IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 August 2022, accepted 15 September 2022, date of publication 22 September 2022, date of current version 5 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3208688

SURVEY

Survey on Blockchain-Based IoT Payment and Marketplaces

AMILA SAPUTHANTHRI[1], **(Member, IEEE), CHAMITHA DE ALWIS**[1], **(Senior Member, IEEE), AND MADHUSANKA LIYANAGE**[2,3], **(Senior Member, IEEE)**
[1]Department of Electrical and Electronic Engineering, University of Sri Jayewardenepura, Nugegoda 10250, Sri Lanka
[2]Center for Wireless Communications, University of Oulu, 90570 Oulu, Finland
[3]School of Computer Science, University College Dublin, D04 V1W8 Dublin, Ireland

Corresponding author: Madhusanka Liyanage (madhusanka.liyanage@oulu.fi)

This work was supported in part by the Academy of Finland under 6Genesis Flagship under Grant 318927, and in part by the Science Foundation Ireland under the CONNECT Center under Project 13 RC/2077_P2.

ABSTRACT The ever-growing smart applications will expand the Internet of Things (IoT) ecosystem to connect over 75 billion devices by 2025. IoT ecosystems comprise sensors that act as data suppliers and applications where monetary transactions are required to compensate the data producers. This signifies the importance of IoT payments and marketplaces to facilitate micro-transactions of billions of connected devices in the IoT ecosystem, which is heterogeneous, decentralized, and diverse. However, realizing such an ecosystem raises multiple challenges such as overcoming poor inter-operability, resource constraints, and security and privacy vulnerabilities of IoT devices and platforms. Blockchain is a Distributed Ledger Technology (DLT) that can be identified as a potential solution to overcome the challenges in realizing IoT payments and marketplaces. This is due to the characteristics of blockchain such as decentralization, traceability, immutability, and non-repudiation. This paper presents a comprehensive survey on blockchain-based IoT payments and marketplaces. This paper provides a brief introduction to the concepts of IoT payments and IoT marketplaces. Then the technical challenges involved in realizing IoT payment and marketplaces are discussed by highlighting the blockchain-based solutions. Furthermore, blockchain-based smart applications which use IoT marketplace and IoT payment concepts are presented marking the role of blockchain in each of the application. Subsequently, the paper discuss the integration challenges while also highlighting possible solutions. It is envisaged that this paper would shed light on the development of blockchain-based solutions to realize IoT payments and marketplaces.

INDEX TERMS Internet of Things, IoT payment, IoT marketplace, blockchain, smart contracts, decentralization.

I. INTRODUCTION

The number of devices connected to the Internet of Things (IoT) is expected to grow beyond 75 billion by 2025, recording an increase of more than 50 billion devices within the next five years [1]. Internet-connected devices communicating with each other were initially referred to as Machine to Machine (M2M) communication-based device networks [2]. These M2M networks have evolved towards IoT connecting heterogeneous devices that can communicate with each other using various protocols over the internet to exchange a wide range of information [3], [4], [5], [6]. IoT is further enhanced together with the dawn of the Internet of Everything (IoE), which facilitates the interactions among people, devices, and data [7], [8], [9].

The world is experiencing the 4th industrial revolution together with the advancements in IoT and Information and Communication Technologies (ICT) [10], [11]. Moreover, recent developments in 5G mobile communication also facilitates the development of IoT through ultra-Reliable-Low-Latency-Communication (uRLLC) and massive Machine-Type-Communication (mMTC) [6], [12],

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

TABLE 1. Summary of Important Acronyms.

Acronym	Definition
5G	Fifth Generation
AI	Artificial Intelligence
AV	Autonomous Vehicles
BDA	Big Data Analytics
BP	Block Producers
BTU	Bitcoin Unlimited
DAG	Directed Acyclic Graphs
DLT	Distributed Ledger Technique
DPoS	Delegated Proof-of-Stake
DS	Double Spending
DSO	Distribution System Operator
EHR	Electronic Health Records
ESS	Energy Storage System
HPBC	High-Performance Blockchain Consensus
ICT	Information and Communication Technologies
IoE	Internet of Every-things
IoT	Internet of Things
IoV	Internet of Vehicles
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LN	Lightning Network
M2M	Machine-to-Machine
M2P	Machine-2-Peer
ML	Machine Learning
mMTC	massiveMachine-Type-Communication
P2P	Peer to Peer
PKI	Public Key Infrastructure
PoS	Proof-of-Stake
PoW	Proof of Work
SCC	Storage Compression Consensus
uRLLC	ultra-reliable-Low-Latency-Communication

[13], [14], [15]. Therefore, IoT enabled smart industries are expected to exhibit an exponential growth [16], [17].

The conventional computer-aided industries are getting converted into smart industries due to various reasons such as better quality and productivity, security issues of existing solutions, and ultimately the disruptive nature of smart solutions. So, the industries that become intelligent by adapting smart solutions will evolve while the others will not be able to cope up with the disruptive nature of the smart industries. These smart industries make data driven decision making based on IoT and Big Data Analytics (BDA) concepts [18]. IoT application areas such as agriculture, utilities, healthcare and transportation are expected to be converted into smart IoT applications [19]. Sensor networks have automated and improved the efficiency of agricultural practices [20]. Smart city concept will be supported by the utility meters which will be deployed worldwide as smart IoT systems. Smart healthcare systems will utilize latest technological advancements to perform critical remote surgeries as well. Connected cars is the next revolution in transportation sector.

