IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 6, 2019, accepted November 25, 2019, date of publication December 4, 2019, date of current version December 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2957660

A Comparative Analysis of Blockchain Architecture and Its Applications: Problems and Recommendations

TOQEER ALI SYED[1], ALI ALZAHRANI[1], SALMAN JAN[2], MUHAMMAD SHOAIB SIDDIQUI[1], (Member, IEEE), ADNAN NADEEM[1], AND TURKI ALGHAMDI[1]

[1]Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah 42351, Saudi Arabia
[2]Universiti of Kuala Lumpur, Kuala Lumpur 50250, Malaysia

Corresponding author: Toqeer Ali Syed (toqeer@iu.edu.sa)

This work was supported by the Deanship of Research, Islamic University of Madinah, KSA, under the tamayyuz initiative Grant 25/ 40.

ABSTRACT In the past few years, the implementation of blockchain technology for various applications has been widely discussed in the research community and the industry. There are sufficient number of articles that discuss the possibility of applying blockchain technology in various areas, such as, healthcare, IoT, and business. However, in this article, we present a comparative analysis of core blockchain architecture, its fundamental concepts, and its applications in three major areas: the Internet-of-Things (IoT), healthcare, business and vehicular industry. For each area, we discuss in detail, challenges and solutions that have been proposed from the research community and industry. This research studies also presented the complete ecosystem of blockchain of all the papers we reviewed and summarized. Moreover, analysis is performed of various blockchain platforms, their consensus models, and applications. Finally, we discuss key aspects that are required for the widespread future adoption of blockchain technology in these major areas.

INDEX TERMS Blockchain, IoT blockchain, healthcare blockchain, permissioned blockchain, business blockchain.

I. INTRODUCTION

Decentralized architecture has received ample acceptance in the past few years because of its need in many fields [1]–[3]. It is also of utility for Internet-ofThings (IoT) to solve their open problems, such as, security. Blockchain was initially introduced through a cryptocurrency, known as bitcoin [4]. It is a peer-to-peer network that is available to everyone, without the users having to provide personal details for authorization. Anyone can be a component of blockchain and perform a transaction. The security and trust aspect is solved through a consensus, along with a public ledger. Proof-of-work (PoW) is the consensus algorithm that is utilized by public blockchains, such as, Bitcoin and Ethereum [5]. All of the transactions are validated through special nodes, called 'miners' [6]. Similarly, each transaction is executed through a public/private key pair that is distributed among the participants. The public ledger is an immutable chain-of-transactions, on which if any record is tempered then the rest of the peer nodes would invalidate the transaction.

Blockchain has the potential to be adopted by the financial organizations, banks, and government organizations for various applications, for example, in e-voting. One of the surveys that was conducted by the International Business Machines Corporation (IBM), with approximately 200 financial institutions, revealed that 91 percent of banks and 66 percent of financial institutions would have fully implemented blockchain technology by 2018 [7]. A reputable research and business consultant institute, Gartner, reported that there is $3.1 trillion worth of investments to be expected in blockchain technology in 2030 (cf. Figure 1). Because of this significant scale of adoption of blockchain technology by the industry, a high volume of research has been carried out in this domain.

The core research of blockchain technology is on the basis of efficient, secure, and scalable consensus algorithms. Public blockchain algorithms are scalable; however, permissioned blockchain algorithms are efficient and secure, but not

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

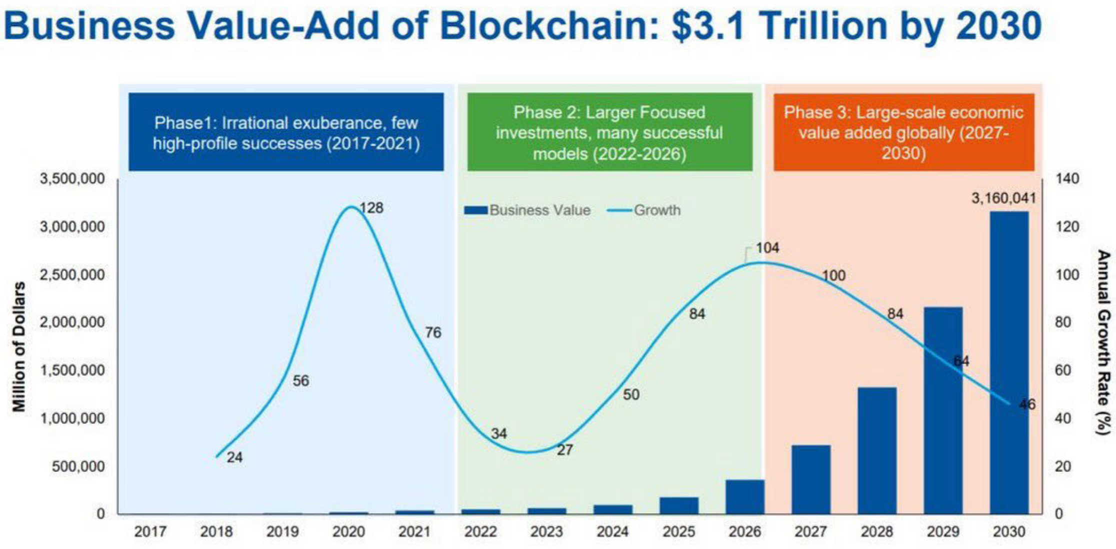


FIGURE 1. Blockchain investment growth rate.

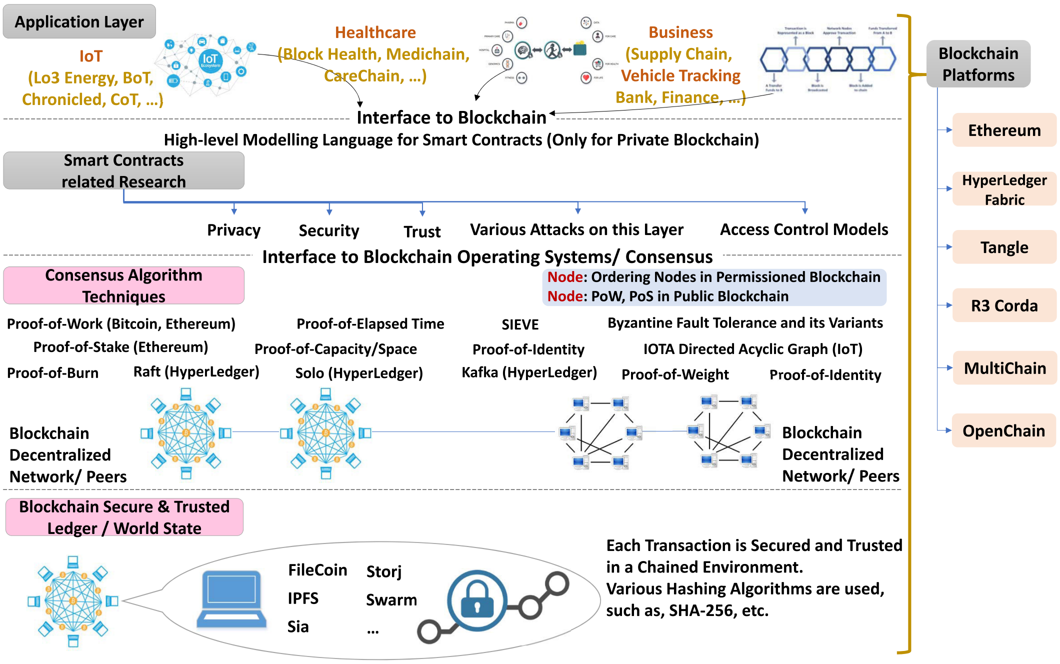

Application Layer
IoT
(Lo3 Energy, BoT, Chronicled, CoT, ...)
Healthcare
(Block Health, Medichain, CareChain, ...)
Business
(Supply Chain, Vehicle Tracking Bank, Finance, ...)
Interface to Blockchain
High-level Modelling Language for Smart Contracts (Only for Private Blockchain)
Smart Contracts related Research
Privacy
Security
Trust
Various Attacks on this Layer
Access Control Models
Interface to Blockchain Operating Systems/ Consensus
Consensus Algorithm Techniques
Node: Ordering Nodes in Permissioned Blockchain
Node: PoW, PoS in Public Blockchain
Proof-of-Work (Bitcoin, Ethereum)
Proof-of-Elapsed Time
SIEVE
Byzantine Fault Tolerance and its Variants
Proof-of-Stake (Ethereum)
Proof-of-Capacity/Space
Proof-of-Identity
IOTA Directed Acyclic Graph (IoT)
Proof-of-Burn
Raft (HyperLedger)
Solo (HyperLedger)
Kafka (HyperLedger)
Proof-of-Weight
Proof-of-Identity
Blockchain Decentralized Network/ Peers
Blockchain Decentralized Network/ Peers
Blockchain Secure & Trusted Ledger / World State
FileCoin
Storj
IPFS
Swarm
Sia
...
Each Transaction is Secured and Trusted in a Chained Environment.
Various Hashing Algorithms are used, such as, SHA-256, etc.
Blockchain Platforms
Ethereum
HyperLedger Fabric
Tangle
R3 Corda
MultiChain
OpenChain

FIGURE 2. The summarized review of blockchain ecosystem.

sufficiently scalable [8]. Some light-weight public consensus algorithms have been introduced, including the Directed Acyclic Graph(DAG) for IoT platforms [9]. The new consensus model assists in the removal of a transaction fee in existing cryptocurrency models.

Blockchain technology is adopted by the IoT for its crucial problems of security, privacy, and provenance tracking [10], [11]. Some IoT platforms employ blockchain as a trusted database. There are architectures that have been adopted to perform each transaction through the blockchain network. Similarly, there exists a utility for combinations of a cloud, the IoT, and blockchain [10]. There are a number of platforms that are specifically designed for the IoT to function in a decentralized manner. A complete review of latest IoT researches that are based on blockchain are thoroughly reviewed in Section III. However, in conclusion, the researchers have summarized an *ecosystem* of the research being done so far (as shown in Figure 2). IoT is covered in application layer of the ecosystem and as a platform.

There are a number of open problems in healthcare that have also been solved through blockchains. For example, the secure exchange of healthcare information among

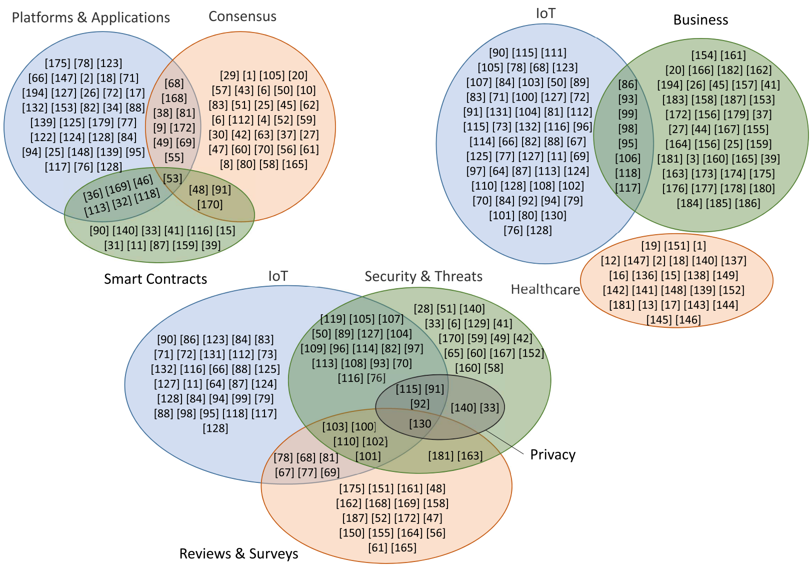


FIGURE 3. Analysis of the past research related to platforms, consensus models, applications-IoT, healthcare, and business, and various threats.

stakeholders, ensuring privacy [12], integrity [13], and the insurance of healthcare records have been discussed in detail [14]. Similarly, reducing the cost of healthcare transactions, as well as, limited access to health records introduces efficiency into the field through blockchains [15]. A number of available platforms for healthcare are also a part of the discussion in the healthcare industry [16]–[18]. A complete review of latest healthcare record sharing and related work is thoroughly reviewed in Section IV which is shown in application layer of the ecosystem Figure 2.

The current digital economy and businesses are built on the basis of trusted authorities. Thus, in cases of carrying out transactions, the authorities are consulted regarding the authenticity of the receiving party. The problem with third parties is that they can also be compromised, manipulated, hacked, or misused, which may ultimately incur wrongdoing [19]. A blockchain provides consensus mechanisms [20], [21] through which the aforementioned problem can be addressed, without compromising the privacy of other entities, including digital assets and parties. All transactional details can be verified at any stage. A blockchain has the ability to serve as an engine of growth in today's digital infrastructure, where businesses and commerce industries are web-based.

A. COMPARISON AND GAP ANALYSIS

There are a number of reviews related to blockchain in last 5 years. In figure 3, the authors compare the literature that was reviewed in this article, through a series of Venn diagrams. Blockchain literature was analyzed and divided into multiple categories, such as, consensus techniques, smart contracts, the IoT, healthcare, business, and various platforms that are related to blockchain. It also shows the intersection between different areas, in the top-left Venn diagram, where the authors summarize the articles that are related to platform and applications, consensus smart contracts and the research that is common between them. Similarly, in the top-right Venn diagram, the review papers that are related to the IoT, business, and healthcare are summarized. There are a few papers that cover both IoT and business applications. The Venn diagram in Figure 3 also summarizes security, threats, and privacy in IoT.

Based on our comparison, we can safely say that most of the review papers until now have focus on investigating blockchain technology for a specific applications area, as illustrated by the Venn diagrams in figure 3. However, there are few recent papers which focus on multiple application areas. For example, in [22], authors have briefly reviewed the blockchain's potential benefits in various businesses, supply chain management, accounting settlement, and smart trading. Similarly, in [23], authors have reviewed the requirements for blockchain implementation in various industries including financial [24],healthcare, logistics, manufacturing, energy, and robotics industries. In this article, we present a thorough literature review of existing blockchain application in the broad areas of IoT, Business, and Healthcare with their challenges and future opportunities. We also review the existing blockchain core architectures in detail. So in summary, this article provides the reader an insight of core architectures and three broad application areas of blockchain technology in a single draft.

A contribution of this article is that the authors provide a complete review of four areas of blockchain, including blockchain core research, the IoT, healthcare, and blockchain for business. In the literature, we found only a few *review* papers that target specific areas, instead of a complete overview of blockchain-related research. Secondly, our review covers the most updated articles and platforms in the

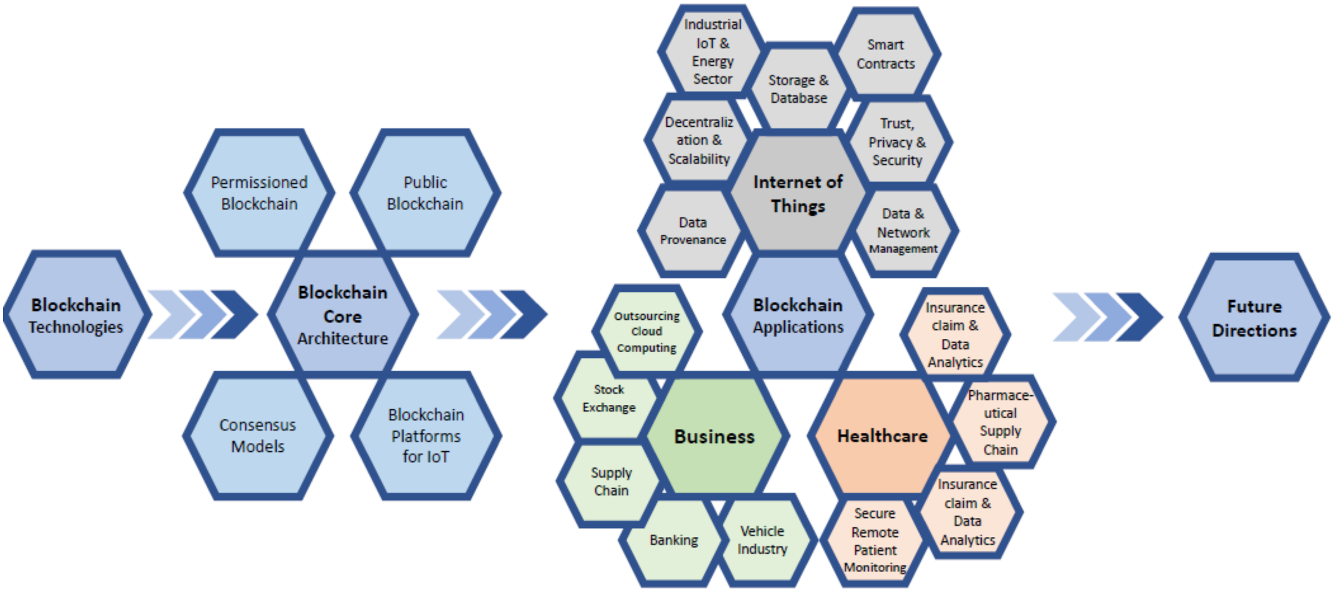

Blockchain Technologies
Permissioned Blockchain
Public Blockchain
Blockchain Core Architecture
Consensus Models
Blockchain Platforms for IoT
Industrial IoT & Energy Sector
Storage & Database
Smart Contracts
Decentralization & Scalability
Internet of Things
Trust, Privacy & Security
Data Provenance
Data & Network Management
Outsourcing Cloud Computing
Blockchain Applications
Insurance claim & Data Analytics
Stock Exchange
Business
Healthcare
Pharmaceutical Supply Chain
Supply Chain
Banking
Vehicle Industry
Secure Remote Patient Monitoring
Insurance claim & Data Analytics
Future Directions

FIGURE 4. A comparative review of blockchain architecture and its applications including IoT – healthcare and business.

aforementioned areas. A large part of the review includes the research that has been completed in the last three years in the specified four areas. In section II, the researchers thoroughly discuss the core blockchain research. That includes the type of blockchain platforms and various consensus algorithms, as well as, their merits and demerits, in order to assist in the correct choice for each application.

Similarly, we thoroughly discuss the existing problems of the IoT and solutions available through blockchain. Healthcare- and business-related research that was conducted in the last few years regarding blockchain is discussed extensively. In short, this article is a comprehensive review of blockchain core architecture and its applications in various fields, which we perceive to be the strength of this article.

