to identify current Blockchain applications and discuss future practical applications.

The remainder of the paper is organized as follows: Section II presents an overview of the Concept of Blockchain Technology; Section III describes in detail the Applications of Blockchain Technology in Business; Section IV presents the Challenges and Barriers of Blockchain Technology; and finally Conclusions and Recommendations are drawn in Section V.

II. The Concept of Blockchain Technology

Blockchain Technology is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash code of the previous block, a timestamp and transaction data (Bogart & Rice 2015), which as designed so that these transactions are immutable.

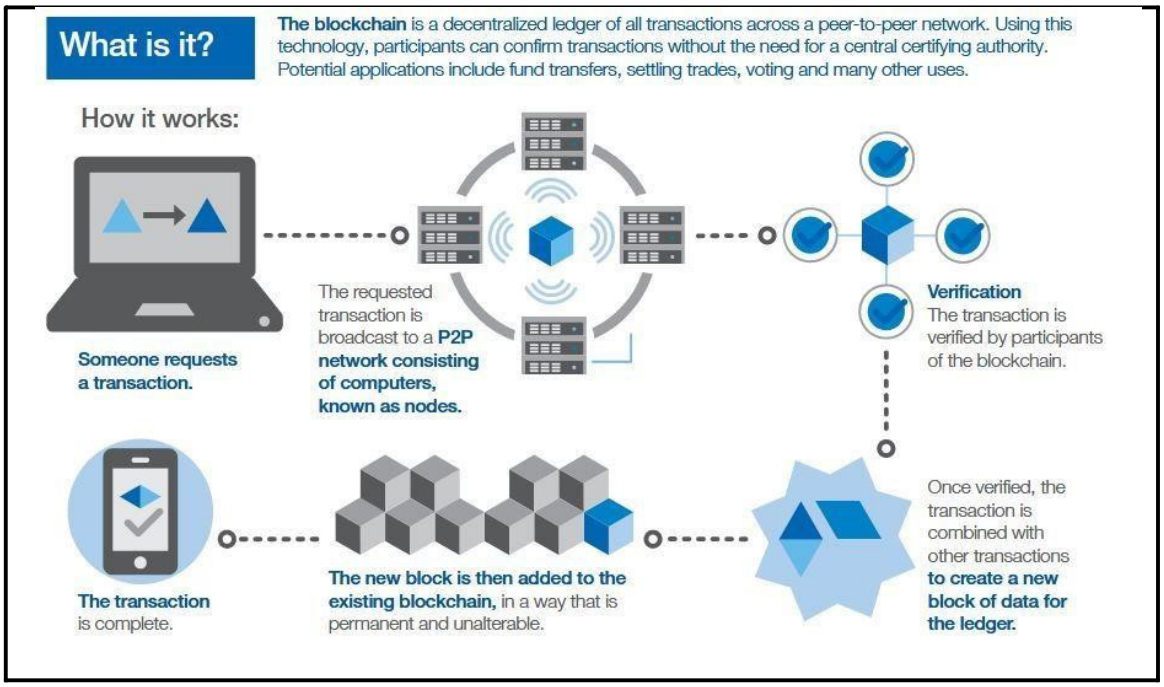

Figure 1: *The Concept of Blockchain Technology*
Source: *World Economic Forum*

The Blockchain concept was devised by Nakamoto (2008) and is displayed in Figure 2. Blockchain or Distributed Ledger Technology (DLT) is a distributed ledger recording technology (Walport 2016), which contains information about transactions or events. It can record transactions in a transparent, secure, decentralized, efficient, and low-cost way (Schatsky & Muraskin 2015; Bahga, A., Madisetti, V., 2016; Bahga, A. & Madisetti V., 2014).

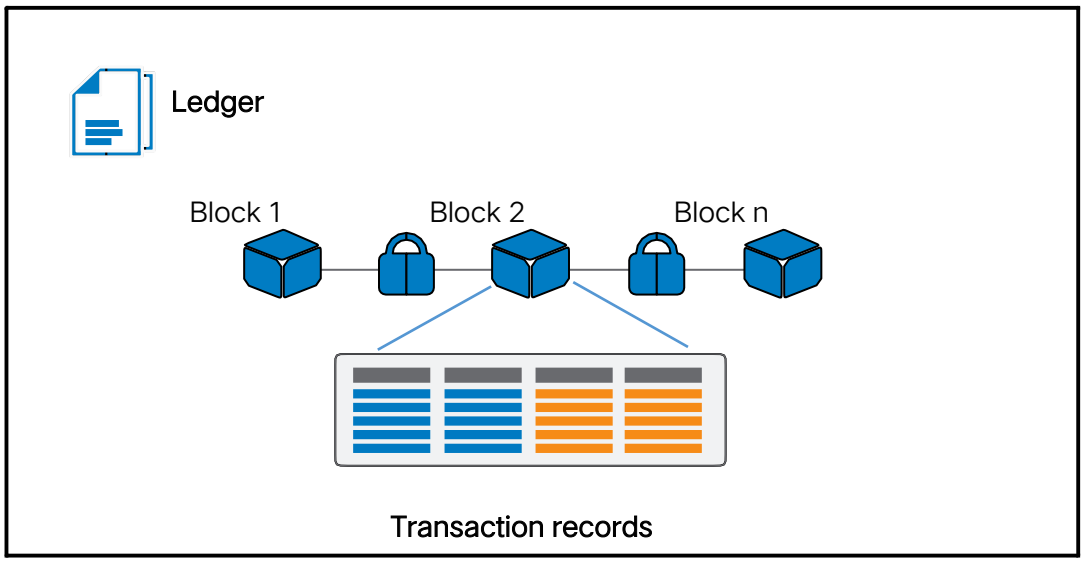

Figure 2: *The Concept of Blockchain Technology:*

Source: *illustration based on Bitcoin (2015) and Nakamoto (2008)*

Hence, the Blockchain Technology has the following characteristics: a distributed ledger, decentralized data management, data security, transparency and integrity, anti-tampering and anti-forgery, high efficiency, low cost, programmable features that increase flexibility and reliability and no risk of a centralized database failure (Glaser & Bezzenberger 2015; Tapscott & Tapscott 2016; Swan 2015).