A. BACKGROUND

Blockchain is a widely used DLT that is decentralized in nature and continuously grows along with the executed transactions. When a transaction is executed, a new block creation request is initiated. Then, all the nodes in the blockchain network initiate the process of block validation, A validated block will be added to the end of the blockchain by inverse reference pointing to the parent block. This block validation process prevents any alterations to the existing blocks in the blockchain as the malicious party needs to change the relevant block of each node in the network. The key characteristics of blockchain such as decentralization, immutability, trustworthiness, and non-repudiation have made it an ideal candidate for applications that require secure but anonymous and immutable transactions [21]. Due to these characteristics, blockchains have the potential to mitigate the existing issues and revolutionize IoT payments and IoT marketplace concept.

- **IoT payments** - Due to the distributed nature of blockchain technologies, P2P transactions without third-party involvement can be performed. Therefore, the bottleneck of having a central authority due to its cost and performance issues can be mitigated by validating the transactions by a decentralized mechanism. Individual nodes in the blockchain keeps all the committed transaction details and its immutable. The cryptographic mechanisms in blockchain guarantee the integrity and enable secure payments. Also it helps with other issues caused by third parties in IoT financial transactions, namely the lack of anonymity for the users and additional security risks.
- **IoT marketplace** - Global IoT data market value will reach over USD 1 trillion by 2026 [22]. There are several IoT data marketplaces that have already been deployed for selling and buying IoT data. But, the unique characteristics of IoT data have created technical challenges for the success of those platforms. A neutral platform that can be trusted by both the data suppliers and the consumers is essential for the success of IoT market. Blockchain can be used as the base technology to create such a digital trading platform. Further, it can allow IoT device owners to monetize any transaction or exchange data among the devices as a reward instead of a monetary transaction.

The use of third parties for IoT-related financial transactions creates issues such as lack of anonymity and security concerns. When the growing hacking attempts on internet-based platforms are considered, users don't prefer to share their credit card information or storing their transactions history in IoT marketplaces. When a third party is involved, it leads to an increased transaction fee, also. This is a major concern considering the small-scale micro-transactions that occur in IoT systems. We can use blockchain-based platforms to develop anonymous solutions and remove third parties involved in centralized systems. On the other hand, transaction fees can be an issue in blockchain technology as well. But, the research community is attempting various mechanisms to resolve this issue using the latest DLTs.

The data generated by IoT are tradeable assets that can be even sold to third-party buyers as well. The traditional marketplaces are generally used to share static data. But, the IoT ecosystem requires near-real-time data streams to utilize

TABLE 2. Summary of important surveys on IoT payments and Marketplaces.

Ref.	Technical Challenges of IoT Market Places	Technical Challenges of IoT Payment	Blockchain-based IoT Market Places	Blockchain-based IoT Payment	Blockchain-based IoT Application	Blockchain Implementation Challenges	Future Directions	Remarks
[23]	M	L	M	L	H	L	M	A survey on the IoT marketplace for smart IoT solutions, relevant application domains and the technologies used.
[24]	M	M	L	L	H	L	M	A review on the use of blockchain for IoT.
[21]	M	M	L	L	H	H	L	A survey on blockchain for IoT and introduces a proposal for a BCoT architecture to converge blockchain and IoT.
[25]	L	M	L	H	L	M	L	A survey on IoT payment systems highlighting the blockchain-based solutions and its limitations.
[26]	L	L	L	L	M	L	M	A survey of IoT security challenges and blockchain solutions to address them.
[27]	L	L	L	L	L	H	M	A detailed analysis of security concerns of blockchain and existing solutions to address the issues.
This	H	H	H	H	H	H	H	This survey .

L Low Coverage   M Medium Coverage   H High Coverage

its actual potential. It requires efficient ways to avoid the initial data consumers from reselling the data without the consent of the data supplier as well. Therefore, mutual trust will be a key component in the IoT marketplace and dynamic trade agreements are required among the parties. The IoT marketplaces do not always consist of trusted parties and smart contracts can be used as a trusted intermediary to create reliable transactions. Datum [28] is a smart contract-based blockchain that provides an option to securely store structured data in decentralized storage. But, this doesn't address the real-time data requirement of IoT applications. Any IoT data producer should be able to trade the generated data in an IoT marketplace [29].

Blockchain is an ideal candidate to address many of the unique challenges observed in the IoT domain [30]. But, there are obstacles that blockchains in IoT implementation should overcome to be the paradigm shift in the IoT domain. The need to pay a transaction fee to reward miners for their time and efforts is a major obstacle. The market-based transaction fees concept used in typical cryptocurrencies is quite expensive and not suitable for IoT transactions. The transaction time of blockchains is another problematic issue. IoT payment systems require many microtransactions to be completed within seconds. But, public blockchains such as Bitcoin, Ethereum and Ripple require each block be validated by the global blockchain [25]. Bitcoin Lightning Network (BLN), virtualized DLTs (vDLTs) and alternative DLT technologies such as Directed Acyclic Graphs (DAGs) are some examples for research attempts to improve blockchain technology to make it suitable for IoT applications. Even though blockchain needs further optimizations to make it an ideal IoT payment and marketplace platform, the already available research results indicate that blockchain based IoT payment and marketplace concepts can revolutionize the IoT ecosystem.

B. MOTIVATION

As per the summary of surveys given in Table 2, already available surveys discussing IoT payments and IoT marketplaces based on blockchain is very limited. Perera *et al.* [23] has done a survey of the IoT solutions in the emerging marketplace by discussing and summarising the functionalities provided by each solution.