B. ARTICLE STRUCTURE AND TAXONOMY

In Figure 4, we have presented the taxonomy of Blockchain architecture and its applications according to our article. The article focuses on the existing literature review of the core blockchain architecture and its application areas, specifically, in Internet-of-Things (IoT), Healthcare, and Business. In Figure 4, the top circle presents the core architecture of blockchain; while the other three circles represents the applications areas. In section II, the core concept of blockchain architecture and various platforms that can benefit from utilizing blockchain are discussed. The section discusses the four aspects of the core architecture, as shown in the figure. The section III lists complete research regarding the blockchain based IoT applications areas, their challenges and various consumer applications. Similarly, IV and V thoroughly discuss the adoption of blockchain in the healthcare and business sectors, respectively. In the busines section, the author also present blockchain potential in vehicular industry. The final section summarizes complete findings and its future prospects.

II. BLOCKCHAIN CORE ARCHITECTURES

There are a number of characteristics required to stakeholders in a corporate organization for survival of the service providers. First and most demanding property is to ensure data integrity i.e. to make sure no transactions are performed, updated or altered without the consensus mechanism within a network. This is generally ensured within an organization through implementation of cryptographic mechanisms. Similarly, organizations need to provide fair chance to all peers to make and update valid transactions, which is also termed as equal rights. Another demanded feature is establishment of trust which can be better obtained through consensus. Consensus actually governs addition of new items; it consists of the rules for validating and broadcasting transactions and blocks, and resolving conflicts.

A. CENTRALIZED SYSTEMS

In centralized systems, users rely on authority to carry on transactions. Like, in banks the customers rely on banking system which adjust customer's account balances after making transactions. In centralized system, the central authority can alter entire system by directly altering and updating databases at the back-end. Centralized services do not allow distribution of authority and thus are single services provider [25]. Online payment, cloud systems, governments, and courts are various examples of centralized system [26], [27]. Employing these systems have deep impact on leveraging the fundamental properties of a good system including integrity, transparency, public access, and trust. The centralized system is also a single point of failure which means that if the service provider crashes, it affects the whole system and the stakeholders are ultimately affected.

B. NEED FOR DECENTRALIZED SYSTEMS

The basic idea behind the use of decentralized systems is to provide fault-tolerant distributed computing system where the authority could be distributed without having trust on central system. This ensures a number of other properties including trust, transparency, data integrity, etc. To provide publicly accessible infrastructure and achieve interoperability, the need for blockchain is imminent. It enables building of decentralized applications and distributed software infrastructures for a large number of untrusted participants. The problem with the centralized system is that it is prone to single point failure and the system does not provide transparency, fair access to resources, integrity, non-repudiation of transactions performed, and data immutability. Famous examples of decentralized systems are implementation of bitcoin and ethereum [28], [29]. Other decentralized systems could be studied through the literature [25], [30], [31].

C. BLOCKCHAIN: IS THE WAY TO GO

Blockchain refers to a distributed system, data structure, or network of blocks that are ordered in the form of a list [32]–[35]. Blockchains have two common types; one is public blockchain and the second one is permissioned blockchain. The former is publicly available where any participant can join and carryout transactions or become part of consensus process to update blockchains; thus the number of participants can be over thousands. This kind of blockchain is more prone to attacks. Famous attack includes Sybil attack, as the participants are anonymous and can have several identities to influence the consensus process [36], [37]. On the other hand, the permissioned blockchain are close ended, example includes Multichain and Hyperlegder Fabric, Parity, BigChainDB, InterPlanetary, Corda and Quorum [38], [39]. The blocks contains transactions as carried out by various peers within networks. The blocks within blockchain are connected back to previous blocks through a chain, which is indeed a hash representation of transactions made up till previous block. The chain ensures integrity of transactions, thus all transactions made in the past are not manipulated and attempts to temper with any of these or making a transaction without Proof-of-Work (PoW) results in invalidating the chain of hashes. Thus, transparency and trusts are established in the blockchains that are essential components that compels a number of organizations to implement blockchain in their respective infrastructure.

Bitcoin is considered as first generation implementation of blockchain employed public ledger in order to keep cryptographically signed financial transactions [40]. Similarly, the smart contract [41], the second generation implementation of blockchain provided general purpose programmable platform with public ledger to keep record of all computational results. Smart contracts implements business logic and conditions [3] in order to perform programmable transactions which makes it different from rest of other techniques. Escrow [42] is one of the systems that implements smart contracts in order to keep funds until certain defined obligations, as provided in the smart contract, are met. Similarly, another example of blockchain implementation that employs smart contract is Ethereum [28].

In blockchain network, the initiator signs transactions in order to ensure expenditure of funds, or to create and execute smart contracts. The newly initiated transactions are propagated to the blockchain nodes which upon validation propagates the transaction to other nodes until the transactional details are shared and validated by all peers of the network. Finding a unique hash(cryptographic value) for the transaction to become part of the blockchain network is termed as mining in bitcoin context. Blockchain relies on miners for appending transactions that are valid after reaching consensus on the whole network level. The consensus mechanism to be adopted for this purpose may include Proof-of-Stake [43].

D. PUBLIC BLOCKCHAIN AS ORDER-EXECUTE ARCHITECTURE

In 2009, a new concept of **blockchain** was introduced by anonymous researcher. A white paper regarding ***Bitcoin***, that is subsequently published in news, provides the author name as *Satoshi Nakamoto* [44]. The basic intention behind this new revolution was to bring a digital currency called **Bitcoin** into the world that does not need any central controlling authority. Using cryptography techniques and some shared consensus algorithms, such as, PoW, *Bitcoin* developed a trust paradigm between untrusted participant around the world. Blockchain can be viewed as a distributed digital ledger containing blockchain information, with each block identified by a cryptographic signature. These blocks are all backlinked by referring to the signature of the previous block in the chain, and the chain can be traced up to the first block.

1) BITCOIN ISSUES

Public blockchain are criticized related to privacy and scalability as there are no privileged users, rather any participant can join network, have access to information as available on blockchain, and also validate new transactions. Similarly, blockchain has scalability limits with reference to size of data and processing rate of transaction. It do suffer from latency of data transmission. Privacy and security issues are major concerns in blockchains [45] as the information is made available to all peers of the network.

The transactions in bitcoin are processed based on predefine consensus rules, thereafter the specific functionality are permitted to process transactions. Presently there are over ten thousand active nodes in Bitcoin. The bitcoin is based on a trustless environment which enables participants to perform monetary transactions e.g. transfer of money, without involving a third party which may include a bank or any payment service. Bitcoin basically a public blockchain and work on the concept of Proof-of-Work which altimately provide trust and security to their users [46]. PoW will be discussed in section II-G. The transactions executed over Bitcoin are *order-execute-architecture*, that means the transactions are given first to the minors to verify and find a specific hashing number. After this preliminary process the transaction is executed. Finding the hash and verify the transaction by all network nodes takes long time to finally commits it. Due to this long execution time various general purpose applications are moving from public blockchain to permissioned blockchain.

2) ETHEREUM

Ethereum was proposed in late 2013 by Vitalik Buterin, a programmer and cryptocurrency researcher, as an open-source, public blockchain-based distributed computing platform and operating system featuring smart contract (scripting) functionality [47]. Ethereum supports an advanced version of Nakamoto-consensus mechanism which works basically on ''Memory Hardness'' instead of fast processing power machines. With Bitcoin PoW large organization and substantial mining pools can influence the network. However, with ehtereum's reliance on fast memory data movements this problem is reduced. The Ethereum Virtual Machine (EVM) is provided by Ethereum which is a decentralized virtual-machine for executing smart contract code on ethereum nodes. Ethereum network is permissionless i.e. any node can join ethereum network if user downloads ethereum client to create account. Moreover, it uses its own consensus model known as EthHash PoW. It is capable of executing scripts using an international network of public nodes. Gas is a transaction pricing-based mechanism to mitigate spam and allocate resources on the network. Minors on the network defines the price of the gas and if a transaction is less the defined gas it will be declined. The system went live on 30 July 2015, with 11.9 million coins ''premined'' for the crowdsale [48].

As such, the blockchain contains an un-editable record of all the transactions made. However, blockchain functionality is not limited to cryptocurrency, rather it can also be adopted to any distributed business environment. For example, due to its transparency and auditability features **Sierra Leone** a west African country conducted world first E-voting system using blockchain technology. Bitcoin placed the building block for the new era of computing. However, Bitcoin does not fit in all scenarios as each and every sector has its own requirements [49]. To adopt blockchain technology in different sectors, general purpose blockchain models are required that should be mature enough to handle all the business logic and practices accurately. Due to this reason world renown IT, financial, and other organizations are taking interest in permissioned blockchain model. Each of them are developing their own solutions for different sectors. Some of the organizations include IBM, Intel corporation, and Wall Street.

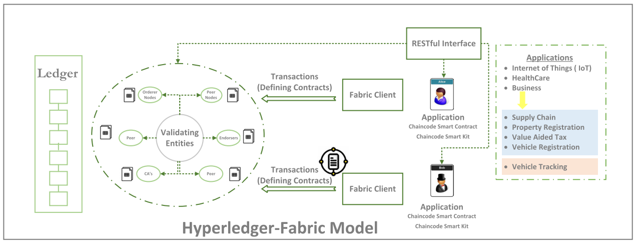


FIGURE 5. Hyperledger fabric model [52].

E. PERMISSIONED BLOCKCHAIN ARCHITECTURES AND PLATFORMS

Among many enterprise blockchain applications are being utilized in finance, health, voting systems, and protecting civil infrastructure. One of the most important aspect of using permissioned blockchain system is that it offers high availability in contrast to single point failure. All transactions recorded in the system remains in the system as all nodes download every transaction or block and it can be retrieved when required from other nodes.

A permissioned blockchain is different from permissionless due to the use of access control layer [50], [51]. It restricts users in terms of access to consensus mechanism and thus enables only the intended participants to join the network. This is in contrary to permissionless blockchains, which can be joined by any user as exemplified through ethereum, and Bitcoin. Following is the discussion of permissioned blockchain platforms.

Quorum [53] is the first blockchain/platform that adopted various consensus algorithms instead of using PoW. It is extension of ethereum and works as permissioned blockchain. It supports smart-contract with crash and BFT consensus models. There are a number of permissioned blockchain platform, however, Quorum is one of them that gains popularity because of ethereum support. Quorum extended the features in ethereum to become a solution for general purpose applications, such as, business and Healthcare.

All of the existing blockchains ranging from permissionless to permissioned blockchains are order-execute architectures which have a common issue, that is, all transactions are to be executed on all nodes which limits performance of the system and give birth to other issues including privacy of the users, concurrency, and denial of service attacks.

Hyperledger Fabric [49], also called 'Fabric', is an open source framework to implement permissioned blockchains (cf. Figure 5). It follows *execute-order-validate* paradigm (cf. Figure 6). The traditional blockchain frameworks, such as, BitCoin and Ethereum uses order-execute architecture which slowdowns the transaction processing time. Digital Asset and IBM were the two companies that built the initial version of Fabric. It however suffers from two drawbacks. First, lack of proven use cases and secondly, an inadequate number of skilled programmers able to use it [52].

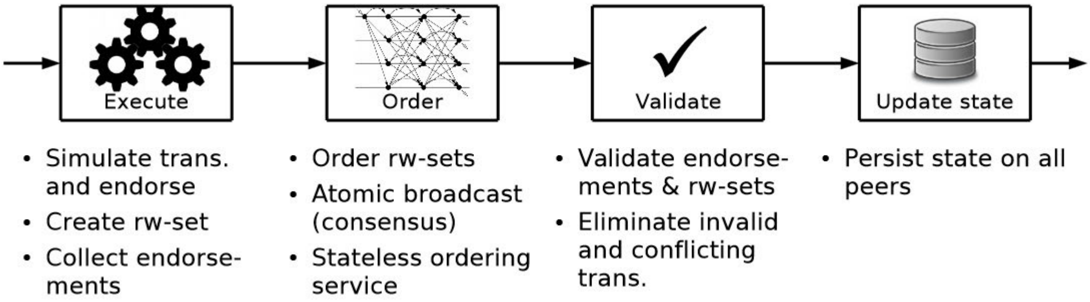

Execute
Order
Validate
Update state
• Simulate trans. and endorse
• Create rw-set
• Collect endorsements
• Order rw-sets
• Atomic broadcast (consensus)
• Stateless ordering service
• Validate endorsements & rw-sets
• Eliminate invalid and conflicting trans.
• Persist state on all peers

FIGURE 6. Execute order validate architecture [49].

Overtime, Fabric is becoming a favorable ledger architecture for general applications. It provides a smart contract interface for application development called Chaincode. Chaincode can be developed in multiple languages such a, NodeJS, Go, Java, typescript. It also provides a Restful interface for existing applications to connect with the Blockchain network. Recently, Hyperledger project provided the second layer on Fabric for rapid application development called composer. However, due to certain reasons there is no further support for composer.

Now, the applications are mostly developed, at the time of writing, in Fabric version 1.4. To develop an application on Fabric, a Blockchain network usually have to set up a user (administrator) belongs to an organization to run the Chaincode. The user creates certain security digital certificates to secure communication between network organizations and their users. Each node in the Blockchain network is developed with Docker containers which are deployed in the geographically distributed locations. The peer nodes in a network can offer one or more services, such as, a node can smart contract, Chaincode, as well as certification authority (CA) and endorsers.

Different applications can be incorporated in Chaincode that may belong to IoT, healthCare, business, etc (cf. Figure 5). The Chaincode can be executed as a smart contract while it offers connectivity with different APIs as well. The execution of a smart-contract requires few primary steps over the Blockchain network. Firstly, chaincode is executed from Chaincode Developer Kit (CDK), thereafter the smart contracts are rendered to *endorsers nodes* that actually endorses the validity of the contract and further permits the execution of the contract. After confirming the legitimacy of the owner of the contract. Thereafter the chaincode is transferring the transaction to Orderer nodes that combines it and generate the blocks as per the predefined legitimate block size. The hashes of the blocks are computed that are thereafter added to the chain through the consensus mechanism. The status of the ledger is maintained consistently in this fashion using either of the BFT, Kafka, Solo, etc. consensus algorithms that could be opted.

Problem and Recommendations: Hyperledger fabric is rapidly gaining popularity and acceptance. It is opted by most of the developers as it allows application development and ease for writing smart-contracts in a number of domains as explained in this paper. However, it offers centralization and includes membership service node that requires the identity of the member as opposed to those of Ethereum that is based on PoW and Proof-of-Stack(PoS) and are purely public blockchain.

F. BLOCKCHAIN PLATFORMS FOR IOT

There are a number of platforms that are specifically designed for IoT networks due to there specific characteristics.

1) IOT CHAIN

IoT chain is a new platform for IoT devices to work as decentralized network. IoT chain has not been open to the public for development, however, has shown its result, securities, consensus and other issues to the IoT network. It compared results with IOTA, SLOCK, IT, IBM-ADEPT and other chimes projects. As blockchain technology, it supports PBFT and DAG as consensus.

2) IOTA

IOTA is another platform that uses DAG (Directed Acyclic Graph) specifically designed for IoT. There is no concept of reward in IOTA, instead a new transaction will appear any two previous transactions into the network. Figure 7 shows a comparison of a traditional blockchain datastructure with IOTA based on DAG. IOTA, being distributed ledger technology (DLT) satiates computers in an IOTA network to transfer immutable data and value (IOTA tokens) among each others. Recently, IOTA Tangle announced integration with Hyperledger Fabric systems, that provides fluid data sharing and validation with permission systems that are siloed. IOTA Connector provides data to be mirrored into Tangle, benefiting from all the features available, including encrypted transaction payload, fee-less payments, and public/private message chains. Upon the execution of the smart-contract, a request is triggered to the IOTA Tangle to allow update and store the results of executing the smart contract and further to make payments between IOTA wallet holders.

3) WALTONCHAIN

Walton chain [54] is another platform that is specifically designed for IoT to work as decentralized network. It mainly

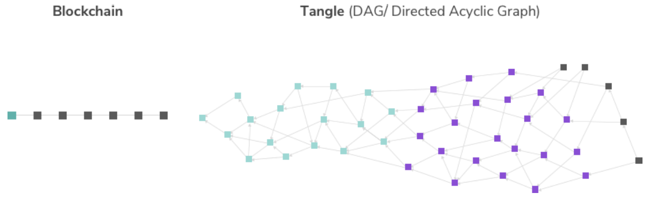


FIGURE 7. Blockchain Vs IOTA [49].

contains two parts, the hardware and the software. RFID is used as a communication medium in IoT devices while the electronic transaction is performed on newly designed blockchain architecture. Software includes the Walton chain protocol and Walton coin. Open IoT blockchain provides an open secure hardware engine to develop secure IoT devices for blockchain.

G. CONSENSUS MODELS

The consensus process allows read from and update to the shared state that ensures ordering of transactions and further guarantees integrity of contents across geographically dispersed areas in a decentralized fashion. Different blockchains have employed various consensus models which include Prove-of-Work, Proof-of-Bayzantine-Fault-Tolerance (PBFT), Proof-of-Stake (PoS), and Proof of Elapsed Time (PoET). Generally, consensus protocols are selected on the basis of three essential properties; namely, 1. Safety, 2. Liveness, and 3. Fault Tolerance. We provide a brief information about some consensus protocol in the following subsections.

1) PROOF-OF-WORK

In order to add blocks to a blockchain, some proof of work has to be communicated. Bitcoin uses PoW concept as consensus mechanism, which scales over 1000 of nodes. PoW requires the initiator to solve a puzzle, a mathematical or cryptographic operation by brute forcing and to produce a value (also called wining value), which is less than a defined one as set forth by the network. At times, more than one node produces winning value at the same time to add block and thereafter ask for reward. This situation creates a fork and is resolved by the network by analyzing the maximum value of prove-of-work i.e. maximum work done by a node. The update request by the node with minimum proof-of-work is discarded. This way the consistency of state among all nodes is ensured. PoW fits best for those networks that requires scalability. Mostly permissionless blockchains utilize PoW as they have authenticity of the participating node, as a result the network size becomes very large. It suffers from few drawbacks, it requires every node to invest huge amount in purchasing equipment used in the mining process. It is more vulnerable to attack because of its open nature. It supports very low transaction rate of only 7 per second, which is far less as compared to Visa or Master card, which offers 10000 transactions per second. In case of fork, the transaction confirmation takes too much time. Beside it requires significant energy expenditure, and high latency; however, to ensure safety of consensus process, the operation is quite acceptable. Other variants of consensus mechanism as adopted by Bitcoin includes DogeCoin, LiteCoin [55], Monero and NameCoin [8], [56]. To implement consensus, RAFT, Paxos, and BFT (Byzantine Fault Tolerance) algorithms are some of the solutions used in distributed systems.