There are several types of Blockchains, some of the most important are: Public Blockchain, Private Blockchain and Consortium Blockchain (hybrid Blockchain). Each type has its advantages and disadvantages, allowing them to meet the needs of various applications (He et al., 2016; Buterin (2015). Figure 3 illustrates the Types of Blockchain Technology.

Specifically, using a) *Public Blockchain*, anyone can transact on the network transactions which are transparent and are anonymous. A Public Blockchain, such as bitcoin, is completely decentralized. The system operates based on users' consensus; there is no central point of failure. However, Public Blockchain is vulnerable to system attacks. For instance, an attacker could recreate and properly chain all the blocks that had been modified, without being detected by the participants; b) *Private Blockchain*, the transactions are secret, the data is not available for public view, but the members are known. In a private Blockchain network, a participant cannot read or write the Blockchain unless the participant has a permission or an invitation to join the network. Private Blockchain is usually used by large companies with permissions defined

between various stakeholders of the enterprise Blockchain. For instance, a bank can have its own Blockchain network for its private use with restricted access to its various stakeholders such as customers, employees and suppliers; c) *Consortium Blockchain* is a hybrid model of both Public and Private

Blockchain. Choosing this model, enterprises or institutions can have their own Private Blockchain network to share the data among the consortium participants (such as banks, institutions and other enterprises or firms).

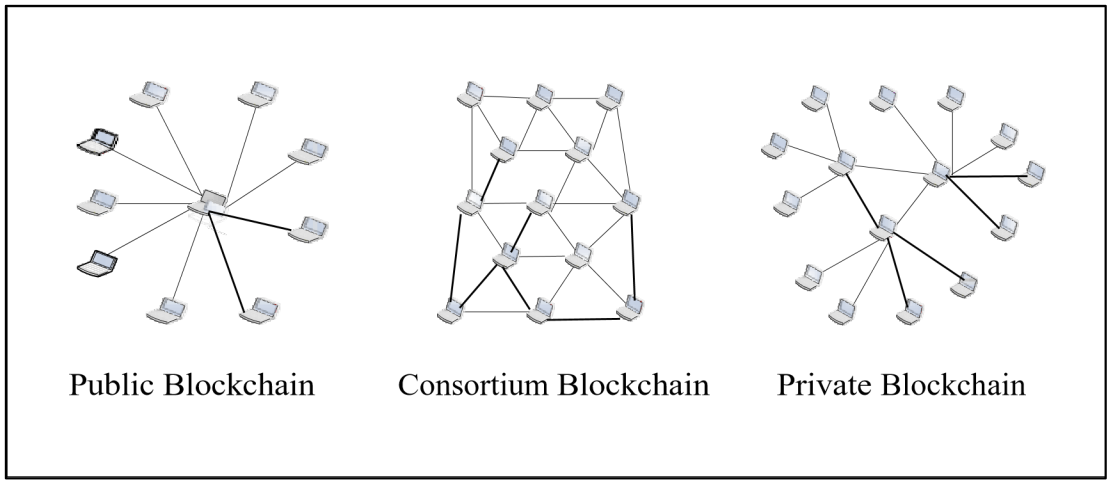

Figure 3: *Illustrates the Types of Blockchain Technology*

CHALLENGES

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. More- over, 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 out- lines some open questions and research challenges, and open requirements that could improve blockchain-IoT capability.