Enser *et. al.* [25] examine the compatibility of blockchains for IoT payment transactions by highlighting the characteristics that have made blockchain an ideal solution for P2P transactions between IoT data producers and consumers. Further, this research paper discusses the integration challenges of blockchain to achieve fast and cheap IoT-related transactions as well. Ozyilmaz *et al.* [31] analyze the positive impact of establishing a decentralized and trustless platform for IoT data sharing. The writers have developed a proof-of-concept data marketplace using Ethereum and Swarm. Shaimaa Bajoudah *et al.* [32] proposed a decentralized marketplace to trade brokered IoT data. Also, Wiem Badreddine *et al.* [33] introduce an IoT data marketplace with three different models using MQTT as the publish/subscribe method, Ethereum as the DLT, and Solidity as the smart contract.

C. OUR CONTRIBUTION

Even though, the existing research and survey papers summarize the possible usage of blockchain for IoT, an extensive survey has not been done to research specifically on possible avenues for blockchain to resolve IoT payment challenges and cater marketplace requirements with the expected IoT boost that will be initiated by smart industries.

This paper aims to

- **Introduce the blockchain-based platforms** - The concepts related to blockchain and smart contracts are summarized. Further, the blockchain-based platforms are introduced.
- **Thoroughly analyze the usage of blockchain for IoT applications** - The blockchain-based IoT solutions are discussed.
- **Examine the IoT payment related issues and the requirement for an IoT market place** - The concept of IoT payments and blockchain-based IoT payment solutions are discussed in detail.
- **Discuss the suitability of blockchain based IoT payment system and IoT marketplace** - The concept of IoT market places and blockchain-based IoT market place solutions are discussed in detail.
- **Discuss technical challenges of IoT** - The technical challenges of IoT solutions are introduced and the role of blockchain in solving those challenges are analyzed.
- **Discuss the integration challenges of blockchain** - The unique challenges of blockchain integration are discussed.

D. OUTLINE

The remainder of the paper is organized as follows. Section II is an introduction to IoT and related challenges. Section III presents an overview on blockchain and smart contracts. Section IV summarizes the payment and market place requirements for IoT. How the payment and market place challenges can be addressed by blockchain is discussed in Section V. Available IoT payment systems and IoT market place options based on blockchain are discussed in Section VI and VII respectively. Section VIII introduces the integration challenges of blockchain. Lessons learned and open research issues are discussed in Section IX. Finally, the paper is concluded in Section X.

II. IoT AND RELATED CHALLENGES

In this section, we discuss the IoT related concepts and the related challenges which have lead to the usage of blockchain-based solutions.

IoT systems connect various smart objects mounted with sensors actuators and software systems. A typical IoT system consists of three main layers including, a perception layer with various IoT devices including sensors and actuators to sense data, a communication layer with various wired and wireless modules to transmit the sensor data, and an industrial application layer with various smart industry verticals. The general IoT architecture which is suitable for describing the latest IoT systems consists of an application layer, cloud computing layer, network layer, fog layer, and object layer is shown in Figure 1. The cloud computing and the fog layers are the major additions to the initial IoT architecture [34].

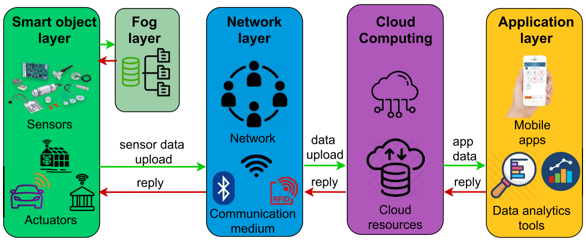


FIGURE 1. IoT architecture.

IoT has the following features [21]:

- Heterogeneity of IoT data - IoT systems consist of heterogeneous IoT devices, communication protocols, and IoT data types [35].
- Decentralization of IoT systems - IoT systems should be capable to exchange, make use of information and collaborate with each other
- Diversity of IoT ecosystems - Sensors, actuators, and software systems used in one IoT system to the other varies a lot.

These characteristics of IoT has resulted in bellow challenges [21]:

- **Heterogeneity of IoT system** – The variation of the devices, communication protocols, etc. have created complex networks and paved the way to many other challenges [35].
- **Poor interoperability** – Due to the decentralized and heterogeneous nature of the IoT systems, it is challenging to exchange information among different IoT systems [36].
- **Resource limitations of IoT devices** – IoT devices consist of limited computing, storage, and power resources. Therefore, the companies are forced to have large-scale cloud infrastructure projects [37].
- **Privacy and security vulnerabilities** – Exchanging IoT data with cloud-based IoT platforms, authentication of vastly decentralized IoT devices using limited resources in IoT devices have created privacy and security concerns [38].

The IoT devices constantly request data from other devices as a service. This ecosystem requires monetary transactions to be performed by sensors and devices in exchange for data services. These transactions and exchanges occur mainly over an internet-based network. Conventional payment models rely on a trusted third-party such as a bank, during transactions. However, considering the number of transactions that can occur with billions of IoT devices and the prevailing trust issues, centralized payment systems will not be able to handle the smart industry predictions. Also, in the IoT ecosystem, devices need to communicate regularly over the internet to exchange information. Malicious attacks from internal or external sources are common during the process. Therefore, at the first gateway to the network, an authentication mechanism that can secure the identity of the IoT devices in the network is essential [39].