2) PROOF-OF-STAKE (POS)

Proof of Stake replaces the mining mechanism of the PoW model which consumes power in abundance. Instead of e.g. purchasing equipments to generate wining values, PoS suggests to purchase cryptocurrency and use the same to buy chances of block creation in blockchain [57]–[59].

3) PROOF-OF-ELAPSED-TIME (POET)

As per PoET, the model randomly selects next leader to finalize the block and in order to select the leader the model broadcasts election among all the participants to ensure fairness. To guarantee that the election is carried out in a secure environment, Trusted Execution Environment (TEE) is utilized. A validating node claiming a leader to mine a block has to produce proof from Trusted Execution Environment that other nodes can easily verify. Prove has to be submitted that it had shortest-wait-time before it is allowed to start mining the next block. Since it relies on specialized hardware, it is the main drawback of utilizing this consensus mechanism [60], [61].

4) BYZANTINE FAULT TOLERANCE

A Byzantine fault is any fault presenting different symptoms to different observers [62]. A Byzantine failure is the loss of a system service due to a Byzantine fault in systems that require consensus [63]. In distributed systems, Byzantine Fault Tolerance is the dependability of fault tolerant computer system, where a node has failed and there is improper information whether the node is failed. Other nodes need to reach a consensus whether to declare node as failed or to remove it from the network based on concerted action. Certain aircraft systems, like Boeing 777 Aircraft Information Management System, the Boeing 777 flight control system, and the Boeing 787 flight control system consider Byzantine fault tolerance in their design, as BFT works well in real time systems and where low latency is required [64], [65].

The Linux foundation developed Hyperledger fabric, a famous permisioned blockchain, which is based on pluggable consensus model. It is designed for a known and registered group of participants, with registered identities on a central registry service. The hyperledger fabric support two consensus models naming Practical Byzantine Fault Tolerance (PBFT) and its variation SIEVE to deal with non deterministic chaincode execution. Chaincode, a smart contract based blockchain, is supported by BFT.

TABLE 1. Comparison of blockchain consensus mechanisms.

	PoET	Proof-of-Work	BFT (Federated)	PoS	BFT (Variants)
Permissioned (or permissionless)	both	Permissionless	Permissionless	Both	Permissioned
Transaction Finality	Probabilistic	Probabilistic	immediate	Probabilistic	immediate
Performance	Medium	Low	High	High	High
Trust	Untrusted	Untrusted	semi trusted	Untrusted	semi trusted
Cost of Participation	No	Yes	No	Yes	No
Scalability	High	High	High	High	Low
Security	Unknown	<= 25%	<= 33%	Depends on algorithm	<= 33%
Power Consumption	Medium	High	Low	Medium	Medium

5) PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT):

Miguel Castro and Barbara Liskov proposed PBFT algorithm for solving consensus and to compensate the failure of Byzantine. PBFT uses the conception of replicated state machine and replicas for state changes. PBFT provides many other features including encryption of messaging among replicas and clients. To tolerate failures of ‘n’ nodes, the algorithm uses 3n + 1 replicas although it places some overhead in terms of messaging and performance over replicated nodes. Literature provides scalability details of 20 replicas for PBFT.

6) SIEVE CONSENSUS MODEL

The chaincode has a non-deterministic approach where upon execution of different replicas, the results may be different over a distributed network. In order to deal with non-determinism, SIEVE consensus model is designed, which speculatively executes all transactions and then results produced by various replicas are analyzed. If the divergence between the output is small over small number of replicas, then the diverging values are seived. If the observed divergence is across a large number of processes, then the operation is seived itself.

A high level comparison of various blockchain consensus mechanisms is provided in Table 1 based on specific characteristics of blockchain. These characteristics are confined to type of blockchain, performance in terms of transaction rate, the trust component, cost of participation i.e. cost to join the network or use specific services, scalability of the network i.e. addition of new nodes, security, and power consumption. The factors are not exhausted, rather these are representative enough to compare usage of various consensus mechanisms. In the next subsection, there are some recent variant of PoW consensus algorithms proposed. The author provided its analysis separately in following section.

7) FLAVORS OF POW

A variant of PoW consensus algorithms are proposed recently. Those are discussed below briefly. **Proof-of-Authority** (PoA) is an energy-efficient and fast consensus mechanism mostly used in permissioned blockchains as being a bit centralized. It is used by Vechain, Ethereum, Kovan, Testnet. In PoA based networks, transactions and blocks are validated using validators that run the software for putting the transactions into blocks once the identity is verified on-chain. For upholding the transaction process, the validators are provided incentives as well.

Proof of Weight (PoWeight) is another scalable and customizable efficient consensus mechanism used by Algorand. As in PoS, the number of tokens owned by the network presents the chances of discovering the next block, the PoWeight system considers weighted value instead of the percentage of tokens. **Proof-of-Reputation** (PoR) serves better in permissioned blockchain and is a collaborative consensus procedure. For ensuring the network’s security, considers the reputation of the node (participant). The nodes that have previously cheated the network face financial consequences that are considered by the PoR. A company that has previously shown a well-received reputation is voted to be an authoritative node and serves as Proof-of-Authority for signing and validating blocks.

Proof-of-Space (PoSpace) or Proof of Capacity (PoC) PoSpace considers capacity in terms of space while PoW considers computation power. PoSpace is more environmentally friendly as it does not require huge computation as demanded by PoW. When there is a legitimate request for service like sending an email, a non-trivial amount of disk space is to be allocated that will be needed during solving a challenge posted by service providers. This is done through PoSpace. i.e. to the prover, a piece of data is sent to a verifier that some amount of space is allocated. It is considered as a greener solution compared to PoW.

The **Proof-of-History** (PoH) consensus mechanism demands to present any evidence that shows the transaction is occurred before the occurrence of an event or after the occurrence of an event. The proof-of-history provides means for creating a record based on a particular history that serves as proof for the specific time period. An example of proof of the history of timestamps can better elaborate the mechanism. **Proof-of-Stake Velocity**, In order to validate transactions and secure the peer-to-peer network of Reddcoin, the proof-of-stake velocity is presented. It serves as an alternative solution to PoW and PoS. The term Stake and Velocity encourage ownership and activity in the network. **Proof of Burn** (PoB) is the process of burning coins refers to sending the digital currency to an address from which it cannot be retrieved back. This is done in comparison to the proof-of-work. By burning the coins, the node gets a chance to be selected in the lottery to mine the upcoming block. The more the coins are burned the maximum chances are availed to mine the block. However, the proof-of-burn just provides opportunities to those who are only ready to burn more money which should not be the only criteria.

The **Proof-of-Existence** (PoE) uses an online system for verification of some digital assets or documents over some specific time via timestamped transactional details in a cryptocurrency network. Its use cases can be found in document time-stamping, digital signed-agreements or for representing ownership of some data rather than the actual data.

Directed Acyclic Graph (DAG) is a fast and energy-efficient consensus mechanism that is used by Iota, Byteball, HashGraph. They are famous for the aspect of scalability and are a more general kind of Blockchain. They have a unique structure that facilitates its scalability. In an ordinary blockchain, blocks are appended in a sequential manner, one after the other in a linear fashion. However, in the Directed Acyclic Graph, blocks are appended in a parallel sessions offering more scalability.

H. BLOCKCHAIN STORAGE AND COMPUTATION MECHANISM

Storage and computation are important considerations to take care of that impacts the fundamental properties of blockchain. The storage design decisions include whether item data, item collection, and computations be placed on-chain or off-chain. These decision affect other attributes of implementing the system i.e. performance, cost, and flexibility. The famous cryptographic system, Bitcoin, embeds the item data in transaction on chain whose impact is more favorable in terms of achieving fundamental properties; however, it is less favorable in terms of cost, performance, and flexibility. Similarly, the public ethereum and smart contract also places item data on chain and embeds the same in transactions which improves cost efficiency. Keeping item off-chain is less favorable in terms of achieving fundamental properties; however, it improves cost, performance, and efficiency. Similarly, placing computation on-chain as per analogy of smart contracts produces good results in terms of achieving fundamental properties; however, the same is less favorable with regard to performance, cost, and flexibility. While keeping the same computations off-chain is less favorable in terms of computations but are more favorable with regards to other properties.

Based on the aforementioned blockchain platforms and related technologies, following studies provide a thorough review of literature in a number of domains pertaining to Internet-of-Things, Healthcare, and Business.

III. BLOCKCHAIN AND INTERNET OF THINGS (BIOT)

The way in which ubiquitous computing is prevailing is the use of smart devices and Internet-of-Things (IoT). Currently, there are more than 20 billion smart phones and IoT devices [66]. IoT devices are becoming a key component of most solutions through IoT-based sensor networks that provide remote monitoring, while smart devices provide remote real-time video-feed to individuals. IoT applications, such as, healthcare, body sensing and diagnostic reporting, industrial automation and monitoring, telemedicine and telemedicine consultation, security and surveillance, telemetry, asset tracking, etc. are making great strides. The success of IoT is in its ability to share information between devices or 'things', ease in accessibility, and support for heterogeneity. However, these characteristics induce some challenges, specifically related to security, privacy, and trust. Due to the absence of a verification or an audit mechanism, the challenges of security, privacy and trust are critical and complex in IoT, especially in a sensitive information domain, such as, economics, healthcare, engineering, and military communication. As blockchain provides a mechanism for information exchange (or transactions) between a group of unreliable entities, its inherent properties, such as, authentication, fraud protection, data integrity, etc. can solve the requirements of security, privacy, and trust in IoT.

A. MOTIVATION FOR BIOT

Blockchains can solve IoT's privacy and reliability issues. Blockchain seems to be the missing puzzle piece for the IoT industry. It can track billions of connected devices and can be used to handle transactions and communication between devices. This distributed nature of the blockchain can eliminate the issue of single point of failure and creates a more resilient IoT system. The encryption algorithms used in the blockchain ensure data privacy on the network [10]. The integrity of the distributed ledger of a blockchain is ensured because of it distributed location and malicious nodes or attackers cannot perform man-in-the-middle attacks as multiple communication channels are used to avoid wiretapping. Blockchain has already proven its value in financial services through cryptocurrencies, such as, Bitcoin and Ethereum, enabling communication between untrusted device groups and ensuring P2P payment services without the requirement of third-party brokers [67].

Distributed, autonomous, and reliable functionality of the blockchain is an ideal component of the IoT solution. It is

TABLE 2. Literature review on the topic of blockchain and IoT integration.

Authors	Domain	Contribution
Fernández-Caramés et al. [67]	Blockchain for the IoT	Blockchain review Identify BIoT applications Design of an optimized BIoT Challenges in BIoT Applications
Panarello et al. [68]	Blockchain and IoT Integration	Identify application areas for BioT Propose device manipulation and data management in BIoT
Reyna et al. [10]	BIoT Integration	Identify the emerging challenges Possible Integration Mechanism and Platforms
M. Atzori [77]	BIoT Platforms and limitations	Critical analysis of BIoT Platforms Discuss Limitation of blockchain in IoT
Conoscenti et al. [78]	BIoT as a Security Solution	Identify Security challenges of IoT Propose Blockchain as a Security solution to IoT
Prabhu et al. [69]	Blockchain and IoT	Blockchain as a backbone of IoT Device to device authentication.
Sagirlar et al. [79]	Enabling Blockchain in IoT	Hybrid blockchain architecture for IoT Pow and BFT based Hybrid-IoT platform
Cha et al. [80]	Enabling Blockchain in IoT	Blockchain connected gateway for IoT Ensure user's data privacy using a digital signature mechanism
Atlam et al. [81]	Blockchain and IoT Integration	Identify the benefits and challenges of BIoT Integration and future research directions

not surprising that corporate IoT firms have quickly adopted block-chain technology due to its advantages. In IoT networks, the blockchain can maintain an unchanging record of the smart device's activities and communications. This feature allows autonomous use of smart devices without centralized access. As a result, the blockchain opens the door to a number of IoT scenarios which were impossible to implement before. For example, utilizing a blockchain, the IoT solution enables secure, reliable messaging between devices in an IoT network. In this model, the blockchain handles the exchange of messages between devices, similar to financial transactions in a cryptocurrency network [68]. To enable message exchange, the device utilizes smart contracts to model communication between the two parties. One of the most interesting features of a blockchain is the ability to maintain a uniformly distributed, reliable ledger of every transaction that occurs on the network. This capability is essential for a wide variety of applications for Industrial IoT (IIoT) without the requirement of a centralized model [69].

B. INTEGRATION OF BLOCKCHAIN AND IOT

The Integration of blockchain into Internet-of-Things (BIoT) is not a novel idea, however, it has open up a relatively newer and broader domain for research and development in the field of IoT applications. Most of the limitations of IoT can be resolved using blockchain technologies; however, high computation, high energy consumption, higher storage and slow nature of transactions are some of the areas that need focus to enable the implementation of BIoT. In this section, we present the updated review of the application areas, available platforms, consumer applications, and challenges in BIoT.

Quite a few research articles have been written on the topic of BIoT, which deeply explore the potential domains of research, identify the issues and challenges, and propose future directions for the research in BIoT. Table 2 shows the details of the review papers in the field of BIoT and their contributions.

Due to the potential advantages of BIoT, quite a few of the IoT enablers have adopted the blockchain technology and developed consortium and alliances for standardization and smooth integration of BIoT. Trusted IoT Alliance [70] is an effort of the blockchain and IoT Protocol working group at Berkley in 2016. It is a consortium of 17 companies that aims at using the blockchain framework in the IoT architecture to enable security, scalability, heterogeneity, trust, and privacy in a decentralized structure. The Linux Foundation's Hyperledger Project [71] is an open source collaborative work which was started in 2015 and has 61 members. Hyperledger Project, with its automated consensus protocol PBFT, is light enough to be implemented on IoT; however in the future it will allow the users to implement their own consensus protocol. There are several other project which are working on enabling blockchain in IoT ecosystem, such as, EthEmbeded supported by Ethereum [72], LO3ENERGY [73], ChainOfThings [74], IoTeX [75], Raspnode [76].

C. MODELS OF BIOT

In an integrated blockchain and IoT environment, the communication model between IoT devices can be classified in three

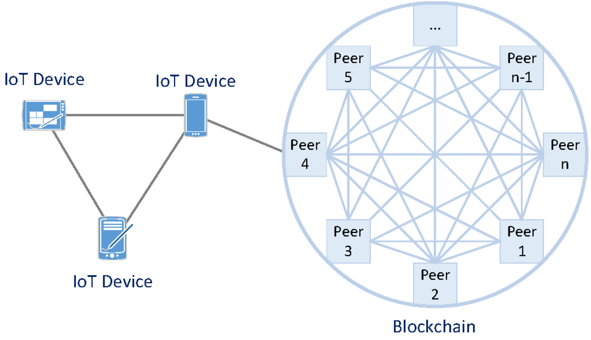


FIGURE 8. Inter-IoT device communication model.

different way, according to the interaction model [10]. The communication between IoT devices, can be either directly or through a blockchain. The third option is through a Fog or a Cloud computing model. These models are discussed in details as follows:

1) INTER-IOT DEVICES COMMUNICATION

In this model, IoT devices are communicating directly without the involvement of the blockchain. This model is the fastest as it does not involve the high computational and time consuming algorithms of blockchain. However, data integrity, privacy and security are not ensured and the mechanisms to enable privacy, reliability and security should be embedded in the inter-IoT communication. Only the history of communication/transactions between the IoT devices is stored at the blockchain. The recorded data, if not corrupted, is then immutable within the blockchain. This model is useful for fast communication between IoT devices with low security level requirements. Figure 8 illustrates the Inter-IoT device communication model.

2) IOT DEVICES COMMUNICATION THROUGH BLOCKCHAIN

In this model, all the communication/transactions between the IoT devices goes through the blockchain. This models ensures the data privacy, reliability and security for the both transactions and their data. An Immutable record of each transaction is again stored; however, the resulting transactions have blockchain overhead which causes latency. Figure 9 illustrates the model for IoT Devices Communication through blockchain.

3) IOT COMMUNICATION INVOLVING CLOUD/FOG NETWORK

Fog based IoT solutions for Cloud computing environment has revolutionized the IoT applications recently. Through this model, some or most of the computation load is transferred to Fog node, which takes away the load from the IoT devices, such as, encryption, hashing, and compression. Similarly, in an integrated blockchain and IoT scenario, the load due to blockchain's high computational and time consuming algorithms can be moved to the Fog node. Figure 10 shows a possible communication model for IoT devices with blockchain using a Fog/Cloud.

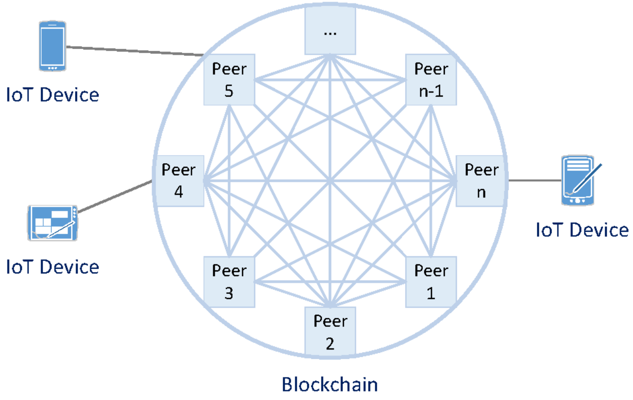


FIGURE 9. Model for IoT devices communication through blockchain.