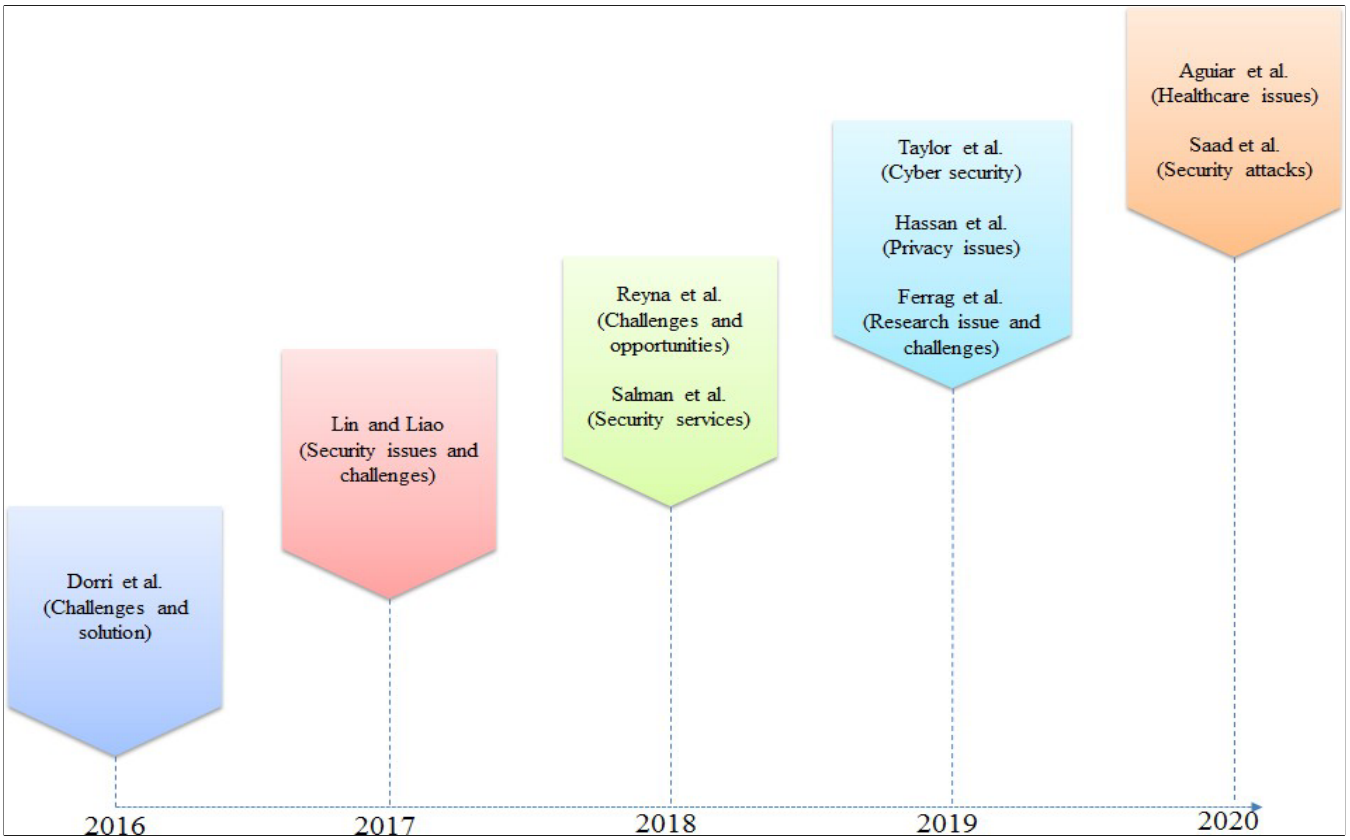

FIGURE 1. Roadmap of different literature on security issues, attacks, and solutions in blockchain technology between 2016 and 2020.

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. The authors also provided a blockchain- based solution. Lin and Liao 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. Salman et al. 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 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. 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. 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. systematically explored the attack surface in terms of blockchain cryptographic construct, distributed architecture, and blockchain application context, while pro- viding 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, trans- actions are validated and data cannot be destroyed. While the decentralized nature of networks allows for peer-to-peer operations, it also poses major challenges to personal data privacy. Gai et al. surveyed some of these security and privacy issues, which include threats, malicious adversaries, and attacks in financial industries. Zyskind et al. examined decentralized personal data management in the context of personal data privacy concerns.

2) CONSENSUS MODEL

Consensus refers to agreement among entities, 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. 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.

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

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

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. 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. 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 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, 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 Com- poser; regarding enterprise ecosystems, MentaGo provides a blockchain solution for financial systems and SXSW uses Hyperledger fabric and IBM.

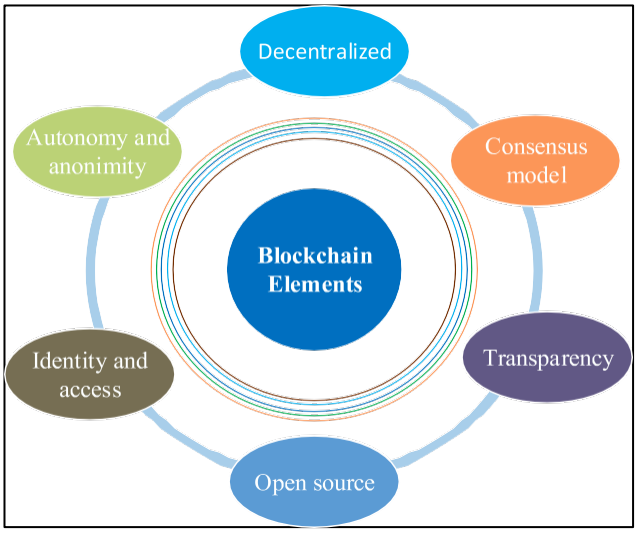

FIGURE 2. Blockchain elements.

6) ANONYMIZATION

Anonymity is one of the most important elements 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

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. Möser 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 num bers 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. 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. presented an in -depth analysis of the current regulatory land- scape of distribution technology, and Yeoh 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 con- tracts 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 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. 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.

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.

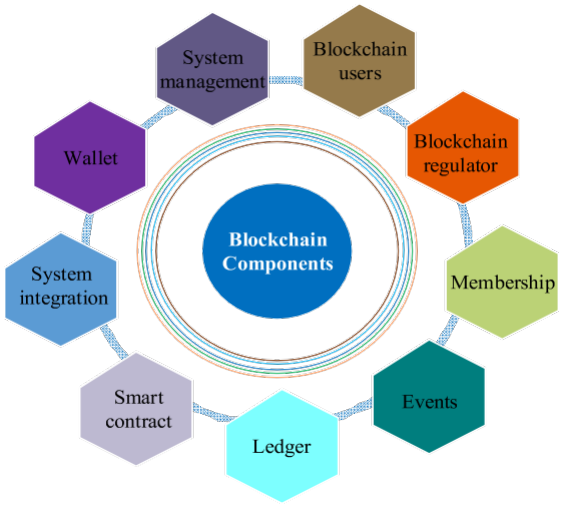

FIGURE 3. Blockchain components

Smart Contract: Encapsulates the business network trans- actions 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 certifi- cates 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, confiden- tiality, 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. who discussed blockchain attacks and security risks. Here, we discuss some of these attacks in further detail.

1) Liveness Attack: Kiayias and Panagiotakos 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. 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. 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 mali- cious miner can do this or dishonest who creates a larger arrival rate than the sum of all other legitimate or honest min- ers”. 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 com- puting 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. By starting a 51% attack, an attacker can arbitrarily manipulate and change blockchain information and perform the following actions:

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. 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 transac- tion. 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.

Wallet privacy leakage can also occur, where com- mon bitcoin wallet operations leak some user information ; this leakage has been exploited in the past. Paul Fremantle et al. 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, 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. 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. 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.

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 net- work by manipulating the BGP, after which data can be routed and the traffic can be modified to the attacker's favor.

Apostolakiet al. 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.

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 trans- action 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.

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.

2) Network Security: An eclipse attack occurs when an opponent controls pieces of network communication and logically divides the network to increase synchronization delay; an example is a simple denial of service attack to improve selfish mining and double-spending. 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. 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.

4) Redundancy: Expensive duplication for the purpose of eliminating the arbitration that allows each node of the net- work 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

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

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 regu latory challenges, but infrastructure regulation is very similar to blockchain regulation. Yeoh discussed the key regulatory issues affecting the blockchain and innovation distributed technology that has been adopted across Europe and the United States.

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-47fc9ce66379)		[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]

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. 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.