The data growth rate in the IoT domain has increased with new devices, sensors, and emerging technologies. The enormous amount of data generated by these IoT applications has enforced companies to deploy large-scale cloud storage solutions. The emerging smart industries need to predict and adapt their solutions based on the insights received from sensor data. Therefore, a trustworthy neutral data-sharing platform is required for the data producers and consumers to trade [31]. These data streams generated by the IoT devices have a resell value to third-party buyers as well. The unavailability of a clearly defined framework for the business side of the IoT ecosystem is negatively impacting its growth. Therefore, a clear business model framework needs to be defined for the IoT data trading.

III. BLOCKCHAIN AND SMART CONTRACT

In this section, we first discuss the summary of blockchain technology, then summarize the key blockchain characteristics. Further, we introduce the IoT application areas and how blockchain is introduced for those IoT applications.

A. BLOCKCHAIN SUMMARY

Blockchain is a DLT that keeps a record of transactions in a transparent, auditable, and immutable manner. Block, chain and network are the three core parts of a blockchain. It stores transactions in a chain of blocks while using cryptographic mechanisms [47]. Except for the first block, each block in a blockchain point to its immediately previous block (parent block) using the inverse reference of the parent block (hash value of the parent block) [48]. The first block of a blockchain which is known as the genesis block doesn't have a parent block. A block structure consists of the following information:

- Block size - the size of the block in bytes
- Block header - contains block version, a reference to a previous block hash, merkle tree root, mining-related parameters, and nonce
- Transaction counter
- Transactions

A blockchain grows with the executed transactions and all the nodes in the network validate the newly generated blocks. Then, it will be appended at the end of the blockchain [21].

Key characteristics of blockchain include:

- **Decentralization** - The decentralization feature of blockchain distributes the authority among all nodes in the network. This ensures the redundancy of the system when compared with the centralized system approach which requires a trusted third party to operate. High availability of services, improved trust and reduced failure risk are the benifits provided by decentralization.
- **Immutability** - The transactions stored in the ledger are permanent and distributed among the nodes. Therefore, they are unalterable. This immutable nature of blockchain ensures the integrity of the data stored in the ledger [49].
- **Enhanced security** - Due to the decentralized nature of blockchain, any fraudulent party who wants to alter the blocks needs to alter the data stored in all nodes in the network. Encryption mechanisms are used to further enhance security and the cryptographic hash is used in the blockchains as well [50].
- **Consensus** - Conses algorithms are considered as one of the core concepts of blockchain which has made the network being trustless [51]. This is a decision-making process performed by the blockchain nodes in the network to validate the transactions. Even though the nodes in a blockchain don't trust each other, they trust the transactions validated by the consensus algorithm.

B. SMART CONTRACT

Smart contracts are programs stored in a blockchain that are executed when a predefined condition is satisfied [52]. They execute the terms of a contractual agreement using computerized transaction protocols [53]. The first implementation of a smart contract on the blockchain is Bitcoin. Later, Etherium developed a wide variety of smart contracts on a blockchain [54]. The contractual terms in smart contracts are enforced automatically when given conditions are satisfied. These enforced contractual terms are converted to executable computer programs while preserving the logical statement flows. Once, a smart contract is executed and stored in a blockchain, it is immutable and cannot be modified [21]. Smart contract solutions are used in various IoT applications such as healthcare, manufacturing, and finance [47].

C. IMPORTANT BLOCKCHAIN PLATFORMS

A comparison of important blockchain platforms is given in Table 3. Blockchain platforms can be categorized into four different types. They are

- **Public blockchain** - permissionless and anyone with internet access is allowed to become a node in the network which can validate the transactions based on the consensus algorithm used. Eg. Bitcoin and Ethereum
- **Private blockchain** - permission blockchain and network access are restricted only to authorized users. Eg. Multichain and Hyperledger Fabric
- **Consortium blockchain** - this is known as a federated blockchain where multiple organizations can govern the blockchain network. So, this is different from the private blockchain. Eg. R3
- **Hybrid blockchain** - a hybrid of both centralized and decentralized features where some processes are kept public and others private based on the transaction which can be shared in the public network. Eg. Ripple

TABLE 3. Blockchain and smart contract platforms and also more features.

Platform	Platform type	Transaction fee	Transaction count	Consensus	Related work
Etherium	Public	4 USD (Varies)	20 TPS	PoW	IoT Data Marketplace on Blockchain [31].
Hyperledger Fabric	Private	Free	2000 TPS	Orders and endorsers	Norwegian Seafood Traceability Network, My Sensor, VideoCoin Network [40], Carbon market [41].
Quorum	Private	Free	100 TPS	BFT	Financial services [42]
EOS	Public	Free	1,000 - 4,000 TPS	DPoS	Gaming solutions [43]
Cardano	Public	0.05 USD (Varies)	257 TPS	Ouroborous	Smart agriculture solution [44]
Ardor	Public	1 ARDR	12 TPS	PoS	Loyalty reward solution - Triffic solution rewards people with tokens for visiting local neighborhoods [45]
Ark	Public	0.1 ARK	18 - 19 TPS	DPoS	Financial tools - Payvo is a financial tool for crypto-based activities [45]
IOTA	Private	Free	250 TPS	Tangle	Smart City Solutions [46]

1) BITCOIN

Bitcoin is a widely used, virtual currency developed based on the concept of cryptocurrency [55]. The validated bitcoin transactions using PoW consensus is updated in a public ledger. Firstly, the transactions generated in a given period will be sorted and stored in a block. Then, the newly generated block will be added to the blockchain using inverse referencing method after it is validated by the other nodes in the public blockchain [56]. Bitcoin operates over a P2P network and it is vulnerable to decentralized network attacks such as the double spending attacks [57].