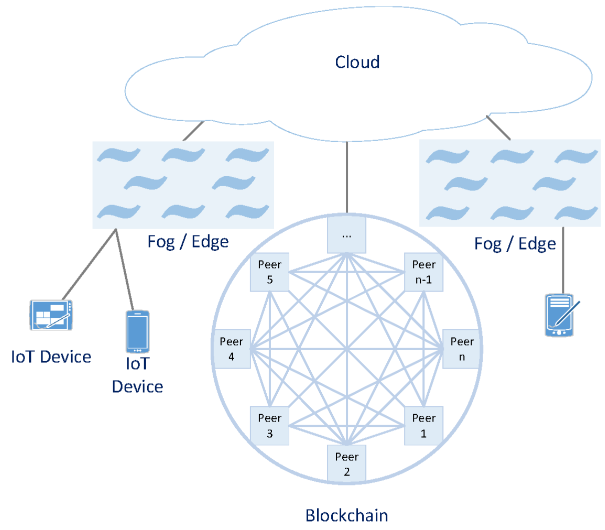


FIGURE 10. Model for IoT devices with blockchain using a Fog/Cloud.

D. APPLICATION AREAS OF BIOT

Integration of the blockchain technology in IoT has enabled the developers to envisage various applications in different areas; from industries, such as, agriculture, energy sector, smart grids, etc., to network designing and modeling, information provenance, storage and databases, and supply chain management. Table 3 shows a summary of the literature review done by the authors in the application areas of BIoT. Some of these areas are discussed in details in the following section:

1) INDUSTRIAL IOT

IoT technology has significantly improved the industry sector in terms of real-time remote monitoring and control, reducing latency, smart manufacturing, supply chain management, and asset tracking. However, due to the inherent characteristics of the Industrial IoT devices, such as, low cost and security standards, these devices are vulnerable to the attacks related to security, privacy and trust. Blockchain, as special ingredient,

TABLE 3. Literature review on the topic of BIoT Application Areas.

Literature	Domain	Contributions
	Application Area: Industrial IoT	
Skwarek[82]	Data Reliability and Security	Proposes a light-weight protocol for achieving industrial grade data reliability and security in Wireless Sensor Network using blockchain mechanism
Miller[83]	Integration of Blockchain and Industrial IoT (BIIoT)	Discusses the efficiencies, business opportunities, standardization and regulatory issues in BIoT.
Bahgaetal [84]	Application Platform for BIoT	Provides a platform for creating decentralized application for industrial manufacturing using BIoT
	Energy Sector	
Grid[119]	TransActive Energy	Discusses the issues and challenges of TransActive Energy
Lombardietal [85]	TransActive Energy in Smart Grid	Proposes an infrastructure for reliable and cost-effective transActive energy based on blockchain and smart contracts in Smart Grids
Zhangetal [86]	IoT based Electric Business	Proposes an IoT based Electric business model and realization of P2P trade using IoT and blockchain technology
	Device and Network Management	
Samaniegoetal [87]	Internet of Smart Things (IoST)	Proposes the use of Multichain to communicate between Smart Things
Huhetal [88]	Configuration and Control of IoT	Proposes an Ethereum based solution for IoT device configuration and builds a key management system
Novo[89]	Scalable Access Management	Proposes a distributed access control system for IoT based on blockchain
	Privacy	
Ouaddahetal [92]	Access Control Privacy	Proposes FairAccess: a decentralized pseudonymous and privacy preserving authorization management framework
Kravitzetal [93]	Identity and Attribute Management	Proposes a permission blockchain for user and device identity and attribute management
Dorrietal [90]	Lightweight blockchain	Proposed a lightweight blockchain for IoT with algorithms for lightweight consensus, distributed trust and throughput management
Dorrietal [?]	Lightweight blockchain	Proposes a lightweight blobkchain-based smart home framework security and privacy gains
ChainofThings[94]	Integrated Blockchain and IoT hardware	Platform for an integrated blockchain and IoT hardware solution to solve IoT's issues with identity, security, and interoperability
Alietal [120]	Privacy in IoT	Provides a mechanism data privacy via blockchains and IPFS
Filament[95]	IoT to blockchain transactions	Provides hardware solutions for IoT transactions against a blockchain, for enterprise and industrial IoT connectivity
	Trust	

TABLE 3. ***(Continued)*** **Literature review on the topic of BIoT Application Areas.**

TrustedIoTAlliance[70]	Blockchain integration for Heterogeneous IoT	Developing a blockchain framework in the IoT architecture to enable security, scalability, heterogeneity,trust, and privacy in a decentralized structure
Otteetal [97]	Trusted BIoT	Proposes TrustChain: a tamper-proof, scalable and blockchain-based data structure, andNetFlow: a Sybil-resistant model to determine trustworthiness.
Quetal [96]	Device Credibility	Proposes a framework for IoT device credibility verification
LO3Energy[73]	BIoT in Energy Sector	Developing blockchain based innovations to revolutionize how energy can be generated, stored, bought, sold and used
Mybit[98]	IoT Ecosystem	Proposes a distributed ecosystem for IoT blockchain for sharing resources and generating revenue
	Security	
Dorrietal [90]	Lightweight blockchain	Proposed a lightweight blockchain for IoT with algorithms for lightweight consensus, distributed trust and throughput management
Dorrietal [**?**]	Lightweight blockchain	Proposes a lightweight blobkchain-based smart home framework security and privacy gains
Skwarek[82]	Data Reliability and Security	Proposes a light-weight protocol for achieving industrial grade data reliability and security in Wireless Sensor Network using blockchain mechanism
Ganetal [104]	Attack Resistance	Proposes multiple architectures and protocols to enable key-based authentication for IoT devices
Otteetal [97]	Trusted BIoT	Proposes TrustChain: a tamper-proof, scalalabal and blockchain based data structure, and NetFlow: a Sybil-resistant model to determine trustworthiness.
Alphandetal [105]	Secure Authorized	Proposes IoTChain, a combination of the OSCAR architecture and the ACE authorization framework
Khanetal [100]	BIoT Security Review	A parametric analysis of the state-of-the-art IoT security issues, BIoT based solutions and challenges
Lietal [101]	Blockchain Security Survey	Provides evaluation of security risk, vulnerabilities and attacks on blockchain systems and review the existing solutions
Banerjeeetal [102]	BIoT Security Review	Identifies the need for blockchain technology in secure sharing of IoT datasets and securing IoT systems
Jesusetal [103]	Stalker Attack in BIoT	Discusses the working of Stalker attack on blockchain mining and identify how blockchain can provide security in IoT
	Reliability	
Modum[106]	Data Integrity & Authenticity	Provides data integrity and authenticity for global supply chain operations
	Services	
Samaniegoetal [121]	Internet of Smart Things (IoST)	Proposes secure communication as a service between Smart Things by using MultiChain
	Authentication and Identity	

TABLE 3. ***(Continued)*** **Literature review on the topic of BIoT Application Areas.**

Kravitzetal [93]	Identity and Attribute Management	Proposes a permission blockchain for user and device identity and attribute management
Ganetal [104]	Privacy & Attack Resistance	Proposes multiple architectures and protocols to enable key-based authentication for IoT devices
Ouaddahetal [92]	Access Control Privacy	Proposes FairAccess: a decentralized pseudonymous and privacy preserving authorization management framework
Wuetal[107]	Identity Management in IoT	Proposes an disjoint two-factor authentication mechanism for devices based on BIoT infrastructure
Ghulietal[110]	Identification of Ownership of IoT devices	Proposes a peer to peer identification mechanism for the ownership of IoT devices in a cloud environment
	Scalablility and Distribution	
Ghulietal[110]	Scalable mechanism for IoT Identification	Proposes a scalable peer to peer identification mechanism for the transfer of ownership of IoT between blockchains
Rutaetal [112]	Semantic Web of Things	Proposes a SOA based on a semantic blockchain for registration, discovery, selection and payment using smart contracts
Novo[89]	Scalable Access Management	Proposes a distributed access control system for IoT based on blockchain
Priscoetal [113]	Ethereum Smart Contracts for IoT	Presents smart locks for smart contracts for providing distributed shared economy
	Data Provenance	
Chronicled[118]	Smart Supply Chain	Proposes a secure exchange of physical IoT assets using data provenance technique based on blockchain
Neisseetal [114]	Data Accountability and Provenance Tracking	Proposes a blockchain of encoded publicly auditable contracts for recording access and usage of data
Liangetal [115]	Cloud Data Provenance	Proposes a system for collecting provenance data, storing in blockchain and validating in a cloud
Ramachandranetal [116]	Scientific Data Provenance	Proposes a mechanism based on the open provenance model (OPM) and smart contracts to trace scientific data
Kimetal [117]	Supply chain Provenance	Proposes the use of traceability ontology for asset tracking in a supply chain by using ontology based smart track execution
	Smart Contracts	
Christidisetal [11]	Blockchain Integration in IoT and Smart Contracts Feasibility	Discusses the feasibility of implementing blockchain in IoT, its usage in IoT solutions, and identify potential issues
Priscoetal [113]	Ethereum Smart Contracts for IoT	Presents smart locks for smart contracts for providing distributed shared economy
	Storage and Database	

TABLE 3. ***(Continued)*** **Literature review on the topic of BIoT Application Areas.**

Zhouetal ~\[122]	Distributed Computation and Storage	Provides secure distributed storage and distributed computation framework
McConaghyetal [123]	Blockchain Database	Present BigchainDB a distributed database
Shafaghetal [124]	Distributed Access Control and Data Management	Proposes a distributed storage for IoT data and its audit
Xuetal [125]	Blockchain based Storage System for Data Analytics	Proposes a Distributed storage enabling IoT devices to provide data analytics using parallelism
	Data Assurance	
Liangetal [108]	Data Assurance	Proposes a mechanism to ensure data collection and communication using a public blockchain for data integrity and provisioning of drones
Liuetal [109]	Data Integrity	Propose a blockchain-based framework for data integrity service for owners and consumers
	Availability and Accountability	
Boudguigaetal [111]	IoT Device Update	Investigates how confidentiality and integrity can ensured in BIoT to maintain availability and accountability

can prevent these attacks and provide data provenance and immutability to the IIoT solutions. Significant efforts have been made in the field of integrating IioT with blockchain, which is named as BIIoT. Researchers have evaluated the challenges posed by BIIoT, identified solutions [82], [83], and proposed platforms for developing BIIoT applications for industry sector [84].

2) ENERGY SECTOR

The implementation of blockchain in the energy sector has shown positive impact with cost reduction and, removal of intermediaries. Transactive energy allows the distributed energy sources and devices to trade energy in a distributed manner without a centralized system. However, when a smart grid with IoT technology is used then the issues of security and data privacy are critical. Authors in [85] have proposed an infrastructure for enabling secure, reliable, and a cost-effective transactive energy solution based on blockchain and smart contracts in Smart Grids. Researchers have also identified the potentials of energy trading using BIoT technology and proposed electric business models and Peer-to-peer energy trade using IoT and blockchain technology [86].

3) MANAGEMENT

The blockchain has also been identified as a management solution for IoT devices and networks. Blockchain stores immutable information about the data transaction and communication between the IoT nodes, maintains the historical data about the mobility, trace data from the origin to the destination, ensure data integrity and authentication. Based on blockchain model, researcher have proposed autonomous network management system for IoT network [87], and IoT devices [88]. Some claim of providing scalability to IoT data access, device networks [89], while others provide IoT devices configuration and key management systems [87].

4) PRIVACY

Due to the lack of standardization in IoT, the large scale of the IoT network, and the centralized access model of IoT data, privacy of IoT data is an ongoing challenge. Many solutions have been proposed to solve the privacy issues in the field of IoT, but they are based on a centralized entity, which effects the scalability of the IoT networks. Blockchain, with its decentralized structure enables the data privacy mechanism without inducing the scalability issue. IoT data is stored on a blockchain and parts of it is release temporarily to receive services and make transactions. To enable privacy in the IoT, researcher have proposed light-weight blockchain solutions. Dorri *et al.* have presented a lightweight blockchain with algorithms for lightweight consensus, distributed trust, and throughput management [90], which is optimized for IoT. Similarly, another lightweight solution is proposed with a case study on BIoT based smart home framework [91]. Furthermore, research has been done in maintaining privacy in data and access control mechanism for IoT [92] and providing anonymity to users and devices in an IoT scenario using blockchain [93]. In [81], the authors have presented a network architecture to provide data privacy using blockchains and InterPlanetary File System (IPFS). In the proposed "Standard

Consortium'' architecture, smart blockchain contracts control access, while providing accountability to both data owners and third parties. Chain of Things [94] is platform for an integrated blockchain and IoT hardware solution to solve IoT's issues related to privacy, security, and interoperability, while Filament [95] provides a hardware solution for transactions between IoT devices using blockchain for enterprise and industrial IoT.

5) TRUST

In IoT infrastructure, the lack of trust between devices is a critical issue as the nodes themselves are not able to implement the complex trust algorithms. Mostly, trust is maintained using a centralized trusted third party, which inherit the issue of single point of failure. Blockchain, with it decentralized mechanism, solves the issue of single point of failure and also ensures that the IoT devices can communicate or perform transaction without the need of establishing trust between stakeholders. By integrating the blockchain in the IoT infrastructure, one can maintain credibility by verifying the IoT entities based on the chain of hashed blocks [96]. Researchers have also worked on identifying attacks on trust, such as, sybil attack and provide scalable solution for making the BIoT communication attack resistant [97]. Different consortium for enabling BIoT, such as Trusted IoT Alliance [70], have ensured that the platforms developed by them maintain trust and credibility in BIoT communications [73], [98], [99].

6) SECURITY

There has been a lot of work done in the field of providing security in IoT communication; however, most of these solutions are based on high computational cryptographic algorithms. The integration of blockchain in IoT brings implicit solution to the security issues in IoT. Blockchain can provide privacy and reliability, authentication, authorization, and access control in IoT ecosystems. Khan *et al.* have discussed the security issues in IoT and the solutions and open challenges to overcome in the field of BIoT [100]. Li *et al.* presented a survey on security of blockchain [101], some of which solution can be implemented in IoT based system by integrating blockchain. Similarly, Banerjee *et al.* gave a literature review of the security solution that blockchain bring to IoT [102]. Lastly, a comprehensive survey for securing IoT is presented by Jesus *et al.* [103]. However, due to the challenges of IoT infrastructure, a lot of research is being done on the topic of securing BIoT and more efficient solutions are being proposed. Due to the low computational capabilities of the IoT devices, Dorri *et al.* has proposed a lightweight blockchain for IoT with algorithms for lightweight consensus, distributed trust and throughput management [91]. It is lightweight blobkchain-based smart home framework proposed for security and privacy gains [90]. Similarly, a lightweight protocol for achieving industrial grade data reliability and security in Wireless Sensor Network using blockchain mechanism is proposed in [82]. Some researcher are working on developing multiple architectures and protocols to enable key-based authentication for IoT devices [104] based on a combination of the OSCAR architecture and the ACE authorization framework (named IoTChain) [105]. A trust is one of the enabling technology for secure communication, have proposed a tamper-proof, scalable and blockchain-based data structure (called TrustChain), and presented NetFlow, which is a Sybil-resistant model to determine trustworthiness [97]. Modum is a platform developed for enabling data reliability and confidentiality in BIoT [106]. In BIoT, maintaining identity for each node, providing privacy to the nodes as well as authentication the devices are some of the major concerns. Therefore, researchers have focused on providing solutions for secure user identity management [93], device authentication [104], [107] and maintaining privacy [92]. Furthermore, state-of-the-art solutions are proposed by researchers for data assurance [108], data integrity [109] and access control mechanism [92], while Ghuli *et al.* presented a peer-to-peer identification mechanism for the ownership of IoT devices in a cloud environment [110]. Similarly, in [111], the authors investigates how confidentiality and integrity can be ensured in BIoT to maintain availability and accountability of IoT data and devices.

7) DECENTRALIZATION AND SCALABILITY

IoT infrastructure relies on the centralized architecture, which make it hard for the IoT ecosystem to be scalable. By integrating the decentralized blockchain technology in the IoT, most of the issues of the IoT can be resolved. Researchers have devised blockchain based solution for solving the scalability issue of IoT. A scalable peer-to-peer identification mechanism is presented in [110] for the transfer of ownership of IoT devices between similar blockchains. A service oriented architecture (SOA) based on a semantic blockchain of IoT devices is proposed in [112] for registration, discovery, selection and payment using smart contracts in BIoT. Furthermore, a distributed access control system for IoT based on blockchain [89] and smart locks for smart contracts for providing distributed shared economy [113] are also proposed.

8) DATA PROVENANCE

As a blockchain is capable of maintaining an immutable record of transactions which is computationally secure and reliable, the historic data about the communication or transaction between the IoT devices can also be recorded in similar way. Data provenance is a technique used to provide traceability of data from the origin to the destination, which is used to ensure data integrity and authentication of sender. With the integration of blockchain mechanism in the IoT infrastructure data provenance can be achieved which is reliable and secure itself from man in the middle and data spoofing attacks. Therefore, quite a few solutions have been proposed for ensuring data provenance in BIoT environment, such as in [114]–[116]. In a supply-chain scenario the data provenance solution based on blockchain can be utilized in asset and goods tracking [117]. Chronicled is such a solution which uses BIoT for secure exchange of physical assets [118].

9) SMART CONTRACTS

Although blockchain provides solutions to many of the IoT problem; however, it has high computational requirements, which demands cost-effective and less time and resource consuming mechanism. Christidis *et al.* have evaluation the potential challenges in integrating blockchain with the IoT framework and identified the issues for developing light-weight solutions for implementing smart contracts in BIoT [11]. In [113] the author proposed Slock.it a solution to implement smart contract in BIoT based on Ethereum [113].

10) STORAGE AND DATABASE

Blockchain technology, due to its distributed nature, can contribute in developing distributed database and storage facilities. Not only the storage system would be distributed, blockchain can also ensure data integrity, access control and authorization of users. Zhou *et al.* have presented a blockchain based IoT system, called BeeKeeper, which provides secure distributed storage and provides distributed computation by using IoT devices computational powers without losing data privacy [122]. BigchainDB is a distributed storage software based on blockchain technology, which provides high transaction rate, low latency, indexing and query of structured data [123]. Shafagh *et al.* have presented a distributed storage solution for recording IoT data and maintaining data audit [124]. As a large amount of data is collected by an IoT ecosystem, a solution for data analytics was proposed in [125] which is based on blockchain technology and provide distributed data storage. Similar to storage, BIoT solutions can be used to provide other resources as a service to the users. In [121], the authors have presented and idea of using blockchain in IoT as a service from Cloud/Fog which can reduce the computational load on IoT devices.