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”. 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. 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,

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

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]

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. 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, including in areas such as

1) the blockchain job market,

2) DTL,not be easy to clearly assess its broader economic impacts over the medium to long term. 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 decentral- ized nature and its function as a constant record, establishing clear governance rules is important for both authorized and unauthorized ledgers. Part of the likely challenge with this governance is the result of selecting a ledger out- side 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. New technology standards can be decisive, particularly with respect to the tightly regulated financial sector. According to Lamarque et al., 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.

1) Regulatory bodies need to develop better understand- ings of ledger activity.

2) Regulatory uncertainty generates platform, price, and novelty risks.

3) Regulators must ensure that innovation is not sup- pressed while simultaneously protecting the end-user privileges.

6) Interoperable Implementations: To realize all the ben- efits 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. One author emphasized the potential risk of inconsistent devel- opments in technology, which can lead to fragmented markets. Some authors have promoted enabling seamless

interactions between blockchain technology and legacy systems. Meijer and Carlo highlighted some imple- mentation standards:

1) intensified conversation

2) concern about interoperability and competition in frag- mented blockchains

3) common interoperability standards for different pro- tocols, 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. Organizations need to ensure that only people with the appropri- ate permissions can access the data and that any

access complies with general data protection laws Lamarque 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. 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 . Some authors have suggested that nodes in distributed ledgers need to be able to view trans- action 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 permission- less ledgers.

9) Energy-Intensive: DLT/blockchain has attracted substantial interest from technology firms, financial institutions, and other user communities. One issue with such technolo- gies is that the ledgers are significantly more energy-intensive than centralized legacy systems; Bitcoin blockchains, for instance, are highly energy-intensive. 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 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. Charles Brennan and William Lunn described how the Ethereum hack was implemented in DLT/blockchain and revealed certain flaws in smart contracts. Many of the challenges associated with smart contracts stem from the lack of clarity and diverse definitions in the contracts them- selves, 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 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. 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 identfication number and an encrypted link along with timestamps to indicate the latest data modifications.

Alhadhrami et al. also discussed how blockchains could be used in the health care sector to maintain, val- idate, 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 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 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. 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. have suggested how blockchain tech- nology 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 intoperability of healthcare databases, accessibility to patient medical records, prescription databases,

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

and device tracking. Moreover, the authors have proposed an access control policy algorithm for improving medical data

accessibility between healthcare providers.

Tripathi et al. 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 trans- parent flow in a secured and privacy-preserved manner.

Kumar et al. performed the simulation and implementation of a novel healthcare design using the 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 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. discussed how Bitcoin is being lever- aged for malicious activities and crimes online. The biggest advantage of Bitcoin is the anonymity of transactions; all personally identifiable information is hidden in the transac- tions. 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 anony- mous 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 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 trans- actions. Moreover, transfers of funds that were previously conducted across banks through gradual gold transfers have now been reduced and partially replaced by cryptocurrency

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 secrity and privacy of customer transactions. Table 5 summarizes the existing blockchain research solutions in the transaction sector.

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

C. BLOCKCHAIN FOR PRIVACY AND SECURITY

Joshi et al. discussed the huge expansion of blockchain technology with an emphasis on the privacy and the security of the vast amounts of data involved. Blockchain trans- actions 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. 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 . 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 loca- tion 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 .

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

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. 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 pro- posed method does not require a third-party anonymizing server, instead satisfying the principle of k-anonymity privacy protection.

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

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

E. SECURITY VULNERABILITY AND TOOLS

Blockchain smart contracts offer security and privacy, but their vulnerabilities must be further understood. Here, we dis- cuss 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.

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, and $32 million was taken by attackers in 2017 . 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.

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.

TABLE 8. Tools and vulnerability.

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

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. One is the optimal strategy that allows quick confirmation and the other is the conservative strategy that guarantees the progress of consen- sus. Conflux is a scalable and decentralized system with high 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 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 addi- tion, Begum et al. 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 have focused on crypto-coin with low hashing power to ana- lyze 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, imple- menting a “Permapoint” finality arbitration system to limit chain re-organizatio.

4) PRIVATE KEY SECURITY ATTACK

Pal et al. 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 Sharmapresented 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. 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 have done a comprehen- sive 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 pro- posed a scheme by conducting experiments using the Con- tiki tool, a low -power-designed tool for resource-constrained devices.

8) BGP HIJACKING ATTACK

Xang et al. 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 secrity solution on the Etherium blockchain and smart contract programming.

9) SYBIL ATTACK

To prevent Sybil attacks in blockchain networks, Swathi et al. 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 seg- ment has a security model plan. 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. 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 develoers 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 syste. 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. Hawk protects the personal information records on a blockchain system because it uses the private smart contract that automatically generates an effective cry tographic model.

4) TOWN CRIER

Application: Town crier works by recovering data demands from clients and gather information from HTTP web- sites. 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.

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

6) SEGWIT

Application: Segwit is one of the sidechain features that runs in parallel with the main Blockchain network. 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. 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 personel to detect anomalous behavior in the network and prevent attacks on the system.

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.

However, some cryptographic works have been done to improve the blockchain network. For example, Wang et al. 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 have worked on security and privacy con- cerns for smart agriculture systems by proposing a data aggre- gation scheme with a flexible property that utilizes

ElGamal cryptosystem. Zhang et al. 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.

TABLE 9. Solving security 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 Integrity of data	No Yes	No No	Yes Yes	No No	Yes No	No Yes	Yes No	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 vulnerble. 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 comprmise 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 implemen- tation 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 under- stand 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 opera- tion, 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, com- bating, detecting, and monitoring of employees. Non-compromising models are required to detect and prevent false alarms in the aspects of the blockchain system.

III. The Applications of Blockchain Technology in Business

The following section is presenting some of the practical applications of Blockchain Technology in different sectors. Applications have been categorized into the following groups: Smart Contracts, Government, Financial industry and Accounting and Business Process Management.

1. Smart Contracts

According to Szabo (1994), a Smart Contract is a computerized protocol that executes the terms of a contract. Simply, Smart Contract is an ordinary contract, but it is written in computer code to be executed in the Blockchain environment Gates (2017). Thus, such agreements in the IT-environment are frequently referred to as Smart Contracts Savelyev (2017).