2) ETHEREUM

Ethereum is an open-source blockchain solution based on the concept of smart contracts [25]. Ethereum uses a programming language - solidity, decentralized storage service - swarm and the cryptocurrency - ether [31]. It used PoW as the consensus algorithm and later changed to PoS due to the transaction throughput related concerns of PoW [58]

3) HYPERLEDGER FABRIC

Bitcoin and Ethereum are famous due to the usage of bitcoin and ether as cryptocurrencies. But, Hypeledger is also gaining popularity, and the software development sector has started using it due to the promising results shown over other competing blockchain platforms [59]. It is an open-source community effort to develop a set of frameworks for industry-level blockchain deployments [60]. Hyperledger fabric is an enterprise-grade DLT platform that is developed to support industry use-cases that require a permissioned network with high scalability and security [61]

4) IOTA

IOTA uses tangle which is a DAG-based DLT technology [62]. IOTA platform is developed to address the IoE requirements by enabling a decentralized IoT data marketplace [31]. IOTA tangle is not a typical blockchain with blocks, chains, and miners. Instead, it uses directed graphs technology to cross-check one another and entangle the steam of transactions together [25]. IOTA platform promises to provide essential characteristics required by IoT.

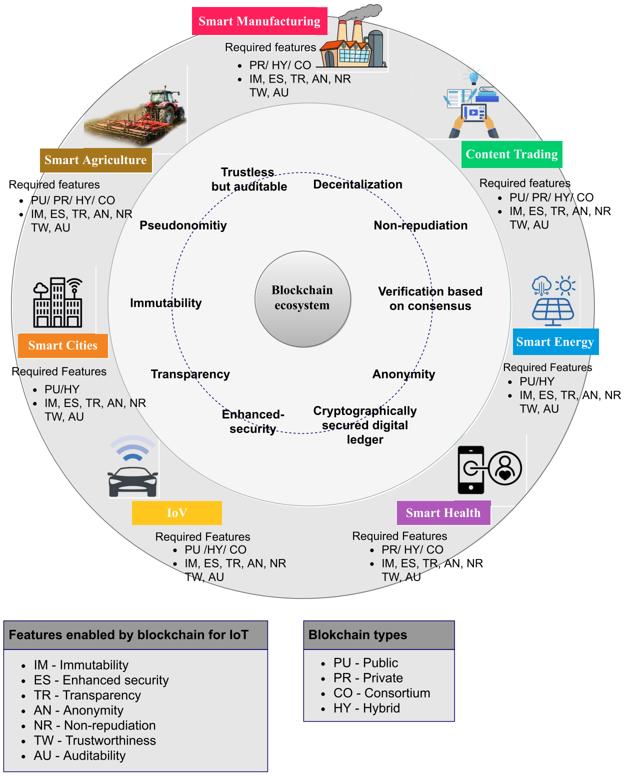


FIGURE 2. Blockchain-based solutions for IoT.

5) OTHER PLATFORMS

- EOS - EOS is an open-source platform for blockchain-based applications which can be deployed as a public or private network [63]. It uses Delegated Proof-of-Stake (DPoS) consensus algorithm to validate block producers and EOS token as the cryptocurrency [64]. Smart contracts and decentralized autonomous applications (dApps) are also used as core technologies.

- Cardano - Cardano is a DLT system that supports smart contracts and dApps. Cardano uses Proof-of-Stake (PoS) algorithm known as Ouroboros [64]. This is the first blockchain platform that was founded based on peer-reviewed research [65].

D. BLOCKCHAIN FOR IoT

IoT systems mainly consist of three major components: sensors, computation engine, and actuators. The actual implementation of sensors, computation mechanism, and actuators vary based on the IoT application [66]. The IoT implementations are suffering from technical challenges to achieve their true potential. Blockchain characteristics show a promising future to address the IoT challenges and take IoT applications to the next level. Hence, the convergence of blockchain and IoT has the potential to be the next paradigm in IoT application domain [21]. The Figure 2 summarises the features that will be enabled by blochain for IoT applications.

1) SMART MANUFACTURING

The conventional manufacturing industry is getting upgraded to smart manufacturing. During a product life cycle, a large amount of data is produced, and BDA-based IoT applications are heavily used [67]. Raw material, Manufacturing equipment, warehouses, and almost everything thing involved in a product life cycle needs to exchange IoT data. Therefore, blockchain-based solutions are suitable for smart manufacturing-related IoT applications and IoT marketplace requirements [68].

2) SMART AGRICULTURE

Smart agriculture applications use technologies such as BDA, cloud computing, IoT sensors to monitor and automate farming operations. Agricultural requirements need IoT applications to install sensors in the land, irrigation systems, weather stations, logistic facilities, and even in seller locations. This is a complex IoT eco-system that can vastly benefit from blockchain IoT applications and IoT marketplace [44], [69], [70].

3) SMART ENERGY

Smart energy applications are observed in various societal domains such as domestic needs, commercial applications, and other industry requirements. A smart grid is a key smart energy requirement where an electricity network is deployed to detect and react based on energy usage and observed issues to heal them. These applications need to coordinate with multiple parties in the eco-system such as consumers, consumer equipment, power generation, and distribution equipment, administrative and payment systems. Therefore, blockchain-based IoT solutions have the opportunity to resolve the challenges in smart energy applications while creating an IoT marketplace [71], [72], [73], [74], [75].