E. CHALLENGES FOR BIOT

IoT, with its applications in variety of industries, has certain characteristics, such as, the limitation of memory, computational capacity and power supply, along with high data generation, that induce high number of challenges [10]. Furthermore, due to its centralized structure, scalability and single point of failure are critical issues. The integration of blockchain within the IoT infrastructure shows potential solution with its distributed nature and immutable data records. However, the integrated IoT with blockchain, BIoT, has certain issues and challenges that the research community is required to address. The requirements, issues and challenges of BIoT have been analyzed by the research community [126] and presented in Table 4; however, the need to comprehensively evaluate the problems and identify solutions to BIoT integration is still a hot and unexplored topic. Some of the major issues in the BIoT are discussed in this section.

1) LIMITED RESOURCES

Due to the limited resources of IoT devices, the high computational and time consuming algorithms of blockchain are not suitable for BIoT in their pure form. Cryptographic algorithm, hash functions, consensus algorithm and Smart contract have high load on computation, power, storage and have high latency. The current size of hash for blockchain is relatively high for IoT devices. Furthermore, IoT nodes generate high amount of data as compared to the cryptocurrency node, which augments the requirement of storage. Research community have analyzed some of these issues and identified possible adaptation in the blockchain mechanism for reducing computational load [127], energy consumption [4], and storage requirements [10] on IoT devices. Dorri *et al.* proposed an optimized blockchain that could be suitable for IoT infrastructure [133]. Concept of virtualization has been introduces for solving limited resource issues [72], [128].

2) SECURITY

In their statistical report, the International Data Corporation has identified the challenge of security to be the most critical. In a report, it says, ‘‘IDC believes that providing security and trust for IoT use cases requires new solutions and approaches that go beyond traditional techniques used in typical IT environments. In this respect, the fundamental concepts behind blockchain technology are quite powerful, offering compelling features to secure IoT applications, networks, and devices’’. However, the current cryptographic functions, due to scarce resources of IoT are hard to implement. Elliptic curve cryptography and RSA based public key encryption have a large footprint and are deemed as not suitable for BIoT [129]. Furthermore, there are still issues in the reliability of the blockchain as it is widely believed that blockchain is used by malicious entities for acquisition of economic gain. On the topic of security in blockchain, some researchers have written comprehensive reviews for identifying issues and challenges [100], [101], [129], however, the need for the optimized solution for tackling these issues is eminent. Data integrity is implicitly implemented in blockchain in maintaining the hash chain for each record [109], however, the issue of maintaining availability and accountability in BIoT pose a challenge. A potential solution is discussed in [111] by Boudguiga *et al.* but a lightweight solution is the missing ingredient. In IoT, the devices are more prone to be hacked or attacked by internal or external nodes due to the lack of update mechanism for configuration and firmware with vulnerabilities.

3) SCALABILITY

IoT is a centralized architecture and lacks scalability. The distributed nature of blockchain has to be carefully implemented as to avoid the issue of scalability. As the scale of a blockchain increases, the size of blockchain hash also increases. This puts a lot of load on the storage of IoT nodes. Researchers have identified this issue and proposed some solutions, such as, the semantic blockchain [112] and the scalable architecture for access management [89] and for solving the scalability issues. It is also recommended to use edge,cloud or fog

TABLE 4. Literature review of the issues and challenges of BIoT.

Issues and Challenges	Authors	Domain
Limited Resources	[127]	Computational load
	[4]	Power Consumption
	[10]	Storage
	[128]	Virtualization
	[67]	Resource scarcity in IoT devices
	[68]	Computational and power cost
Security	[129]	ECC and RSA performance analysis on IoT devices
	[101]	Security challenges of BIoT systems
	[100]	Issues in the Integration of blockchain and IoT
	[102]	Challenges in the Integration of blockchain and IoT
	[109]	Data Integrity in BIoT
	[111]	Availability & Accountability in BIoT
	[67]	Critical analysis of security issues in BIoT
	[68]	Identification of issues and solution in securing BIoT
Identity & Privacy	[130]	Challenges in providing Identity and privacy in BIoT
	[93]	Identity and Attribute Management
	[91]	Lightweight blockchain
	[67]	Critical analysis of privacy issues in BIoT
	[68]	Identification of issues and solution in ensuring privacy in BIoT
Scalability	[131]	Challenges in scalability in edge/fog based BIoT
	[112]	Issues of scalability and a proposed solution
	[89]	Scalable access management in BIoT
	[67]	Critical analysis of scalability issues in BIoT
	[68]	Identification of issues and solution in ensuring scalability in BIoT
Consensus	[132]	Consensus issues in IoT
	[67]	Critical analysis of consensus issues in BIoT
	[68]	Identification of issues and solution in ensuring consensus in BIoT
Legal Issues	[10]	Regulatory issues in BIoT
	[67]	Critical analysis of legal issues in BIoT
Smart Contracts	[131]	Limitation of smart contract implementation in fog based BIoT
	[68]	Futuristic demand of smart contracts in BIoT
	[10]	Analysis of IoT constraints in implementing smart contracts

computing nodes to relieve the load from the IoT devices by maintaining a hybrid distributed architecture of centralized BIoT networks [131].

4) PRIVACY/ANONYMITY

The public key or hash is used by the node in the BIoT as its ID, hence there can be an issue of anonymity and privacy. In cryptocurrency, anonymity may not be an issue, but in an application like smart healthcare. A user may not want to identify his/her identity or maintain privacy about his/her data. Moreover, as the IoT devices are physically and computational easy to be hacked or attacked, the issue of data privacy becomes critical. Also, different countries of the world have separate rules about data privacy of the user and devices. Hence, a global privacy standard is needed to be implemented all over the world [130]. This would simplify the privacy issues and requirements. Kravitz *et al.* have presented a solution for securing user identity in a BIoT environment [93], while a case study for smart home is presented in [91] to identify privacy issues and challenges in BIoT [91]. Filament [95] and Chain of Things [94] are platforms that promise solutions for maintaining privacy in BIoT environment. The use of private blockchain can be used to limit the access of users in a blockchain, which can limit the loss of privacy to certain domain.

5) CONSENSUS, SMART CONTRACTS & REGULATORY ISSUES

In BIoT, due to the limited resources of computation, storage, memory, and bandwidth, the consensus algorithms used in cryptocurrency blockchain are hard to be implemented. Although, there are some solutions proposed by the research community for devising a consensus algorithm [132], which is lightweight enough to be more suitable for IoT devices in terms of energy consumption. But they still require a lot of computational resources and time. Some have suggested to put the load of consensus and mining on the Fog nodes [131], however, this would disrupt the distributed nature of the blockchain. Smart contracts have introduced potential killer applications in IoT, such as, automated reliable transactions, payment, fee collection, etc. However, their effectiveness is related to the low cost implementation solution for blockchain in BIoT. Due to the lack of standard for implementing blockchain, the legal issues are also needed to be solved for BIoT [10]. From supply chain to asset tracking, to online shopping, these application would not be envisaged unless there is a global standard defined that can be implemented all over the world [130].

6) MISCELLANEOUS ISSUES

Apart of the issues and challenges that are discussed above, there are many important issues and challenges that need to be resolved for fully utilizing the true potential of blockchain based IoT. Some of these challenges are: Device heterogeneity in IoT, Interoperability of protocols and standards, throughput and latency, federation between BIoTs, IoT device firmware trusted updates, and vulnerabilities in blockchain algorithms. These issues seem small but it affects the optimization of BIoT.

F. CONSUMER APPLICATIONS OF BIOT

Although there are a lot of challenges, issues and requirement that needed to be answered in realizing the full potential of the BIoT, it shows promising potential in the field of future applications [134], [135]. According to the International Data Corporation (IDC) almost 20% of IoT deployments will include blockchain technology by 2019. Some of the promising applications of BIoT are: supply chain management, border control, food provenance, drug authentication, smart metering, crypto-asset management, digital identity, deed authentication, smart cities, data provenance for medical records, etc.

IV. BLOCKCHAIN IN HEALTHCARE

A. EXISTING HEALTHCARE PROBLEMS

Blockchain is an emerging enabling technology that can provide solutions for real world problems including healthcare which is considered as one of the basic human rights. In the last few years, blockchain technology has gained reasonable confidence as a smart new trusted distributed system for performing and storing transaction record in the form of distributed ledger. However, according to the healthcare perspective, the stakeholders are more involved in discussing and questioning blockchain as a platform rather than focusing on healthcare issues that can be solved by blockchain. Therefore, in this section, we will first highlight the healthcare major issues that can be addressed by this technology then we will discuss the possible solutions [12].

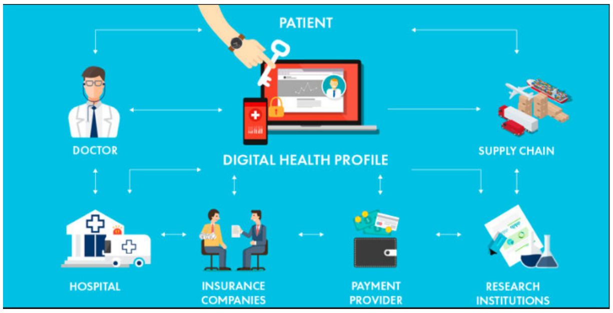


FIGURE 11. Blockchain in healthcare: Eco system [136].

Figure 11 shows the conceptual ecosystem for the use of blockchain technology in healthcare [136]. The figure highlights various stakeholders involved including patient, doctor, insurance companies, payment provider, and research institutions. Blockchain can facilitate the interoperability of updated digital health profile of patients in a timely manner along with other benefits, such as, patient data security, protecting patient's identity, and the coordination of care. Now we highlight the major healthcare issues that can be addressed by the blockchain technology.

1) SECURE HEALTH INFORMATION EXCHANGE BETWEEN STAKEHOLDERS

a: ENSURING PRIVACY

The ensuring privacy of healthcare record is one of the major concerns while exchanging information between various stakeholders, such as, doctors, local and international research and development units, health organizations, government sectors, patients history, and information forwarded to their caregivers.

b: IMPROVE INTEGRITY OF HEALTH RECORDS

Improving or maintaining the high level of data integrity is critical in healthcare as the prescription, lab test and major operation are suggested based on these records. Errors in the record could lead to wrong diagnosis and inappropriate care. These errors can be produced in electronic systems during exchange, sharing, and storing record.

c: DECENTRALIZED HEALTH INSURANCE RECORD

Most countries are following health insurance system in which insurance is used to pay the expenses against the healthcare services that are provided to the patient, both locally and internationally. Various models of health insurance are followed all over the world but mostly this insurance is provided through social insurance system or private insurance companies. Decentralization of these insurance record is critical for ensuring health services to patients irrespective of their resident country.

2) COST OF HEALTHCARE TRANSACTIONS

In healthcare system transaction, there are various factors that produces cost including redundant transmission cost, intermediary between related organizations, and near real-time processing. The challenge is to propose a model that will incur low cost healthcare transactions between stakeholders.

3) MASTER PATIENT IDENTIFIER

In enterprise systems there is a concept of master patient index or identifier to maintain consistent and accurate medical record of patient across various organizations. Patient identification matching is a major problem when it comes to global healthcare services. Identification matching in Healthcare transaction, such as, exchange of healthcare record, can violate the integrity of medical record and this could have severe consequences.

4) LIMITED ACCESS TO HEALTH RECORD

In terms of healthcare information exchange, limited access to health record is provided to maintain security; however, this also creates hurdles in researching about the analyses of various diagnosis and effects of certain prescriptions. In general, it is an obstacle to further ethical research and development.

5) CONFLICTING OR INCONSISTENT RULES AND PERMISSION RELATED TO HEALTHCARE

This highlights the issues of allowing right health organization to access required patients medical record at the right time. There are different regulations by countries related to the access-rights of patients' medical record and this introduces challenges related to the availability of medical record for right stakeholder at the desired time. We believe smart contract concept in blockchain can reasonably address this issue which we will discuss in detail in the next section.

6) INTEROPERABILITY WITH HEALTHCARE DATA AND APPLICATIONS

There are challenges of interoperability when it comes to access, exchange, and storage for healthcare application and data. It first requires establishment of trust between various stakeholders and then assurance of secure access and transactions. We believe blockchain has the capability to address these challenges.

B. BLOCKCHAIN APPLICATIONS IN HEALTHCARE

We observe that there is a lot of talk about the blockchain technology itself; however, the discussions on solution of existing healthcare industry problem using this technology is ignored. Here, we review suggested solutions for the existing healthcare problems by the researchers, industries, and other stakeholders.

There are various use cases and exemplary applications prototype of blockchain technology in healthcare. For example, in a recently published paper [137], authors have classified blockchain healthcare applications in six narrow areas. In this article, we present review of applications from two perspectives; (a) proposed by research community and (b) from industry and then classify them in four broader applications areas: 1) Secure Electronic Health record exchange, 2) Pharmaceutical Supply chain, 3) Secure Remote patient monitoring, and 4) Healthcare Insurance claim and Data Analytics. We now briefly review some of these healthcare applications.

1) SECURE ELECTRONIC HEALTH RECORD EXCHANGE

In the last few years researchers have focused on proposing blockchain technology as secure solution for online exchange of healthcare data between parties. For example, in the white paper published by Deloitte [12], the authors proposed a new distributed blockchain framework for supporting integration and secure interoperability of healthcare information across a range of stakeholder worldwide. Lack of common architecture and standards for efficient secure exchange of healthcare information is their main motivation in this paper.

In the first phase, they suggest to check for the four preconditions before initiating the use of blockchain technology for healthcare sector. They suggest to use blockchain in case of fulfillment of these pre-conditions. In second phase, they suggest healthcare organizations to design use cases mainly to verify and authenticate information or value of transactions involves in the use case. Third phase discusses the smart contract that automatically executes on fulfillment of conditions. This strengthen the technology by enhancing the trust between stakeholders. Last phase proposes to implement the proposed blockchain solution as either permissioned or permissionless blockchain. They also define the concept of on-chain and off-chain data in a transaction layer.

In [138] authors have suggested an approach for health information exchange using blockchain. They address the problem of cross institutional exchange and sharing of healthcare data. This is the major problem for healthcare sector mainly due to the privacy concerns and rules. First, they define some assumptions related to the stakeholders involved, then they define the structure and semantics of the block containing entries of the patient in the healthcare blockchain. Then they define four phases of adding a new block in the blockchain, similar to Bitcoin. They use SHA 256 as hashing algorithm. Then they suggest an algorithm for proof of interoperability for network consensus. Fast Healthcare Interoperability Resources (FHIR) [139] is used as standard for exchanging health record. The proposed algorithm inputs pending transactions, set of FHIR profiles URLs, current block, and set of valid transaction. It checks profile conformance then makes a validate request for FHIR server and finally checks the response for the proof of interoperability.

Authors in [140] proposed a model to ensure privacy of patient data on private blockchain. They propose to apply privacy preserving online machine learning algorithm, such as, explorer on a private blockchain network. Figure12 shows the example of the block in the proposed model. Each bock represents a transaction and each transaction consists of model, flag, hash, and error. Then the authors propose an algorithm for the proof of information. The algorithm inputs the site S (stakeholder), waiting and polling time periods, and number

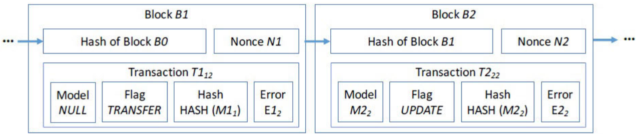
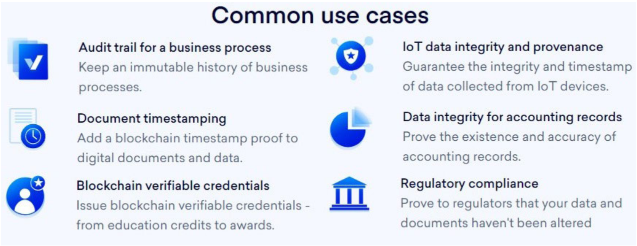


FIGURE 12. Proposed model chain example of two blocks.



Common use cases

Audit trail for a business process
Keep an immutable history of business processes.

Document timestamping
Add a blockchain timestamp proof to digital documents and data.

Blockchain verifiable credentials
Issue blockchain verifiable credentials - from education credits to awards.

IoT data integrity and provenance
Guarantee the integrity and timestamp of data collected from IoT devices.

Data integrity for accounting records
Prove the existence and accuracy of accounting records.

Regulatory compliance
Prove to regulators that your data and documents haven't been altered

FIGURE 13. Common Use cases of blockchain technology by TIERION [16].

of sites N participating in the transaction. The algorithm outputs the latest online machine learning model M.

Since year 2015, many companies worldwide started investigating in the blockchain technology in healthcare, business and other sectors.

TIERION [16] creates technology and products related to healthcare. As per our knowledge this is the first company to complete project related to use of blockchain in healthcare in 2015. They foresee blockchain technology for verification of range of things from medical record to online shopping. They initiated a project with the name ''Proof'' [141], which uses Bitcoin blockchain to prove integrity and timestamp of the data. Figure 13 shows the common use cases of blockchain technology proposed by the TIERION company including record of immutable history of business process, credential for verification, in IoT, etc.

2) PHARMACEUTICAL SUPPLY CHAIN

There are some blockchain health care applications in terms of Pharmaceutical supply chain. For example, authors in [142] propose to use blockchain to provide secure access to the temperature record of pharmaceutical products during their transportation to the various stakeholders in the market. This allows the pharmaceutical company to monitor the quality control process of drugs during their transportation. Similarly authors in [91], propose a conceptual design of pharmaceutical turnover control system using hyperledger fabric platform of blockchain. They have identified three types of nodes (namely, client, ordering, and endorsing nodes) and role of each node type. The client node places a transaction execute order which is supervised by endorser node, and ordering node involves in creating block of transactions and their status update.

GEM [17] is a company that provide solution in healthcare and supply chain. GEM has created GEMOS (a blockchain based operating system), which is an enterprise platform that will enable data driven healthcare economy to securely share and access data with the right permission. They investigated the healthcare use cases with their partner company PHILIPS to explore how blockchain technology facilitates in patient centric approach to healthcare. They have also published their finding related to blockchain use in healthcare.