A Smart Contract is designed to assure one party that the counterparty will fulfill his promises with certainty. The

Blockchain concept aims to remove third-party intermediary for transactions. Traditionally this third-party is responsible for maintaining and executing the contracts and build the trust between any involved parties (Porru, et. al., 2017). Thus, Smart Contracts can overcome moral hazard problems such as strategic default, and they can dramatically reduce costs of verification and enforcement.

One of the most promising areas of implementation of Blockchain Technology is its use for creating fully automated Smart Contracts, which are performed without human involvement. Smart Contracts allow for automatic procedures for repeat transactions, or transactions with a certain level of importance.

Blockchain will automatically verify, execute and enforce the contract terms between agreed parties. These contracts are called Smart because they can be partially or fully self-executing and self-enforcing Gates (2017).

Some Blockchain Applications of Smart Contracts are the following:

- *Contract Management* – Blockchain Technology in a Contract Management provides a solution for companies validating contract information that could be highly beneficial for organizations and enterprises of all kinds of businesses, such as in the technical industries and construction (Christidis & Devetsikiotis 2016). Thus, Contract Management via Blockchain Technology would allow organizations to optimize the performance of their supply chains, evaluating vendors and obtain higher value and shorter lead times Morrison (2016).

- *Entertainment* – Blockchain within Smart Contract provides a transparent transference of royalties in real-time distributions to everyone involved in both the music and film industries (Dair & Beaven 2017).

- *Healthcare* – The healthcare sector has already taken steps of the use of Blockchain Technology. Smart Contracts can be used in medical industries for keeping tabs between payers, providers, and drug manufacturers. Healthcare

providers can set up Smart Contracts for any payer or supplier, which is then stored in their digital records Mettler (2016).

- *Insurances* – Insurance is a new sector for Blockchain Technology where the industry is estimated to spend more than $2 billion each year on fraud and compliance. The use of Blockchain Technology has significant potential for the entire insurance value chain. Certain insurance products can be automated through Smart Contracts. Blockchain has the potential to eliminate error, negligence and detect fraud and verify the authenticity of customers and their policies.

- Blockchain Internet-of-Things – Internet-of-Things (IoT) is a system of interconnected computing devices to the internet, mechanical and digital machines, objects, animals or people that are provided with unique identifiers with the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction (Bahga &, Madisetti, 2016). It allows the collection and exchange of data with one another, (Chen, et al., 2015; Dorri, et al., 2017) using sensors, embedded software, and a common language to communicate.

  Gartner (2017) predicts that there will be 20.4 billion IoT devices by the year of 2020. With this number of devices to join IoT hubs in the future, the system could show vulnerability, such as network security, speed, and affordability. Blockchain Technology deals with the problems mentioned and strengthens the interconnectedness of IoT. Its network will enable devices to perform smoothly, securely, and autonomously by creating Smart Contracts that are only implemented upon the accomplishment of specific requirements. This encourages better automation, cheap transfers (no need for third-party to supervise transactions), scalability, and security (prevents overrides and compromise of network security), (Christidis & Devetsikiotis, 2016) since Blockchain provides one interface for all devices to be controlled.

2. Blockchain Technology for Implementing e-Government

The ability of Blockchain Technology to record transactions on distributed ledgers offers new opportunities for governments to improve transparency, prevent fraud, and establish trust in the public sector. Blockchain has the potential to make government operations more efficient by improving the delivery of public services and increasing trust in public sectors, Konashevych (2017). Similar, Ølnes, et al., (2017), stated that Blockchain Technology presents a lot of benefits for governments such as data integrity, improving transparency, enhance security, preventing fraud, and establish trust and privacy by recording transactions on distributed ledgers for the state management system. Thus, a distributed ledger is a unique tool for the improvement of transparency of the budgetary process and the reduction of corruption factors.

Using Blockchain Technology, cryptocurrency tools and Smart Contracts, is possible to build an e-Government. Since a distributed ledger contains legally valid information, a number of mechanisms and procedures of interaction between citizens

and the state, could be implemented through Smart Contract. The source code eliminates the risk of unauthorized changes and ensures the uniqueness of the execution of the contract algorithm at any time and at any node of the network. Thus, state documents, e-voting, auctions, public procurement and the registration of companies could be possible through Blockchain Technology, preventing fraud, establishing trust between the citizens and the state, and enhancing business performance in the public sector (Barnes et al., 2016).

In the present, numerous countries such as the USA, China, United Kingdom, Sweden, Netherlands, United Arab Emirates and Estonia announced Blockchain initiatives to explore its uses in the public sector and in government. Deloitte Insights (2017) indicated that some of the potential benefits such as trust and transparency can be especially beneficial for developing countries since they are more vulnerable to corruption, fraud, and lack of trust than developed countries.

In closing, adopting Blockchain Technology and Smart Contracts will be possible to implement an e-Government. Thus, e-Government with Blockchain Technology will significantly reduce bureaucracy, exclude hard copy paperwork, minimize transaction costs, fully control officials, eliminate fraud, fight corruption and as a result, it will improve business performance in the public sector.

3. Blockchain Technology for Financial industry

According to Iansiti & Lakhani (2017), Blockchain is a foundational Technology having the potential to dramatically reduce the cost of transactions and reshape the economy. Harvard Business Review stated that Blockchain Technology will do to financial institutions what the internet did to media (Joichi, et al., 2017).

Blockchain was initially developed as the backbone for Bitcoin, which is the most popular decentralized digital currency Nakamoto (2008). Blockchain is particularly beneficial for financial transactions and banks, and has the potential to solve a lot of problems, when it comes to exchanging data, information, and money (Tapscott & Tapscott 2016). Financial institutions and banks can handle sensitive information with Blockchain and provide secure services with minimum risk that can be decentralized and transparent at a low cost Forrest (2016). Broby & Paul (2017) discussed the importance of Blockchain in the financial settlements, and in enhancing the reliability of financial statements. Similarly, Brian (2017) stated that Blockchain as a technology can revolutionize economic sectors resulting in lower transaction costs, and highlighted numerous advantages of this technology.