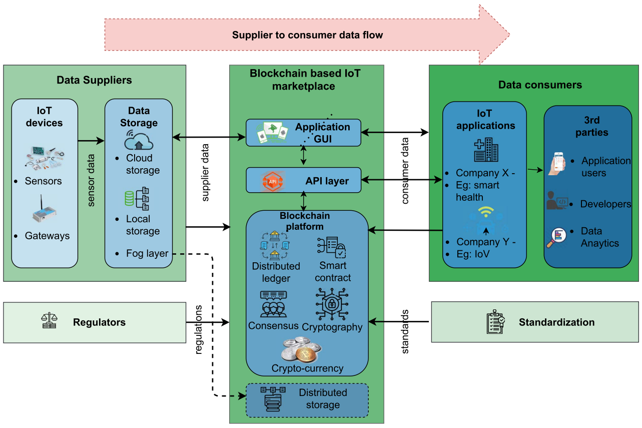


FIGURE 3. IoT data marketplace architecture.

4) SMART HEALTH

Healthcare-related applications should be dealt cautiously as it involves human life. The healthcare sector includes hospitals, health staff, patients, health equipment, logistics, etc. Therefore, IoT applications need to integrate all these sectors to provide solutions such as patient monitoring, health record maintenance, system automation, and disease predictions. Blockchain-based smart health applications can address strict security concerns related to the healthcare sector and deploy an IoT marketplace solution to allow health data sharing requirements as well [76], [77], [78], [79].

5) IoVs

IoV needs to integrate vehicle networks with other vehicle networks, roadside networks, infrastructure networks, and pedestrian networks to function. Therefore, IoV applications need to exchange sensor data and obtain feedback for users, manufacturers, etc. where an IoT marketplace would also require. Blockchain-based IoV applications have shown promising results to resolve the current IoV challenges and to provide a truly decentralized solution [80].

6) OTHER IoT APPLICATION

The other IoT application domains include transportation, supply chain and retail sector. The concept of IoE has enabled things, processes, data and people to create various IoT domains together. These IoT domains require IoT payments to handle micro-transactions and IoT marketplaces to enable data sharing applications.

IoT applications are expected to be the next paradigm, but the IoT application predictions have not yet been met due to the technical challenges observed during practical implementations. Blockchain-based solutions provide a trustworthy neutral platform for IoT applications to overcome the technical challenges prevailing currently. Blockchain itself needs improvements to handle IoT transaction expectations. But, the current research shows promising results with blockchain-based IoT solutions mainly in the IoT payment and marketplace application domains.

IV. IoT MARKETPLACE

IoT systems use sensors that are capable of sensing the relevant conditions, platforms that can process the collected data, and devices that can function as actuators based on processed data. These IoT eco-systems use cloud computing concepts such as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and emerging concepts such as Sensing as a Service. The IoT platforms require sensor data to function. Therefore, the data consumers are waiting to obtain the sensor data over the internet and they are willing to pay for the obtained sensor data as well.

The concept of the IoT marketplace has become an essential component in modern-day smart application ecosystems. The IoT marketplace value by 2030 is predicted to be over USD 3 trillion [81]. Further, more than one million organizations are expected to use IoT marketplaces to monetize their data. This will generate more than 12 exabytes of IoT data sets for the transactions performed daily [81]. BDEX [82] is a Data as a Service (DaaS) platform established in 2014 to provide actionable data for companies. DAWEX [83] is another global data exchange platform established in 2017 to monetize the generated data.

An IoT data marketplace mainly consists of three components. They are data suppliers, data consumers and the platform to handle the data marketplace.

- **Data suppliers** - They are the data owners. IoT devices such as smart home appliances, smart watches, weather stations and health monitoring devices are a few examples for the commonly used IoT data suppliers which generate data.
- **Data consumers** - They are the parties who are willing to purchase and use the data generated by the data suppliers. Research institutions,smart applications such as IoV and marketing agencies are a few examples for IoT data consumers.
- **Data platform** - It is required to handle the enormous amount of data generated by IoT sensor applications and share the data among the data consumers. Both the data consumers and suppliers need to register in this platform. Then based on the requirement of the data consumer, the platform should handle any relevant transaction fee and distribute data as per pre-defined policies that can be agreed by both the parties.

Figure 3 shows an IoT data marketplace architecture that can be used to share the generate IoT data among the required consumers. The registered IoT sensors generate IoT data and act as the data suppliers. The type of IoT data generated and the relevant compensation details must be updated during the registration process. The consumers need to compensate the suppliers and obtain the generated data.

A. KEY CHALLENGES IN CURRENT IoT MARKETPLACES

Data consumers and data suppliers seamlessly trade in an IoT marketplace. This allows companies to make use of both publicly available data and privately-owned data for their use cases. But IoT when creating an IoT marketplace, below mentioned challenges can be observed.

- **Lack of cooperation among IoT platforms** - It is challenging to exchange data between different IoT systems, due to the inherent nature of being decentralized and heterogeneous. Hence, the interoperability of IoT platforms is challenging to be achieved while results in data silos.
- **Requirement of a trusted third party** - Currently, the normal practice is to compensate the IoT data suppliers using a trusted third party such as a bank. When the micro-transactions that occur in the IoT ecosystem are considered, transaction fees and the centralized mechanism are not efficient approaches.
- **IoT devices specific technical challenges** - Limited resource availability is a common feature in IoT systems. Hence, the typical authentication and authorization approaches cannot be implemented and the systems are vulnerable to security threats.

B. ROLE OF BLOCKCHAIN FOR IoT MARKETPLACES

The contributing parties have multi-dimensional benefits from a decentralized IoT data marketplace.