3) SECURE REMOTE PATIENT MONITORING

In this subsection, we review blockchain applications related to secure patient monitoring. In [143], authors have proposed to use blockchain technology for secure remote patient monitoring. They suggested to use Ethereum based public blockchain system that uses smart contract system that allow real time monitoring of patients, sending notification to medical experts, patients, care-givers and allow secure storage of all events as transactions records on the blockchain. This solves common security vulnerabilities of general remote patient monitoring system by providing resilient to various type of manipulations. The transaction can be traced back to its origin in blockchain. Verified blocks are immutable in blockchain; however, this process of verifying each block requires time which results in a delay. Privacy of patient health record is ensured by assignment of anonymous identity to each record.

4) HEALTHCARE INSURANCE CLAIM AND DATA ANALYTICS

We can find some example of using blockchain for healthcare insurance. For example,a healthcare insurance storage system using blockchain is proposed in [144]. They suggest secure storage of healthcare insurance record that can help hospitals and insurance companies requirement of huge storage spaces and security mechanisms. This blockchain consists of nodes representing hospitals, insurance companies, servers, and record nodes. In [145] authors have suggested how insurer and insurance companies will benefits from blockchain technology to target specific needs and secure storage and access of healthcare insurance record.

HealthCoin [18] is a platform that uses blockchain technology that allow employee, their insurer, and government to publicize diabetic prevention awareness to all stakeholder of the society. Some examples of blockchain in data analytics were also found, such as, authors in [146] have investigated the use of blockchain technology to train, retrain and classify deep learning architecture in Patient-Specific Arrhythmia Classification. Similarly, a software company named ''Blockchain Health'' [147] created a secure connection between stakeholders to share healthcare research data securely. GitHub [2] has also initiated projects related to using blockchain technology in healthcare. It also provides the platform where researcher and industry can share and collaborate.

C. COMPARATIVE ANALYSIS

In this subsection, we compare, categorize and analyze existing solution for using blockchain technology for healthcare.

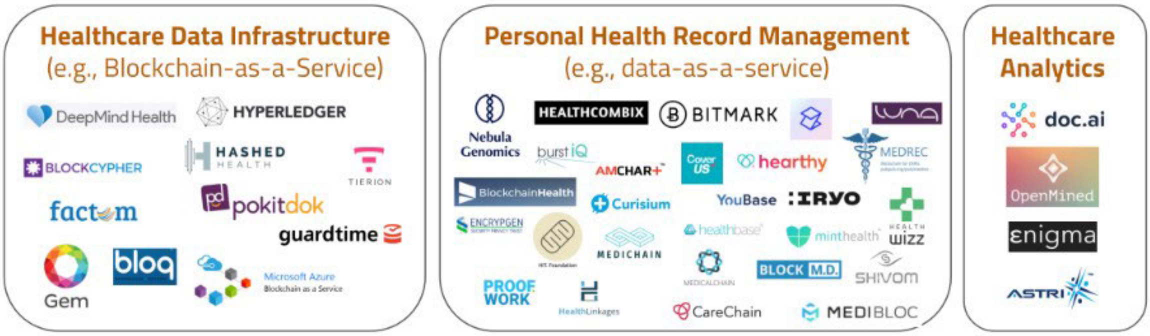


FIGURE 14. Categorization of healthcare related blockchain projects [2].

TABLE 5. Blockchain solutions for healthcare.

Contribution from Research Community				
Author Referred	**Problem Addressed**	**Major Contribution**	**Strength & Weakness**	**Year**
Delotite [12]	interoperatibility of health care information	proposed distributed blockchain framework for secure info exchange	Increase trust by smart contract parties needs to trust	2016
Peterson [138]	Secure health info exchange Limited access to healthcare info	Heath information exchange blockchain model	Use FHIR[7] for proof of interoperability	2016
Tsung [140]	Ensure privacy	Privacy preserving online machine learning algorithm	Each Block has flag, hash and error	2018
Iyengar [148]	Access Control	Cloud based healthcare system	Requirement of cloud app with strict privacy	2018
Zhang [149]	Interoperability of healthcare information	Apply software pattern for Interoperability in blockchain healthcare	Discuss implementation challenges	2017
Leo [136]	Challenges to Adoption of blockchain for healthcare	Blockchain uses in healthcare & Complex challenges	Benefits and adoption challenges presented well.	2018
Contribution from Industry				
Author Referred	**Problem Addressed**	**Major contribution**	**Project or Product**	**Year**
TIERON [16]	Verification of medical records	Foreseeblockchain for verification of range of things	Product	2015
Proof [141]	Integrity of healthcare data	Use BitCoinblockchain to prove integrity and timestamp of data.	Product	2016
GARTNER [150]	Privacy	Number of projects to use of blockchain technology	Projects	2016
GEM [17]	Secure sharing and access control	GEMOS(blockchain based operating system)	Product	2017
Blockchain Health [147]	Interoperability	Secure connect between stakeholder to share health research	Research projects and Product	2016
GitHub [2]	Interoperability	Projects related to using blockchain in healthcare	Projects	2017

Blockchain healthcare solutions from industry and research community point of view are summarized in Table 5. Blockchain solutions for Healthcare are also summarized in Table 5.

An illustration of healthcare related blockchain projects is provided in Figure14. These projects from various companies are categorized in three main categories: a) Healthcare data infrastructure which focuses on providing blockchain as a service b) Personal Health Record Management provides health data as a service c) Health Analytics which focuses on analytics and research findings

To sum up, we have observed the tremendous potential of blockchain technology in healthcare. Specifically, in providing secure healthcare data infrastructure sharing healthcare data between various stakeholders. Both research community and industry also realized this potential and explored the use of this technology for healthcare aggressively in the last three years. Table 5 shows the basic analysis of the work done so far related to blockchain in healthcare highlighting key parameters. These parameters include the problems addressed, major contribution in the research paper or the project, and major strength and weakness.

V. BLOCKCHAIN IN BUSINESS

Bockchain technology is shy of the ''peak of inflated expectations'' for the most emerging technologies. A range of industries including healthcare [1], [151], [152], supply chain management [153]–[155], finance [156]–[158], insurance [159]–[161], and logistics [162]–[164] are use cases of blockchain.

Blockchain is a replicated, append-only dataset, which has the major strength of maintaining tamper-proof distributed digital ledger of transactions that is updated based on consensus mechanism [36], [165] within entities. This integrity aware append-only technology helps in many business related use-cases and applications. In blockchain, all the transactions or digital events are recorded in public ledger [166] accessible to all nodes in the network thus enforces integrity of data over the network [167]. The data and information once uploaded to the network can never be altered or removed without consensus [168]. It ultimately offers a democratized system which can contribute in improving economy.

One of the most emergent use cases of blockchain in businesses is a computer program known as smart-contract, introduced in 1994 by Nick Szabo, which automatically executes based on predefined configuration to fulfill various terms of contract [169]–[171]. Ethereum [28] and Codius [172] have implemented smart contracts alongside blockchain.

A. BLOCKCHAIN IN CLOUD - OUTSOURCING

Blockchain solutions are adopted in cloud computing, such as, in [173] the author adopted blockchain for providing trusted solution for outsouring of services and for their customer's secure payment. Trust is a real concern in cloud computing adoption. However, by enabling blockchain underlying the cloud services. It will strengthen the outsourcing business and will get more customer.Similarly, in [174] the author has given more detailed analysis and results regarding the trusted payment system among the users and outsourcing service providers.

B. REAL-ESTATE USE-CASES

Another business related implementation of smart contract is the smart property [175], [176] which deals with buying and selling of physical and non-physical properties including buildings, houses, lands and even the organizational shares [177], [178]. There are applications of property registration system that can register the Lands of the country and any other real-estate. The existing property registration systems are either manual or its on centralized which off-course do not offer any restrictions to record tempering and transparency. Some of these real-estate proposals are based on permmissioned blockchain while some of them are on public blockchain, such as, ehtereum.

C. BANKING

Banking sector is shifting and looking for opportunities to implement its applications as per blockchain analogy in its setup. Famous banks including Barclays [179], Goldman Sachs [180], LohmusRain, LHV bank [181] have shown that the blockchain can be the most secure and tested mean for implementation of finance and banking related matters [182]. They are working on creation of framework to utilize benefits of blockchain. Consequently, Mastercard, NASDAK, Visa, and life insurance companies [183] are investing to explore the possible adoption of blockchains into their respective systems. Table 6 shows a comparison of traditional banking with Internet and additionally blockchain enabled bank services with various parameters. That helps to judge the benefits of blockchahin enabled banking with traditional services.

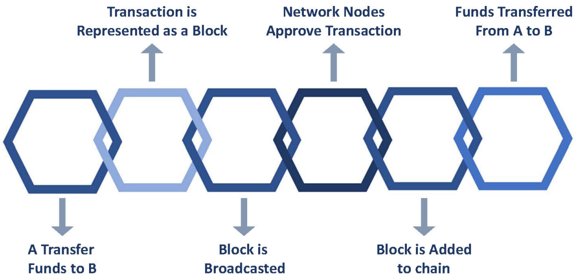

Transaction is Represented as a Block
Network Nodes Approve Transaction
Funds Transferred From A to B
A Transfer Funds to B
Block is Broadcasted
Block is Added to chain

FIGURE 15. Financial transaction using blockchain.

D. STOCK EXCHANGE/FINANCE

For successful and in time trades settling and clearing in securely fashion, stock exchanges list company shares. Theoretically, possibility does exist to transfer shares via the blockchain which can be purchased and sold in a secondary market that resides on top of blockchain. Figure 15 shows various steps involved in the transfer of funds using blockchain technology.

Famous organizations including overstock, Samsung, IBM, Amazon, Citi, Ebay, Verizon Wireless, UBS and many more are striving for new opportunities of utilizing blockchain in their domains [184]–[186]. Similarly, non-financial applications can be implemented through blockchain. As a result, proofs of health records, legal documents, payments, notary services, and marriage licenses in the blockchain can be effectively managed [14], [31]. Privacy can be maintained by storing digital signature of the asset rather than the asset itself.

E. SUPPLY-CHAIN

Crosby *et al.* [34] conducted a study of financial and non-financial sectors that have adopted blockchain and provides challenges faced by businesses in the current digital world. The merchants and consumers during businesses may come across problems wherein counterfeit products are sold. Imagine usage of blockchain which can perform role as a third party which possesses details of counterfeit and original products. The consumers using such services may purchase products with much ease. **BlockVerify** [187] can verify a number of products including electronic devices, pharmaceuticals,

TABLE 6. Comparison of traditional banking, internet finance, and blockchain businesses.

Parameters	Traditional Banking Business	Internet Finance Businesses	Blockchain Plus Banks
Customer Experience or Service	Uniform scenarios	Rich scenarios	Rich scenarios
Customer Experience	Poor customer experience	Good customer experience	Good customer experience
Personalize or Homogenous service	Homogenous service	Personalized service	Personalized service
Efficiency	Low	Low	High
Clearing Process	complex	complex	Distributed Ledger, easy
Inspection	Manual	Manual	Automated
Cost	High	High	Low
Centralization /Decentralization	Centralized	Centralized	Decentralized
Tampering	Possible	Possible	Distributed Ledger cannot be tampered
Safety	Poor	Poor	Good

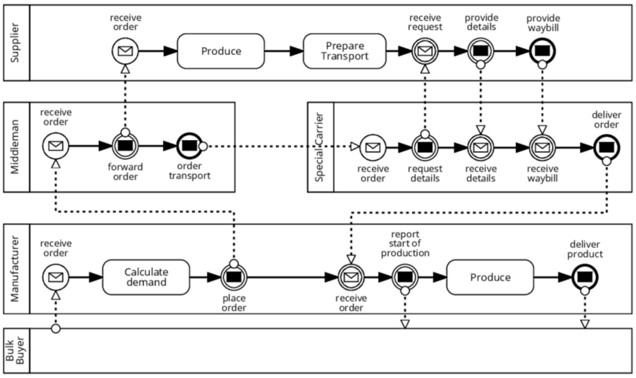


FIGURE 16. Supply chain scenario [3].

luxury items, diamonds, etc. DNS servers are currently controlled by governments and organizations. These servers are at risk as they are operated in centralized fashion where the system can be hijacked to observe the usage of the Internet by particular users. **NameCoin** [56], a fork of blockchain, is a distributed network that resolves such issues as users can have same phone-book on their computers. Blockchain has remained a best choice in the music industry as well. Writers, singers and other stakeholders involved in the music industry do utilize public ledger to store various information and have smart contracts. In order to ascertain possession of legal documents and properties, blockchain provides an online solution known as **Proof of Existence** [34]. It is pertinent to mention here that not the original item is stored rather fingerprint of the property is stored in the blockchain. Challenges do exist in collaborative business process execution as depicted in Figure 16.

There are at least five parties involved and challenges include placing of orders with manufacturer from the buyer, calculation of demand placement of order through a third party which forwards order to supplier and makes arrangement for transportation. In case of delays, the five parties involved usually blame each others. For example, if the manufacturer receives materials four days after the agreed date and refuses to accept the material then the transportation charges are at least needed to be paid; however, due to the lack of maintaining proper history of transactions, the same does not happen and the carrier is at risk. Weber *et al.* [3] proposed and developed a technique comprising of various components that integrates blockchain in the business processes to coordinate each other in a manner so that the central authority is not required and still the trust is maintained. They provided idea of using translators to translate business rules into smart contract for implementation using blockchain infrastructure. In order to connect with external world, triggers are utilized that acts as a bridge between blockchain and organization's private process implementation. A trigger converts API calls into transactions. The solution is evaluated through experiments and the creation of 500 smart contracts and the execution of over 8000 transactions to show the efficiency of the approach.

VI. BLOCKCHAIN IN VEHICULAR INDUSTRY

Automobile industry is also adopting blockchain technology due to its cutting edge benefits. Volkswagen has shown the use of IOTA Tangle system [188] for autonomous cars. BMW is using blockchain technology for managing its asset and logistics. BMW, Ford, Renault and General Motors are among the 30 companies in Mobility Open Blockchain Initiative (MOBI) along with IBM, Bosch and Blockchain at Berkeley. MOBI's mission is to accelerate the adoption of blockchain and to make sure that the industry is on the same page, not only by changing the mode of transportation, but also through use cases ranging from autonomous payment to ride sharing [189], [190]. Similarly, Toyota in investing in blockchain supply chain management since 2016 through R3CEV consortium [191].

Renault working on its car passport system based on blockchain [192] suggests Blockchain technology is also effective in tracking vehicles transporting goods. It will allow all stakeholders involved in transporting process to check

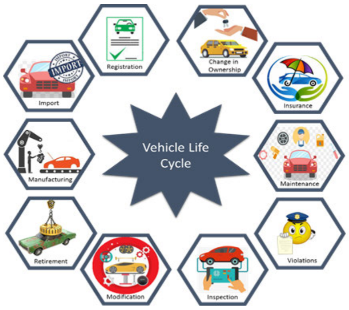


FIGURE 17. Vehicle life-cycle tracking.

relevant data and status while providing traceability and transparency. However, in best of our knowledge there is no work so far which uses blockchain technology for vehicle life cycle tracking. The authors of this paper are currently working on a project [193] related to implementing a blockchain based prototype system for vehicle life cycle tracking in Saudi Arabia. The project consists of designing and implementing a complete life cycle of vehicle tracking, starting from manufacturing, customs, registration, violations to buying and selling. We designed a secure and transparent architecture over selected blockchain platform(cf. Figure 17).

A. BENEFIT OF USING BLOCKCHAIN IN BUSINESS SECTOR/SUMMARY

Benefits of Implementation of Blockchain in Business Sector:

a. The blockchain stores status of process under execution across the involved participants and on the basis of stored information, it creates audit trails. As a result, automated payment can be managed and thus behaves as an active mediator for data transformation or calculation.

b. In order to interact with processes outside the blockchain environment, interfaces or triggers are utilized. They connect process within the blockchain to external world processes i.e. outside the blockchain. To impose security and integrity of contents, smart contracts are not allowed to directly interact with the world outside the blockchain. Triggers are utilized to act as agents of organization.

In a nutshell through the use of blockchains, all participants have the opportunity to execute collaborative processes over networks of nodes which are not trusted. Secondly, the state of processes is advanced based on the confirming messages. Third, funds and payments can be coded into the process and forth, a changeless ledger maintains log of transactions, which may not be successful.

B. BLOCKCHAIN APPLICATION SCENARIOS

Blockchain can turn as a fundamental innovation for efficient financial management in the business sector. Subsequently, given its impressive linger behind the FinTech 1.0, managing an account industry ought to use the benefits of its assets and size, with a specific end goal to effectively lead research and testing of blockchain applications. This will empower them to wind up the pioneers of technological applications that can lead and take an interest in the development of new business scenes.

Blockchain can set up credit components in situations where there is no shared trust among parties that introduce high costs induced by the unspecialized part of centralization. Money management procedures include issues, such as, productivity bottlenecks, exchange margins, fraud, and activity risks. Blockchain technologies can solve such problems by applying decentralized trust.

1) DISTRIBUTED CLEARING MECHANISM

Interbank transfer of funds regularly depend on handling by middle person clearing firms, which includes a progression of confounded procedures, including accounting, exchange balancing transactions, initialization of payments and so forth. In this way, the procedure included is extensive and exorbitant. Table 7 summarized various implementations of blockchain business.

VII. DISCUSSION AND FUTURE PROSPECTS

Centralized IoT network affected by traditional Botnets and other malware. Around two million devices,DNS services and others affected, in 2017 only, by Botnets of Things. That shows the IoT devices in the centralized network are not protected and vulnerable for tempering of data. Blockchain based solutions can provide security for data theft due to the inscripted transactions among the devices. Similarly, some IoT solutions are only utilizing the secure storage of blockchain which is its core characteristic of the blockchain. So, shifting completely to blockchain or partially, both provide strong benefits to the current security issues of centralized IoT network. So, in our recommendation is atleast partial adoption of blockchain will provide quick security to the existing IoT infrastructure.