Now days, the leading platforms for Blockchain development in financial industry are Hyperledgers, an open-source industry consortium formed by the Linux Foundation, and Ethereum, a custom-built platform that was introduced in 2013. As of February 2018, more than 1,500 cryptocurrencies have a market capitalization in excess of $ 400 billion, with Bitcoin accounting for more than $ 150 billion.

In closing, financial institutions have realized the potential of Blockchain Technology comparing to the existing infrastructure and legacy systems. Blockchain will resolve a lot of problems for the financial industry and boost their business performance dramatically such as Trade Finance, Smart Assets, Payments, and Smart Contracts (Tapscott & Tapscott 2016).

4. Blockchain Technology and Real Time Accounting

Digitalization of the accounting system is still in its infancy compared to other industries, some of which have been massively disrupted by the advances of the Blockchain Technology. Using Blockchain will improve audit efficiency as auditors will increase the potential of accounting profession by reducing the cost of maintaining, providing highly secured environment and reconciling ledgers, Swan (2015). Blockchain will ensure traceable audit trails, automated accounting and reconciliations, tracking of ownership of assets and authenticating transactions.

Specifically, Blockchain Technology can assist accounting by writing the firm's transactions directly into a joint register, creating an interlocking system of enduring accounting records. Since all entries are distributed and cryptographically sealed, changing or destroying them to conceal activity is practically impossible. This is similar to transactions that are being verified by a notary, since all entries are distributed electronically and cryptographically stamp.

Moreover, using Blockchain technology all accounting data could be recorded permanently with a time stamp, preventing it from being altered. The firm's entire joint register would then be visible to customers, suppliers, shareholder, bank creditors, or any other interested party Swan (2015). Thus, accounting transactions, balance sheet or income statements could be available at any time, and would no longer need for someone to rely on company's quarterly financial statements, increasing business performance in the organization.

Concerning security issues, all accounting transactions will be digitally timestamped with a cryptographic hash code, which is a unique 64-digit alphanumeric signature that is recorded to every single transaction. Hash code will make the transaction immutable and transparent while establishing grater security. Therefore, blockchain will ensure greater data security and authenticity of recording to a degree that not even the system administrator would be able to alter the data written to a Blockchain (Fanning & Centers 2016). Thus, Blockchain Technology has the potential to reshape the nature of today's accounting and auditing.

5. Blockchain Technology and Business Process Management

The traditional Business Process Management (BPM) is concerned with the design, execution, monitoring, and improvement of business processes. Business processes are the series of events executed by an organization to deliver a product or a service to customers (Dumas, et. al., 2013). Thus, BPM assists organizations in improving existing business processes, business rules, overall efficiency and management.

Business processes consist of two categories, intra and inter-organizational processes. Intra-organizational processes are those processes within an organization, whereas inter-organizational processes are those processes that go beyond the boundaries of an organization (Dumas, et. al., 2013). However, business processes such as interoperability, flexibility to adapt to changes, lack of trust and security are not fully addressed in inter-organizational collaborations between mutually untrusted parties (Pourmirza, et. al., 2017).

Blockchain Technology has the potential to provide a suitable platform to execute inter-organizational processes in a trustworthy manner. (Hull, R., 2017). Similar, Milani (2016) stated that Blockchain technology has the potential to significantly transform business processes. The difference, however, is that traditional BMP services tend to handle internal workflows within a single organization only. In contrast, Blockchain technology allows the creation of a peer-to-peer BPM system

that has no central authority Weber (2016), provides a tamper-proof mechanism for decentralized execution of collaborative business processes and allows multiple corporations to exchange information directly with counterparties while guaranteeing the integrity of the process (Porru, et. al., 2017). This is crucial when dealing with regulated transactions that require specific guideline compliance.

Moreover, (Weber et. al., 2016) proposed that inter-organizational processes through Blockchain Technology and Smart Contracts can code guidelines and allow organizations to verify and enforce specific steps, ensuring the joint process performed correctly, by any counterparty on the network without any mutual trust between nodes. Additionally, Blockchain Technology allows participants and counterparties to maintain control of their own data, even though counterparties have enforced rules upon them by the network (Porru, et. al., 2017).

Concluding, it seems that Blockchain Technology with Smart Contracts have the potential to significantly change the environment in which interorganizational processes are able to operate. Blockchains Technology offers a way to execute processes in a trust manner, even in a network without any mutual trust among the counterparty. In addition, combining both BPM and Blockchain Technology can assist an organization in reaching the next level of integration and automation of business processes.

v. Challenges and Barriers of Blockchain Technology

In spite of the numerous potential benefits and application areas of Blockchain Technologies such as in e-Government, Accounting, Finance BPM and several others, the literature presents various challenges and barriers that need to be addressed. The following table 1 summarizes the main advantages and disadvantages of Blockchain Technology.

Table 1: summarizes the main advantages and disadvantages of Blockchain Technology.

Advantages of Blockchain Technology		
1.	*Data integrity and Immutability:* Participants can reduce fraud while strengthening regulatory compliance. Once a record has been stored in the ledger, it can only be deleted after a consensus.	(Swan 2015; Fanning & Centers 2016).
2.	*Security:* All transactions will be digitally timestamped with a cryptographic hash code, a unique 64-digit alpha-numeric signature is recorded corresponding to every single transaction.	Swan (2015).
3.	*High availability and Accessibility:* Due to decentralized networks, Blockchain Technology data would be complete, timely and accurate.	(Bahga & Madisetti, 2016; Bahga & Madisetti 2014).
4.	*Reliability:* Blockchain Technology it is not regulated by a single control center and there's no single point of failure.	(Glaser & Bezzenberger 2015; Tapscott & Tapscott 2016).