1) TECHNICAL BENEFITS

- No need to maintain backend IoT platforms - The IoT data marketplace will act as the backend to integrate the sensors and the IoT applications.
- Availability of a vast pool of IoT data - IoT applications have insights from a pool of sensors. So, individual data silos with limited insights aren’t getting created.
- Optimized software for IoT sensors and applications - The IoT data marketplace is responsible for integrating the consumers and the suppliers. Therefore, the relevant software code or other application configurations that should run in sensors and IoT applications can be standardized.
- Actionable insight reselling capability - The data consumers can obtain raw data and further improve them into actionable insights and sell them to other interested third parties. Since we have a common IoT data marketplace, it is possible to compensate the original data suppliers.

2) ECONOMICAL BENEFITS

- IoT data monetization for data suppliers - New set of business models involving sensor data generators, data consumers will create more diversified IoT application use cases.
- Reselling IoT data with added value - The data obtained by data consumers can be resold after converting them into actionable data insights.

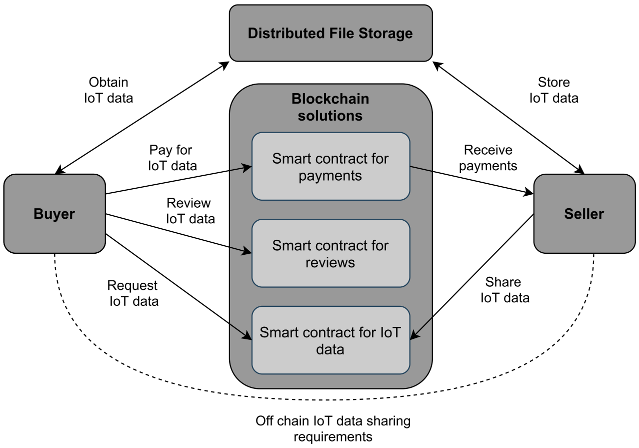


FIGURE 4. **Functional block diagram of blockchain-based IoT data marketplace.**

- IoT data economy - Even though it is predicted that IoT applications will revolutionize the world, only data silos are getting created. An IoT data marketplace will allow the true potential of IoT data monetization to be achieved.

The functional block diagram of a blockchain-based IoT marketplace varies based on the technologies used and a general block diagram is given in Figure 4. Let's analyze the already deployed similar solutions based on previous research.

Kazım Rıfat Özyılmaz et al [31] introduced a decentralized and trustless data marketplace platform for non-real-time and non-critical IoT applications to store and access IoT data. They highlight the fact that on-chain or off-chain data storage mechanism, monetization method and suitable tools and capabilities to create an IoT platform are the key considerations, when creating an IoT marketplace. The blockchain used is Ethereum and the decentralized storage used is Swarm. Smart contract is used for transparent data collection sharing to implement the decentralized IoT data marketplace. It is important for the data consumers to know the geolocations. Hence, GeoHex is used to facilitate easy querying of geolocations. A validation and feedback mechanism is used to rank the quality of IoT data, based on consumer feedback. Ether is used as the monetizing method. A off-chain scaling solution called payment channels (Raiden for Ethereum) is used to support instant transactions.

Gowri Sankar Ramachandran et al [84] propose a decentralized marketplace for smart cities. Sellers with data products and buyers interested in their data are fundamental components in the data marketplace. They have used smart contracts to register sellers and post data products for the buyers to search and find them. In this implementation, Ethereum blockchain is used along with an off-chain distributed file storage system named InterPlanetary File System (IPFS). Meta-data organization is proposed to follow any standard JSON format. Streaming Data Payment Protocol (SDPP) is used to enable real-time micropayments. The rating process of buyers and sellers in the marketplace is implemented using a smart contract as well.

Pooja Gupta et al [85] proposed a three-tiered architecture consists of participants of the marketplace, facilitators to supervise service areas, and regulators to ensure that the facilitators are adhering to the privacy regulations. IoT devices are resource-constrained, so facilitators ease the burden on those devices by acting as fog nodes. They used BigChainDB, a decentralized database system to maintain IoT system data. A blockchain named Martchain is built using Ethereum and smart contracts is executed to automate the trading. A watermarking technique is used to identify reselling of data and compensate the data suppliers. The regulators form a consortium blockchain named policy-chain to validate the compliance of facilitators by executing a policy contract, a smart contract.

Wiem Badreddine et al [33] developed a blockchain-based IoT data monetization framework. They use Message Queuing Telemetry Transport (MQTT) protocol and Ethereum smart contract to build three different real-time IoT data sharing solutions. The overall system architecture consists of a smart contract, publishers who provide IoT data, subscribers who consume IoT data, and an untrusted MQTT broker to connect the publishers and subscribers. They propose three solutions; Trace-MAX provides maximum traceability by asking the participants to write detailed information in the distributed ledger. Trace-MIN is the minimum traceability solution that required only the brokers to record minimal information allowing only a basic trace. Trace-BF uses bloom filters to manage data hashes with fewer verification operations on the blockchain.

V. IoT PAYMENTS

In an IoT ecosystem, based on the application the devices use various technologies to generate, communicate and analyze data. The interaction among people. devices and data are called the Internet of Everything (IoE) [25] nowadays. IoE needs the ecosystem to perform monetary transactions in exchange for services over the internet. The introduction of 5G technology is expected to further grow the potential use-cases of IoE.

IoT payment requirements are generated by various IoT verticals. Some of the example scenarios would be a smart car authorizing fuel payments as it approaches the fuel station, a smart health device sharing the prescription with a smart pharmacy, and proceeding with the drug purchase, and a smart agricultural applications ordering and paying for fertilizer and water supplies. M2M transaction value is expected to reach USD 27.62 billion by 2023 [86].