Centralized IoT network faces high cost of server maintenance on a single body. According to the current statistics, the IoT device manufacturers keep very small margins. At the same time, plenty of investment is needed to serve hundreds of billions of smart devices. To reduce the cost of smart IoT devices, decentralized network can distribute cost on multiple stakeholders as well as better security, integrity and reliability of network will be provided. So, in all aspects, it is highly recommended to adopt blockchain as a future network infrastructure for IoT devices.

As a result of the thorough review, in this article, we realize the potential of blockchain technology in improving global healthcare data exchange and applications. After reviewing the solutions from both research community and industry in recent years, we believe this technology can address the major issues in improving global healthcare services around the world. However, we believe there are challenges in adaptation of blockchain technology in general. These adaption challenges will be the point of discussion in various forums in the next five years by all stakeholders including healthcare industries, research community, industry and major healthcare solution providers.

TABLE 7. Various implementation of blockchain for business & their comparison [179].

	Public blockchains	Consortium blockchains	Private blockchains
Cenralized/ Decentralized	Decentralized	Multi-centralized	Decentralized
Participants	Open	Specific group of people who agree to enter an alliance	Central controller decides members that can participate
Credit mechanism	Proof of work	Collective endorsement	Self-endorsement
Bookkeeper	All participants	Participants decide in negotiation	Self-determined
Incentive mechanism	Needed	Optional	Not needed
Prominent advantage	Self-established credit	Efficiency and cost optimization	Transparency and traceability
Typical application scenario	Bitcoin	Clearing	Audits
Load capacity	3-20 times/second	1000-10000 times/second	

Blockchain emerging technology in effectively been utilized in the businesses, finance, industries sectors. Its use cases as reported earlier are smart contracts, Ethereum, smart property which includes buying and selling of physical as well non-physical properties including cars, lands, buildings, transferring shares etc. Similarly, banking sector is investing resources to look for opportunities to utilize the features offered by blockchain and to effectively manage matters relating to finance and banking. Through the use of blockchain, stakeholders involved in the businesses have now to execute collaborative processes over networks of nodes while the distributed automated transfer of funds and clearing mechanism satiate the overall business activities and ensure the timely execution of processes. The distributed changeless ledger further imposes integrity of the contents as stored on the blockchain which is more appealing.

Here we highlight the future prospects of blockchain technology from various point of views, such as, in terms of its core architectures (in section II), its applications in IoT (described in section III), healthcare applications (discussed in section IV), and similarly, business related applications (as elaborated in section V).

Consensus algorithm plays a vital role in the core functionality of blockchain. A critical future prospects is the transition from Proof-of-Work to new consensus algorithm, its testing, implementation and performance analysis. Ethereum has initiated this work. In another aspects, research community will observe, ‘‘how enterprise blockchain and alliance will react and adopt new cryptocurrencies like NEM and EOS’’. As off now there are no software standards that define connectivity between IoT and blockchain. Authors in [194] suggested that an embedded wallet for IoT could solve this issue in the future application of blockchain in IoT. Blockchain can play a critical role in ensuring secure storage and sharing of information for smart cities and house in the future along with IoT technology. Blockchain technology has the potential to revolutionize the future of Global collaboration for effective Healthcare services around the world. The features of secure sharing and storage of data gives confidence to the users around the world to upload medical data for example DNA data. This will not only help the healthcare institutions but will also allow to create powerful data-sets for research community. Authors in [195] suggested that the most of the applications of blockchain in healthcare are short term projects focusing on healthcare consortium and drug supply chain. However, the long term applications focusing on universal identities and effective patient health record is yet to be investigated in future. Blockchain technology potential and existing applications in business have shown a new viewpoint of decentralized economical system in future. However, there are various hurdles and speculations about the limitation of this technology when it comes to adoption of this technology by the banking systems. Blockchain is consider as antithesis of central banking system due to the way it functions which is contradictory to conventional monetary polices. We believe study of possible legal framework and standards in future will certainly allow adoption of this technology in businesses and financial industry.

From security point of view, we think investigation of Distributed Ledger Technology (DLT) is required in terms of privacy and security of the individual node. We believe some other aspects, such as, process of standardization, legal issues, and rights of individuals and organizations will be investigated in the future.

VIII. CONCLUSION

There is continuous susceptible threats to integrity of personal sensitive data and other expensive resources in the hands of third parties. There are more chances that resources are misused. Best practices to effectively execute processes are more vital and essential to address issues during interoperability. The blockchain is receiving widespread acceptance and deployment throughout fields of interests where users do not trust third party and are always aware of data collection and its usage. Similarly, laws and regulations are enforced automatically through programming and the computationally tamper proof ledger acts as legal evidence for processing data. This paper provides a extensive details of various use cases of blockchains that could provide readers and researchers insight to further explore possibilities to work in the domains of IoT security, healthcare, business and many others, such as, vehicle tracking - real estate - Banking. Implementing blockchain in the healthcare can engage millions of healthcare practitioners and experts to share vast amount of healthcare data, identify and share new ways of curing and preventing diseases. Similarly, utilizing blockchain in IoT can significantly reduce cost and capacity constraints with more robust security. Addressing security concerns, through the blockchain malicious processes can be detected easily and prevented accordingly which is in contrast to previous solution which are susceptible to manipulation. Moreover, blockchain architectural designs do address issues like single point failure and provides features where many systems hold identical information.

ACKNOWLEDGMENT AND CONFLICT OF INTEREST

This work was supported by the Deanship of Research, Islamic University of Madinah, KSA, under the tamayyuz initiative Grant 25/ 40. The authors declares that there is no conflict of interest with any individual or organization regarding the study in this article. The study does not involve any experiments involving animal or human subjects. The authors declares the paper follows the general ethical guidelines.

REFERENCES

[1] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.

[2] A. Corvas. (2018). *Healthcare Related Blockchain Projects*. Accessed: Sep. 2018. [Online]. Available: https://github.com/acoravos/healthcare-blockchains

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

[4] K. J. O. Dwyer and D. Malone, "Bitcoin mining and its energy footprint," in *Proc. 25th IET Irish Signals Syst. Conf.*, Limerick, Ireland, 2014.

[5] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme, "Can we afford integrity by proof-of-work? Scenarios inspired by the bitcoin currency," in *The Economics of Information Security and Privacy*. Berlin, Germany: Springer, 2013, pp. 135–156.

[6] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proc. WEIS*, 2013, p. 11.

[7] (2018). *IBM Blockchain for Financial Services Means More Trust for All*. Accessed: Oct. 30, 2018. [Online]. Available: https://www.ibm.com/blockchain/industries/financial-services

[8] A. Baliga, "Understanding blockchain consensus models," *Persistent*, vol. 2017, no. 4, pp. 1–14, 2017.

[9] S. Popov, "The tangle," *Cit. On*, vol. 2017, p. 131, Oct. 2016.

[10] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 8, pp. 173–190, Nov. 2018.

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

[12] C. P. Transaction, "Blockchain: Opportunities for health care," Deloitte Touche Tohmatsu Ltd., London, U.K., Tech. Rep. 1, 2018.

[13] T. StClaire. (2018). *How Blockchain Can Solve Real Problems in Healthcare*. Accessed: Oct. 10, 2018. [Online]. Available: https://www.linkedin.com/pulse/how-blockchain-cansolve-real-problems-healthcare-tamara-stclaire

[14] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, vol. 13, Aug. 2016, p. 13.

[15] T. Ali, "Z notation formalization of blockchain healthcare document sharing based on crbac," *J. Inf. Commun. Technol. Robot. Appl.*, vol. 9, no. 1, pp. 16–29, Jun. 2018.

[16] TierIon. (2018). *TierIon: Technology and Products That Reduce the Cost and Complexity of Trust*. Accessed: Sep. 2018. [Online]. Available: https://tierion.com/

[17] GEMOS. (2018). *The Blockchain Operating System*. Accessed: Sep. 2018. [Online]. Available: https://enterprise.gem.co/

[18] B. Brannan. (2018). *Healthcoin—Blockchain-Enabled Platform for Diabetes Prevention*. Accessed: Aug. 2018. [Online]. Available: https://blockchainhealthcarereview.com/healthcoin-blockchain-enabled-platform-for-diabetes-prevention/

[19] F. Haidar, A. Kaiser, B. Lonc, P. Urien, and R. Denis, "C-its use cases: Study, extension and classification methodology," in *Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring)*, Porto, Portugal, 2018.

[20] Y. Xu, Q. Li, X. Min, L. Cui, Z. Xiao, and L. Kong, "E-commerce blockchain consensus mechanism for supporting high-throughput and real-time transaction," in *Proc. Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*. Beijing, China: Springer, 2016, pp. 490–496.

[21] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *Proc. IEEE 19th Int. Conf. High Perform. Comput. Commun., IEEE 15th Int. Conf. Smart City, IEEE 3rd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2017, pp. 466–473.

[22] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2018.

[23] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

[24] B. A. Tama, B. J. Kweka, Y. Park, and K.-H. Rhee, "A critical review of blockchain and its current applications," in *Proc. Int. Conf. Elect. Eng. Comput. Sci. (ICECOS)*, 2017, pp. 109–113.

[25] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of money," in *Banking Beyond Banks and Money*. Zürich, Switzerland: Springer, 2016, pp. 239–278.

[26] P. Kouvelis and G. J. Gutierrez, "The newsvendor problem in a global market: Optimal centralized and decentralized control policies for a two-market stochastic inventory system," *Manage. Sci.*, vol. 43, no. 5, pp. 571–585, 1997.

[27] S. Roy and P. Venkateswaran, "Online payment system using steganography and visual cryptography," in *Proc. IEEE Students' Conf. Elect., Electron. Comput. Sci.*, Mar. 2014, pp. 1–5.

[28] G. Wood, "Ethereum: A secure decentralized transaction ledger," Daniel D Wood (Self-published), Tech. Rep. EIP-150 REVISION (1e18248-2017-04-12), 2014.

[29] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2018.

[30] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in *Proc. 13th Work. IEEE/IFIP Conf. Softw. Archit. (WICSA)*, 2016, pp. 182–191.

[31] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?" UCL Centre Blockchain Technol., London, U.K., Tech. Rep. SSRN 2709713, 2015.

[32] I. Belle, "The architecture, engineering and construction industry and blockchain technology," in *Proc. Int. Conf. Digit. Archit.*, Nanjing, China, 2017, pp. 279–284.

[33] M. Pilkington, "11 blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. Cheltenham, U.K.: Edward Elgar Publishing, 2016, p. 225.

[34] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, pp. 6–10, Jun. 2016.

[35] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," Cryptocurrency Res. Group, Yeshiva Univ., New York, NY, USA, Tech. Rep. SSRN 2580664, 2015.

[36] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. 1st Workshop Syst. Softw. Trusted Execution*, 2016, p. 2.

[37] I. Abraham and D. Malkhi, "The blockchain consensus layer and BFT," *Bull. EATCS*, vol. 3, no. 123, pp. 1–23, 2017.

[38] G. Greenspan. (2015). *Multichain Private Blockchain-White Paper*. [Online]. Available: http://www.multichain.com/download/MultiChain-White-Paper.pdf

[39] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 310, pp. 1–4, 2016.

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

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

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

[43] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.* Zürich, Switzerland: Springer, 2015, pp. 112–125.

[44] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, Tech. Rep., 2014. [Online]. Available: http://www.bitcoin.org

[45] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—A systematic review," *PLoS ONE*, vol. 11, no. 10, 2016, Art. no. e0163477.

[46] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[47] S. Bragagnolo, H. Rocha, M. Denker, and S. Ducasse, "Smartinspect: Smart contract inspection technical report," Ph.D. dissertation, Dept. RMOD-Analyses, Lang. Constructs Object-Oriented Appl. Evol. Res. Team, Inria, Lille, France, 2017.

[48] C. P. Jiménez, "Analysis of the ethereum state," Universitat Oberta de Catalunya, Barcelona, Spain, Tech. Rep., 2017.

[49] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, and Y. Manevich, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, Art. no. 30. [Online]. Available: https://dl.acm.org/citation.cfm?id=3190538

[50] J. Kwon, *Tendermint: Consensus Without Mining*, document Draft v. 0.6, fall, 2014.

[51] C. Cachin, M. V. Sorniotti, and T. Weigold, "Blockchain, cryptography, and consensus," IBM Res., Zürich, Switzerland, Tech. Rep. 2016, 2016.

[52] Aran Davies, DevTeam.Space. (2018). *Pros and Cons of Hyperledger Fabric for Blockchain Networks*. Accessed: Aug. 12, 2018. [Online]. Available: https://www.devteam.space/blog/pros-and-cons-of-hyperledger-fabric-for-blockchain-networks/

[53] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, 2017, pp. 1–5.

[54] Verkkoaineisto. (2018). *Waltonchain White Paper*. [Online]. Available: https://www.waltonchain.org/doc/waltonchain-whitepaper_en_20180208.pdf

[55] D. Bradbury, "Bitcoin's successors: From litecoin to freicoin and onwards," *Guardian*, vol. 25, Jun. 2013. [Online]. Available: https://www.theguardian.com/technology/2013/jun/25/bitcoin-successors-litecoin-freicoin

[56] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design," in *Proc. WEIS*, 2015, pp. 1–21.

[57] P. Vasin. *Blackcoin's Proof-of-Stake Protocol V2*. (2014). [Online]. Available: https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf

[58] A. Poelstra, "Distributed consensus from proof of stake is impossible," Blockstream, Austin, TX, USA, Self-Published Paper 1, 2014.

[59] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.* Santa Barbara, CA, USA: Springer, 2017, pp. 357–388.

[60] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.* Lyon, France: Springer, 2017, pp. 282–297.

[61] W. Wang, D. T. Hoang, Z. Xiong, D. Niyato, P. Wang, P. Hu, and Y. Wen, "A survey on consensus mechanisms and mining management in blockchain networks," 2018, *arXiv:1805.02707*. [Online]. Available: https://arxiv.org/abs/1805.02707

[62] K. Driscoll, B. Hall, M. Paulitsch, P. Zumsteg, and H. Sivencrona, "The real byzantine generals," in *Proc. 23rd Digit. Avionics Syst. Conf. (DASC)*, vol. 2, 2004, p. 6-D.

[63] K. Driscoll, B. Hall, H. Sivencrona, and P. Zumsteg, "Byzantine fault tolerance, from theory to reality," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Edinburgh, U.K.: Springer, 2003, pp. 235–248.

[64] R. Zurawski, "Industrial communication technology handbook," in *Industrial Information Technology*. Boca Raton, FL, USA: CRC Press, 2017. [Online]. Available: https://books.google.com.pk/books?id=ppzNBQAAQBAJ

[65] Y. C. Yeh, "Safety critical avionics for the 777 primary flight controls system," in *Proc. 20th Digit. Avionics Syst. Conf. (DASC)*, vol. 1, Oct. 2001, pp. 1C2-1–1C2-11.

[66] Statista. (2018). *Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025 (in Billions)*. Accessed: Sep. 2018. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[67] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[68] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[69] K. Prabhu and K. Prabhu, "Converging blockchain technology with the Internet of Things," *Int. Edu. Res. J.*, vol. 3, no. 2, pp. 122–123, 2017.

[70] U. Trust IoT Alliance. (2018). *Trusted IoT Alliance*. Accessed: Oct. 10, 2018. [Online]. Available: https://www.trusted-iot.org/

[71] T. L. Foundation. (2018). *The Hyperledger*. Accessed: Sep. 2018. [Online]. Available: https://www.hyperledger.org

[72] EthEmbeded. (2018). *Ethereum Computer Built on Embedded Devices*. Accessed: Sep. 2018. [Online]. Available: http://ethembedded.com/

[73] Lo3Energy. (2018). *Reshaping the Energy Future*. Accessed: Sep. 2018. [Online]. Available: https://lo3energy.com/

[74] H. K. Chain of Things Limited. (2018). *Chain-of-Things*. Accessed: Oct. 10, 2018. [Online]. Available: https://www.chainofthings.com/

[75] IoTex Blockchain for IoT. (2018). *IoTex*. Canada. Accessed: Oct. 10, 2018. [Online]. Available: https://iotex.io/

[76] Raspnode. (2018). *DIY Raspberry Pi Cryptocurrency Node*. Accessed: Sep. 2018. [Online]. Available: http://raspnode.com/

[77] M. Atzori, "Blockchain-based architectures for the Internet of Things: A survey," UCL Centre Blockchain Technol., London, U.K., Tech. Rep. SSRN 2846810, 2017.

[78] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov./Dec. 2016, pp. 1–6.

[79] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-iot: Hybrid blockchain architecture for Internet of Things-pow sub-blockchains," 2018, *arXiv:1804.03903*. [Online]. Available: https://arxiv.org/abs/1804.03903

[80] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for ble-based devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.

[81] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," *Int. J. Intell. Syst. Appl.*, vol. 10, no. 6, pp. 40–48, 2018.

[82] V. Skwarek, "Blockchains as security-enabler for industrial iot-applications," *Asia Pacific J. Innov. Entrepreneurship*, vol. 11, no. 3, pp. 301–311, 2017.

[83] D. Miller, "Blockchain and the Internet of Things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 15–18, 2018.

[84] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, p. 533, 2016.

[85] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," IET, London, U.K., Tech. Rep. CP740, 2018.

[86] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw. (ICIN)*, 2015, pp. 184–191.

[87] M. Samaniego and R. Deters, "Internet of smart things-ioST: Using blockchain and clips to make things autonomous," in *Proc. IEEE Int. Conf. Cognit. Comput. (ICCC)*, Jun. 2017, pp. 9–16.

[88] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 464–467.

[89] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[90] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and privacy," 2017, *arXiv:1712.02969*. [Online]. Available: https://arxiv.org/abs/1712.02969

[91] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[92] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in iot," in *Proc. Eur. MENA Cooperation Adv. Inf. Commun. Technol.* Springer, 2017, pp. 523–533.

[93] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Global Internet Things Summit*. New York, NY, USA: IEEE Press, 2017, pp. 1–6.

[94] (2018). *Chain of Things*. Accessed: Sep. 2018. [Online]. Available: https://www.blockchainofthings.com/

[95] (2018). *Filament*. Accessed: Sep. 2018. [Online]. Available: https://filament.com/

[96] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," *Secur. Commun. Netw.*, vol. 2018, no. 1, pp. 1–11, 2018, Art. no. 7817614.