5.	Decentralization: Blockchain is a decentralized technology peer-to-peer transaction, removing the need for a third-party to intermediate, avoiding all the additional overhead cost and transaction fees.	(Christidis & Devetsikiotis, 2016; Porru et. al., 2017).
6.	*Transparency and Consensus:* All transactions conducted on the Blockchain Technology are transparent by any counterparty and allow for subsequent audits anytime. The shared ledger includes the details of the original source, destination, time and the date of the transactions.	(Christidis Devetsikiotis 2016).
7.	*Automation:* Blockchain Technology uses Smart Contracts which are self-executed code commands that can be stored and executed on Blockchain.	(Christidis & Devetsikiotis, 2016; Porru et. al., 2017).
8.	*Processing Time:* Using Blockchain technology one can reduce time for processing transactions or records, approximately from 3 days to minutes or seconds.	(Data flair team 2018).
	Disadvantages of Blockchain Technology	
1.	*Cost issues:* Blockchain Technology has initial costs and the use is not free of cost which is a drawback of decentralization. The users have to pay for the transactions and computational power.	(Beck et. al., 2016; (Marsal -Llacuna & Luïsa 2017; Angraal et al., 2017).
2.	*Data malleability issues:* Data malleability is a potential issue in the Blockchain implementation. The signatures do not provide guarantee of the ownership. An attacker can modify and rebroadcasts a transaction which can cause problems in transaction confirmation.	(Decker & Wattenhofer 2014; Yli-Huumo et. al., 2016; Hou 2017).
3.	*Latency issues:* Time factor is one of the most critical issues in Blockchain implementations, since it is not appropriate for massive transactions, due to complex verification process	(Beck et. al., 2016; YliHuumo et al., 2016).
4.	*Wasted Resources:* Requires large amounts of energy. The energy spend of mining in the Bitcoin network is approximately $15 million per day	Swan (2015).
5.	*Integration concerns:* Blockchain Technology offer solutions that require significant changes of existing legacy systems in order to incorporate.	(Yli-Huumo et al., 2016).
6.	*Immaturity of the Technology:* Blockchain is a new technology, represents a complete shift to a decentralized network and might lead to organizational transformation, including changes in strategy, structure, process, and culture.	(Aru 2017; Ølnes et al. 2017).

According to Yli-Huumo et al. (2016), the challenges and barriers are related to the technological aspects of Blockchain Technology, such as usability, interoperability, security, computational efficiency and storage size. Many studies (Ahram et al., 2017; Angraal et al., 2017; Decker & Wattenhofer, 2014; Yli-Huumo et al., 2016), questioned

the cyber security issues and threats. Hou (2017) stated that the blind trust on the part of Blockchain developers, security and performance are serious issues and drawbacks of Blockchain Technology. Moreover, Blockchain Technology is not bounded by any international rules and regulations. Also, with the increasing need for interoperability among large industries like banks, the technology needs to be compatible with different legacy systems (Yli-Huumo et al., 2016). The interconnection with the existing systems is a big challenge today as the current legacy systems and processes cannot be entirely eliminated and require significant changes of existing legacy systems in order to incorporate (Yli-Huumo et al., 2016).

Additionally, Blockchain Technology is not appropriate for massive transactions, due to complex verification process, (Beck et. al., 2016). In Blockchain Technology, in order to provide security, all transactions will have to be digitally time-stamped with a cryptographic hash code, a unique 64-digit alpha-numeric signature to record each single transaction, which consumes a lot of computing power and time.

Furthermore, some scholars recommend that the benefits of Blockchain adoption into public or private services must be identified carefully since the cost might be higher than the benefits for developing, running and maintaining the Blockchain Technology, (Marsal-Llacuna & Luïsa 2017; Angraal et al., 2017). However, the immaturity of the technology itself is at the base of all existing technological challenges in adopting Blockchain Technology. This can be understood as something that is common in all new technology introductions.

In closing, Blockchain adoption might lead to organizational transformation, including changes in strategy, structure, process, and culture. This transformation requires organizational members' cooperation and commitment in order to enable the organization to survive and to improve the level of performance and effectiveness.

VI. Conclusion and Recommendations

From a theoretical perspective, based on the literature review, Blockchain Technology has high value and good prospects in resolving problems of data integrity, improving transparency, enhance security, preventing fraud, and establish trust and privacy. Blockchain Technology can bring revolution in the areas of Finance, Accounting, e-Government, BPM, insurance, entertainment, trading platforms, healthcare, internet-of-things, as well as law firms and others. Hence, Blockchain Technology has a huge potential in introducing innovative solutions, depending on the area or the sector of its implementation, since economic efficiency and social benefits can be achieved through technical innovation and applications.

However, implementing Blockchain Technology at organizations in different industries, could prove to be very costly. Migrating or moving legacy systems require a significant amount of investment from organizations. Adopting the Blockchain Technology, at this early stage, organizations will have to deploy a unified platform to support such hybrid application architecture, incorporating Blockchain and legacy systems. Thus, they need to deepen their understanding of Blockchain Technology, its value, its opportunities, and its risks. As a result, there are only a small number of instances in which the technology has been applied with these systems.

Therefore, Blockchain Technology may not replace legacy systems or old applications soon. However, Blockchain can certainly be a complementary application to legacy systems and may even lead to the development of new systems in the near future.

In conclusion, more intensive research in this area of Blockchain Technology is necessary to advance the maturity of this field, since it is still in the exploratory stage and there are many legal and technical issues to be resolved. Therefore, this review offers a useful starting point for future research themes for the development of Blockchain application, and assist practitioners and researchers.

References

Ahram, T. et al., (2017). Blockchain technology innovations. 2017 IEEE Technology & Engineering Management Conference (TEMSCON) (Jun. 2017), 137–141.

Angraal, S. et al., (2017). Blockchain Technology: Applications in Health Care. Circulation. Cardiovascular quality and outcomes. 10, 9 (Sep. 2017), e003800. DOI:https://doi.org/10.1161/CIRCOUTCOMES.117.003800.

Aru I., (2017). Full Stack Development Tools Lowering Blockchain Entry... News Cointelegraph. Available at:https://cointelegraph.com/news/fullstack-development-tools-lowering-blockchain-entry-barriers.

Bahga, A., Madisetti, V., (2016). Blockchain Platform for Industrial Internet of Things, Journal of Software Engineering and Applications, No. 9, pp. 533-546.

Bahga, A., Madisetti, V., (2014). Internet of Things: A Hands-On Approach, Atlanta.

Barnes A., Brake C., & Perry T., (2016). *Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers - Plymouth University*.

Beck R., Stenum Czepluch, J., Nikolaj Lollike, N., & Malone, S., (2016). Blockchain-the Gateway to Trust-Free Cryptographic Transactions. In ECIS. Research Paper 153.

Bogart S. & Rice K., (2015). The Blockchain Report: Welcome to the Internet of Value, http://www.the-blockchain.com/docs/The%20Blockchain%20Report%20%Needham%20(huge%20report).pdf.

Broby, D., & Paul, G., (2017). Blockchain and its use in financial settlements and transactions. The Journal of the Chartered Institute for Securities and Investment (Review of Financial Markets), 53-55.

Buterin V., (2015). On Public and Private Blockchains. Ethereum Blog., https://blog.ethereum.org/2015/08/07/on-publicand-private-blockchains/. Accessed 28 Nov 2016.

Chen F., Deng P., Wan J., Zhang D., Vasilakos A. V., & Rong X., (2015). Data mining for the internet of things: Literature review and challenges, International Journal of Distributed Sensor Networks, 11 431047.

Christidis, K. & Devetsikiotis, M., (2016). Blockchains and Smart Contracts for the Internet of Things, IEEE Access, 4, 2016, pp. 2292–2303. Dataflair team, (2018). Advantages and disadvantages of Blockchain Technology (online). Available from: https://dataflair.training/blogs/advantagesand-disadvantages-of-blockchain/

Dorri A., Kanhere S. S., & Jurdak R., (2017). Blockchain in internet of things: challenges and solutions, arXiv preprint, arXiv:1608.05187.

Düdder, B. and Ross, O., (2017). Timber tracking: Reducing complexity of due diligence by using blockchain technology (position paper). CEUR Workshop Proceedings (2017).

Dumas, M., La Rosa, M., Mendling, J., Reijers, H., (2018). Fundamentals of Business Process Management. Springer Berlin, Berlin.

Fanning, K. & D.P., Centers, (2016). Blockchain and Its Coming Impact on Financial Services", Journal of Corporate Accounting & Finance, 27(5), pp. 53–57.

Forrest P., (2016). Blockchain and non-financial services use cases.Linkedin.https://www.linkedin.com/pulse/blockchain-non-financialservices-use-cases-paul-forrest.

Gates M., (2017). Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. Create Space Independent Publishing Platform, 2017.

Glaser, F. & Bezzenberger, L., (2015). Beyond Cryptocurrencies—A Taxonomy of Decentralized Consensus Systems. 23rd European Conference on Information Systems, Munster, 1-18.

Iansiti, M., & Lakhani, K. R., (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.

Marsal-Llacuna & Maria-Lluïsa (2017). Future living framework: Is blockchain the next enabling network? Technological Forecasting and Social Change. December (Dec. 2017), 0–1.

DOI:https://doi.org/10.1016/j.techfore.2017.12.005.

Mettler M., (2016). Blockchain technology in healthcare: the revolution starts here.IEEE 18th International Conference on e-Health Networking, September 14–16. Piscataway, NJ: IEEE.

Milani, F.P., L. García-Bañuelos, and Dumas M., (2016). Blockchain and Business Process Improvement.

M. O' Dair & Beaven Z., (2017). The Networked Record Industry: How Blockchain Technology Could Transform the Record Industry. Strategic Chamnge 26, no. 5, 472-480.

Morrison A., (2016). Blockchain and smart contract automation: How smart contracts automate digital business. http://www.pwc.com/us/en/technology-forecast/blockchain/digitalbusiness.html

He D, Habermeier K, Leckow R, Haksar V, Almeida Y, Kashima M, Kyriakos-Saad N, Oura H, Sedik TS, Stetsenko N, and Verdugo-Yepes C., (2016). Virtual Currencies and Beyond: Initial Considerations (No. 16/3). International Monetary Fund. Washington, D.C., U.S.A.

Hou, H., (2017). The application of blockchain technology in Egovernment in China. 2017 26th International Conference on Computer Communications and Networks, ICCCN 2017, 1–4.

Hull, R., (2017). Blockchain: Distributed event-based processing in a data-centric world. Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems, DEBS 2017, Barcelona, Spain, June 1923.

Ølnes, S. et al. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. Government Information Quarterly. 34, 3 (Oct. 2017), 355–364.

Joichi I., Neha N., & Robleh A., (2017). The Blockchain Will Do to the Financial System What the Internet Did to Media. Harvard Business Review. Nakamoto S., (2008). Bitcoin: A peer-to-peer electronic cash system.

Porru, S., Pinna, A., Marchesi, M., & Tonelli, R., (2017). BlockchainOriented Software Engineering: Challenges and New Directions", 39th International Conference on Software Engineering Companion, pp. 169–171.

Pourmirza, S., Peters, S., Dijkman, R., Grefen, P., (2017). A systematic literature review on the architecture of business process management systems. Information Systems 66, 43-58.

Savelyev S. (2017). Contract law 2.0:'Smart'contracts as the beginning of the end of classic contract law. Information & Communications Technology Law.

Schatsky D. and Muraskin C., (2015). Beyond Bitcoin. Blockchain is coming to disrupt your industry. Deloitte University Press.

Swan M., (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc, Sebastopol, CA, U.S.A.

Tapscott, D., & Tapscott, A., (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World. *New York, NY: Penguin Random House*.

Tapscott D, Tapscott A., (2016). The impact of the blockchain goes beyond financial services.Harvard Business Review.

Understanding the basics of blockchain in government | Deloitte Insights (2017),https://www2.deloitte.com/insights/us/en/industry/publicsector/understandingbasics-of-blockchain-in-government.html. Accessed: 2018-01-09.

Walport M., (2016). Distributed Ledger Technology: Beyond Blockchain. UK

Government Office for Science, Tech. Rep, pp. 19.

Weber, I., X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, (2016). Untrusted Business Process Monitoring and Execution Using Blockchain. Springer, Cham, 9850.

Yli-Huumo, J. et al., (2016). Where is current research on Blockchain technology? A systematic review. PLoS ONE. 11, 10 (Oct. 2016), e0163477. DOI:https://doi.org/10.1371/journal.pone.0163477.