[97] P. Otte, M. de Vos, and J. Pouwelse, "Trustchain: A sybil-resistant scalable blockchain," in *Future Generation Computing Systems*. Rio de Janeiro, Brazil: Elsevier 2017.

[98] (2018). *My Bit*. Accessed: Sep. 2018. [Online]. Available: https://mybit.io/

[99] Aigang. (2018). *Autonomous Insurance Network—Fully Automated Insurance for IoT Devices*. Accessed: Oct. 10, 2018. [Online]. Available: https://aigang.network/

[100] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[101] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 2017, pp. 1–13, Aug. 2017.

[102] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, 2018.

[103] E. F. Jesus, V. R. Chicarino, C. V. de Albuquerque, and A. A. D. A. Rocha, "A survey of how to use blockchain to secure Internet of Things and the stalker attack," *Secur. Commun. Netw.*, vol. 2018, no. 1, pp. 1–27, 2018, Art. no. 9675050.

[104] S. Gan, "An IoT simulator in ns3 and a key-based authentication architecture for IoT devices using blockchain," Ph.D. dissertation, Dept. Comput. Sci. Eng., Indian Inst. Technol., Kanpur, India, Jul. 2017.

[105] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, and F. Zanichelli, "IoTChain: A blockchain security architecture for the Internet of Things," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[106] (2018). *Modum*. Accessed: Sep. 2018. [Online]. Available: https://modum.io/

[107] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for Internet of Things using blockchain technology," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, 2018, pp. 769–773.

[108] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 261–266.

[109] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Jun. 2017, pp. 468–475.

[110] P. Ghuli, U. P. Kumar, and R. Shettar, "A review on blockchain application for decentralized decision of ownership of iot devices," *Adv. Comput. Sci. Technol.*, vol. 10, no. 8, pp. 2449–2456, 2017.

[111] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for IoT updates by means of a blockchain," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2017, pp. 50–58.

[112] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, "Semantic blockchain to improve scalability in the Internet of Things," *Open J. Internet Things*, vol. 3, no. 1, pp. 46–61, 2017.

[113] G. Prisco. (2016). *Slock. it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy*. Bitcoin Magazine. Accessed: May 20, 2016. [Online]. Available: https://bitcoinmagazine.com/articles/sloc-itto-introduce-smart-locs-lined-to-smart-ethereum-contractsdecentralizethe-sharing-economy-1446746719

[114] R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, 2017, p. 14.

[115] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput.*, May 2017, pp. 468–477.

[116] A. Ramachandran and D. Kantarcioglu, "Using blockchain and smart contracts for secure data provenance management," 2017, *arXiv:1709.10000*. [Online]. Available: https://arxiv.org/abs/1709.10000

[117] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intell. Syst. Accounting, Finance Manage.*, vol. 25, no. 1, pp. 18–27, Jan. 2018.

[118] (2017). *Chronicled*. Accessed: Sep. 2018. [Online]. Available: https://chronicled.com/

[119] Grid. (2018). *Building a Robust Value Mechanism to Facilitate Trans-Active Energy*. Accessed: Feb. 2018. [Online]. Available: https://exergy.energy/wp-content/uploads/2017/12/Exergy-Whitepaper-v8.pdf

[120] M. S. Ali, K. Dolui, and F. Antonelli, "IoT data privacy via blockchains and IPFS," in *Proc. 7th Int. Conf. Internet Things*, 2017, p. 14.

[121] M. Samaniego and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Dec. 2016, pp. 433–436.

[122] L. Zhou, L. Wang, Y. Sun, and P. Lv, "Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

[123] T. McConaghy, A. Marques, Rodolphe, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, "BigChainDB: A scalable blockchain database," BigChainDB, ascribe GmbH, Berlin, Germany, White Paper 1.0, 2016.

[124] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in *Proc. Cloud Comput. Secur. Workshop*, 2017, pp. 45–50.

[125] Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong, "A blockchain-based storage system for data analytics in the Internet of Things," in *New Advances in the Internet of Things*. Zürich, Switzerland: Springer, 2018, pp. 119–138.

[126] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," 2016, *arXiv:1608.05187*. [Online]. Available: https://arxiv.org/abs/1608.05187

[127] R. B. Chakraborty, M. Pandey, and S. S. Rautaray, "Managing computation load on a blockchain–based multi–layered Internet–of–Things network," *Proc. Comput. Sci.*, vol. 132, no. 2018, pp. 469–476, May 2018.

[128] M. Samaniego and R. Deters, "Hosting virtual iot resources on edge-hosts with blockchain," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Dec. 2016, pp. 116–119.

[129] M. Bafandehkar, S. M. Yasin, R. Mahmod, and Z. M. Hanapi, "Comparison of ECC and RSA algorithm in resource constrained devices," in *Proc. Int. Conf. IT Converg. Secur. (ICITCS)*, Dec. 2013, pp. 1–3.

[130] N. Fabiano, "The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard," in *Proc. Int. Conf. Internet Things Global Community (IoTGC)*, Jul. 2017, pp. 1–7.

[131] P. Veena, S. Panikkar, S. Nair, and P. Brody, "Empowering the edge-practical insights on a decentralized Internet of Things," in *Empowering the Edge-Practical Insights on a Decentralized Internet of Things*, vol. 17. Armonk, NY, USA: IBM Institute for Business Value, 2015.

[132] B. Fog. (2018). *Accessing Bitcoin Fog*. Accessed: Sep. 2018. [Online]. Available: http://bitcoinfog.info/

[133] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. 2nd Int. Conf. Internet Things Design Implement.*, 2017, pp. 173–178.

[134] H. Malviya, "How blockchain will defend IoT," Self-published, India, Tech. Rep. SSRN 2883711, 2016.

[135] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of Things, blockchain and shared economy applications," *Proc. Comput. Sci.*, vol. 98, pp. 461–466, Sep. 2016.

[136] L. Carpio, "Blockchain in healthcare: Complex challenges, overshadowed by the hype, need to be overcome," DataArt, Corrientes, Argentina, Tech. Rep. 2018, 2018.

[137] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, Apr. 2019.

[138] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.

[139] D. Bender and K. Sartipi, "HL7 FHIR: An Agile and RESTful approach to healthcare information exchange," in *Proc. 26th IEEE Int. Symp. Comput.-Based Med. Syst. (CBMS)*, Jun. 2013, pp. 326–331.

[140] T.-T. Kuo and L. Ohno-Machado, "Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," 2018, *arXiv:1802.01746*. [Online]. Available: https://arxiv.org/abs/1802.01746

[141] PROOF. (2018). *Prove the Integrity and Timestamp of Data Without Depending on a Trusted Third-Party*. Accessed: Sep. 2018. [Online]. Available: https://tierion.com/proof/

[142] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.

[143] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, p. 130, Jul. 2018.

[144] L. Zhou, L. Wang, and Y. Sun, "Mistore: A blockchain-based medical insurance storage system," *J. Med. Syst.*, vol. 42, no. 8, p. 149, 2018.

[145] J. Breteau. (2019). *The Future of Blockchain in Health Insurance*. Accessed: Oct. 2, 2019. [Online]. Available: https://www.the-digital-insurer.com/future-blockchain-health-insurance/

[146] A. Juneja and M. Marefat, "Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification," in *Proc. IEEE EMBS Int. Conf. Biomed. Health Informat. (BHI)*, Mar. 2018, pp. 393–397.

[147] R. Singer. (2018). *Blockchain For Health Research*. Accessed: Sep. 2018. [Online]. Available: https://www.blockchainhealth.co/

[148] A. Iyengar, A. Kundu, U. Sharma, and P. Zhang, "A trusted healthcare data analytics cloud platform," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2018, pp. 1238–1249.

[149] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability in blockchain-based healthcare apps," 2017, *arXiv:1706.03700*. [Online]. Available: https://arxiv.org/abs/1706.03700

[150] L. Parker. (2018). *GARTNER Puts Blockchain at the Peak of Inflated Expectations, While Bitcoin Slides Into the Trough of Disillusionment*. Accessed: Sep. 2018. [Online]. Available: https://bravenewcoin.com/Cnews/gartners-puts-blockchain-at-the-peak-of-inflated-expectations-while-bitcoin-slides-into-the-trough-of-disillusionment/

[151] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3.

[152] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *Proc. ONC/NIST Use Blockchain Healthcare Res. Workshop*. Gaithersburg, MD, USA: ONC/NIST, 2016, pp. 1–11.

[153] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM)*, Jun. 2016, pp. 1–6.

[154] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 4182–4191.

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

[156] B. Scott, "How can cryptocurrency and blockchain technology Play a role in building social and solidarity finance?" UNRISD Work. Paper, Geneva, Switzerland, Tech. Rep. 2016-1, 2016.

[157] I. Eyal, "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.

[158] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harvard Bus. Rev.*, vol. 1, no. 9, pp. 2–5, 2017.

[159] A. Cohn, T. West, and C. Parker, "Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids," *Georgetown Law Technol. Rev.*, vol. 1, no. 2, pp. 273–304, 2017.

[160] I. Nath, "Data exchange platform to fight insurance fraud on blockchain," in *Proc. IEEE 16th Int. Conf. Data Mining Workshops (ICDMW)*, Dec. 2016, pp. 821–825.

[161] F. Lamberti, V. Gatteschi, C. Demartini, C. Pranteda, and V. Santamaria, "Blockchain or not blockchain, that is the question of the insurance and other sectors," *IT Prof.*, vol. 2017, p. 1, Jun. 2017.

[162] K. Sadouskaya, "Adoption of blockchain technologyin supply chain and logistics," Finnish Univ. Appl. Sci., Lappeenranta, Finland, Tech. Rep. 2017(4), 2017.

[163] A. Badzar, "Blockchain for securing sustainable transport contracts and supply chain transparency-an explorative study of blockchain technology in logistics," LUND Univ., Lund, Sweden, Tech. Rep. 8880383, 2016.

[164] M. Petersen, N. Hackius, and B. von See, "Mapping the sea of opportunities: Blockchain in supply chain and logistics," Walter de Gruyter, Berlin, Germany, Tech. Rep. 5(6), Sep. 2017.

[165] A. Castor. (2017). *A (Short) Guide to Blockchain Consensus Protocols*. [Online]. Available: http://www.coindesk.com/short-guide-blockchain-consensus-protocols

[166] D. Evans, "Economic aspects of bitcoin and other decentralized public-ledger currency platforms," Univ. Chicago, Chicago, IL, USA, Tech. Rep. 685, 2014.

[167] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," in *Proc. 1st Italian Conf. Cybersecur. (ITASEC)*, Venice, Italy, 2017.

[168] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.

[169] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum, White Paper 3, 2014. [Online]. Available: http://www.ethereum.org

[170] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Christ Church, Barbados: Springer, 2016, pp. 79–94.

[171] Y. Zhang, R. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets," *IEEE Trans. Dependable Secure Comput.*, to be published.

[172] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: Platforms, applications, and design patterns," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Sliema, Malta: Springer, 2017, pp. 494–509.

[173] Y. Zhang, R. Deng, X. Liu, and D. Zheng, "Outsourcing service fair payment based on blockchain and its applications in cloud computing," *IEEE Trans. Services Comput.*, to be published.

[174] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Inf. Sci.*, vol. 462, pp. 262–277, Jun. 2018.

[175] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," Ph.D. dissertation, Dept. Sustain. Develop., Columbia Univ., New York, NY, USA, 2015, vol. 10.

[176] I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, "Design of the blockchain smart contract: A use case for real estate," *J. Inf. Secur.*, vol. 9, no. 3, p. 177, 2018.

[177] A. Spielman, "Blockchain: Digitally rebuilding the real estate industry," Ph.D. dissertation, Dept. Urban Stud. Center Real Estate, Massachusetts Inst. Technol., Cambridge, MA, USA, 2016.

[178] J. Veuger, "Trust in a viable real estate economy with disruption and blockchain," *Facilities*, vol. 36, nos. 1–2, pp. 103–120, 2018.

[179] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innov.*, vol. 2, no. 1, p. 24, 2016.

[180] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Mar. 2017.

[181] M. Mainelli and A. Milne, "The impact and potential of blockchain on the securities transaction lifecycle," Swift Inst., London, U.K., Tech. Rep. 2015-007, 2016.

[182] H. Leinonen, "Decentralised blockchained and centralised real-time payment ledgers: Development trends and basic requirements," in *Transforming Payment Systems in Europe*. Zürich, Switzerland: Springer, 2016, pp. 236–261.

[183] M. Mainelli and M. Smith, "Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology)," *J. Financial Perspect.*, vol. 3, no. 5, 2015.

[184] K. Heires, "The risks and rewards of blockchain technology," *Risk Manage.*, vol. 63, no. 2, pp. 4–7, 2016.

[185] M. Hooper, "Top five blockchain benefits transforming your industry," *IBM Blockchain*, vol. 2018, Feb. 2018. [Online]. Available: https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/

[186] P. Rimba, A. B. Tran, I. Weber, M. Staples, A. Ponomarev, and X. Xu, "Comparing blockchain and cloud services for business process execution," in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, Apr. 2017, pp. 257–260.

[187] G. Caglar and Y. S. Hanay, "Blockchain: Vision and challenges," *Newsletter*, vol. 2017, Sep. 2016. [Online]. Available: https://internetinitiative.ieee.org/newsletter/september-2017/blockchain-vision-and-challenges

[188] S. Town. (2019). *IOTA and Volkswagen Will Launch Blockchain-Enabled Cars in 2019*. Accessed: Oct. 2, 2019. [Online]. Available: https://cryptoslate.com/iota-and-volkswagen-will-launch-blockchain-enabled-cars-in-2019/

[189] N. Maslova, "Blockchain: Disruption and opportunity," *Strategic Finance*, vol. 100, no. 1, pp. 24–30, 2018.

[190] M. Community. (2019). *Mobility Open Blockchain Initiative*. Accessed: Oct. 2, 2019. [Online]. Available: https://www.dlt.mobi/

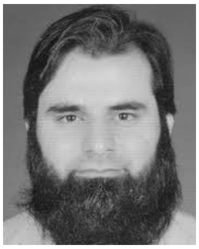
[191] H. Peter and A. Moser, "Blockchain-applications in banking & payment transactions: Results of a survey," *Eur. Financial Syst.*, vol. 2, no. 24, p. 141, 2017.

[192] K. L. Brousmiche, A. Durand, T. Heno, C. Poulain, A. Dalmieres, and E. B. Hamida, "Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul./Aug. 2018, pp. 1281–1286.

[193] T. Ali, A. Nadeem, M. Shoaib, M. Nauman, and A. Alzahrani. (2019). *Blockchain-Based-Vehicle-Life-Cycle-Tracking-System*. Accessed: Oct. 2, 2019. [Online]. Available: https://www.researchgate.net/project/Blockchain-Based-Vehicle-Life-Cycle-Tracking-System

[194] A. Hauser. (2019). *What is the Future of Internet of Things (IoT)—Blockchain*. Accessed: Sep. 20, 2019. [Online]. Available: https://dataconomy.com/2018/10/what-is-the-future-of-internet-of-things-iot-blockchain

[195] Cbinsights. (2019). *How Blockchain Technology Could Disrupt Healthcare*. Accessed: Sep. 25, 2019. [Online]. Available: https://www.cbinsights.com/research/report/blockchain-technology-healthcare-disruption



TOQEER ALI SYED received the master's degree in computer sciences and the Ph.D. degree in engineering technology (IT) from University Kuala Lumpur, in 2014. He was a Senior Lecture with University Kuala Lumpur for two years. He is currently an Associate Professor with the Islamic University of Madinah, KSA. He is a professional, Teacher and a Researcher working in the field of system security, deep learning, blockchain applications and cloud computing. He has been actively involved in research and teaching activities, since last ten years. He has published his research findings in several forums of international repute.

ALI ALZAHRANI is currently an Associate Professor and the Dean of the Faculty of Computer and Information Systems, Islamic University, Madinah, KSA. His research interests include computer security, distributed systems, the IoT, and blockchain.

SALMAN JAN received the master's degree in computer science from the University of Peshawar and the Ph.D. degree from the University of Kuala Lumpur, in 2019. He is working in the area of information security, especially in Android malware analysis and its blockchain integration. He has also experience in deep learning models to detect threats in various Android's application dataset.

MUHAMMAD SHOAIB SIDDIQUI received the B.S. degree from the Department of Computer Sciences, University of Karachi, in 2004, and the M.S. and Ph.D. degrees in computer engineering from Kyung Hee University, South Korea, in 2008 and 2012, respectively. His research interests include routing, security, and management in wireless networks, IP traceback, and remote monitoring using the IoT. He is a member of ACM.

ADNAN NADEEM received the Ph.D. degree from the Institute for Communication Systems, U.K., in 2011. He has been an Associate Professor with the Faculty of Computer and Information System (FCIS), Islamic University in Madinah, KSA, since 2016. He is also with the Federal Urdu University of Arts Science and Technology, Pakistan. During this period, he earned several research grants. He has published more than 50 articles in international conference and journals, and completed several funded research projects. He has mainly work on network layer security, QoS and reliability issues of mobile Ad Hoc and sensors networks. He is currently focusing on blockchain technology applications. He received the 5th HEC Outstanding Research Award 2013/14 for his article published in the IEEE COMMUNICATION SURVEY AND TUTORIALS (I.F = 20.30). During his pedagogical journey, he has received several awards and achievements, including the Foreign Ph.D. scholarship, Associate Fellowship of Higher Education Academy (AFHEA), U.K., in 2009, and the Best Paper and Best Track Paper Award in the ICICTT 2013 and ICEET 2016 conferences, respectively. He received Nishan-e-Imtiaz for his outstanding research from Federal Urdu University, Pakistan, in August 2016. He received the Best Academic Advisor and Best Researcher Award from FCIS, Islamic University of Madinah, in 2018.

TURKI ALGHAMDI received the B.Sc. degree in computer science from Taif University, KSA, in 2005, the M.Sc. degree in software engineering from the University of Bradford, U.K., in 2008, and the Ph.D. degree in software engineering from De Montfort University, U.K., in 2012. He is currently an Associate Professor with the Faculty of Computer and Information Systems, Islamic University in Madinah, KSA, where he was the Dean and the Founder.

• • •