- **Smart cities** - The concept of cashless cities can connect any object to smart city network and eliminate the inefficiencies of payment mechanisms that can be observed in current systems. A research done by Visa in 100 cities shows that smart payment mechanisms can provide USD 470 billion in direct net benefits per year [87].

TABLE 4. Blockchain solutions for IoT payments and marketplaces.

Challenge of existing system	Description of the challenge	Solution via blockchain	Possible limitations in blockchain system
Requirement of a trusted 3rd party	• Rely on a trusted third party to perform financial transactions. • Usually, a bank acts as the trusted third party.	• Decentralized and immutable in nature. • The dependency with a trusted third party can be avoided and the transactions will still be reliable.	• The scalability concerns in terms of transactions and storage. • IoT payments require a scalable blockchain platform to handle its continuous growth.
Lack of anonymity for the users	• The users need to share their payment information and • Allow the transaction history to be maintained in IoT applications. • Considering the recent scandals, users always prefer to perform transactions anonymously.	• The keys used in blockchain and the personal identifiable information of the users can be separated and avoid linking them via pseudo-anonymity.	• A completely anonymous solution can lead to criminal activities. • The right balance of anonymity need to be carefully analyzed based on the application with the regulatory authorities.
Requirement of micro-payments	• IoT transactions are micro-transactions by default • The behavior of IoT applications require to perform multiple sub-transactions during a transaction. • The conventional payment mechanisms use trusted third parties • Centralized payment systems are not designed to handle micro-payments • Transaction fee is increased.	• Since, blockchain is a distributed ledger, a trusted third party is not required. • The transactions fees that need to be paid to the trusted third parties during micro-transactions can be avoided.	• Blockchain transaction validation via miners involves transaction costs. • It is a major concern in blockchain platforms as the IoT transaction values are very small.
Issue of fiat currency	• The use of fiat currency is common in both developed and developing countries. • The cost of producing, printing, and securing fiat currency, the inefficiency of payments and unsuitability to digital economic needs are major disadvantages.	• It can use crypto-currency based payments and avoid the usage of fiat currency completely.	• The regulatory bodies have not yet approved cryptocurrencies. • Usage of non-regulated and non-standardized cryptocurrencies is a challenge.
Static agreements on payment rates	• The traditional IoT businesses models primarily allow only static agreements with IoT data suppliers. • Due to dynamic micro-transactions it requires dynamic payment rates.	• The decentralized blockchain platforms enable P2P transactions. • The IoT data suppliers and the consumers can perform dynamic transactions. • It is flexible to allow P2P data sharing without performing a financial transaction as well.	• Blockchain transaction fee is a major blocking point to establish dynamic payment rate agreements.

- **Smart homes** - Modern day houses contain devices with embedded financial functionalities. Automated utility payments and automated supply ordering are a few examples where IoT has enabled pay-per-use business models and service offerings.
- **Smart transport** - The latest connected cars have inbuilt payment functionalities for everything from gas to parking and infotainment. Similar functionalities are introduced to the whole ecosystem of smart transportation. As an example, Honda and Visa together have introduced infotainment system that allows users to pay gas, parking, food, etc [87].
- **Smart retail** - IoT payments have created a subdivision of commercial activities where unattended retail is becoming more common. Amazon's new cashless, cashier-less stores which allow customers to collect items off shelves and automatically get charged upon exiting. According to new estimates, this has generated more than 50 % more revenue on average than typical convenience stores [88].
- **Smart grids** - The power production, transmission and distribution is monitored, controlled and smart concepts such as smart metering and peer to peer energy trading are introduced with smart grid concept [89].
- **Smart agriculture** - This domain mainly deals with buyer-seller relationship in many areas including purchasing seeds, sharing climate data, selling crops, agriculture field monitoring, etc. Therefore, IoT related micro-payments which can vastly benefit by introducing a distributed payment mechanism

based on blockchain is an integral part of the eco-system [69]
- **Smart healthcare** -Smart healthcare systems deals with sensitive patient information and deals with various payments requirements with patients, hospitals, healthcare staff, pharmaceutical industries etc. [90]
- **Supply Chains** - Supply chains related transactions are subjected to issues such as money laundering, sanction violations, bribery, etc. Therefore, blockchain-based IoT payment solutions can improve the efficiency and reduce frauds [91].

A. KEY CHALLENGES IN CURRENT IoT PAYMENTS SYSTEMS

Conventional IoT applications deploy their own IoT ecosystem with sensors and actuators with network connectivity and IoT platform to run the relevant control algorithms to run the application. This has created IoT network silos for individual applications. As a result, the capital cost of IoT application deployments is high and the widespread use of IoT solutions is hindered.

- **Requirement of a trusted 3rd party** - Traditional IoT business models rely on a trusted third party to perform financial transactions. An intermediary such as a bank is used during the process and the actual advantages of P2P transactions are not allowed to be obtained because of this.
- **Lack of anonymity for the users** - IoT application users are reluctant to share their payment information and allow the transaction history to be maintained in IoT applications.
- **Requirement of micro-payments** - IoT deals with micro-transactions and in order to perform a single IoT transaction, multiple sub-transactions might need to be performed. The conventional payment mechanisms are not designed to handle such micro-payments and using a trusted third party has increased transaction fees as well.
- **Issue of fiat currency** - Even in today's world, the paper-based currency is used for 85% of all global transactions. This is common in developed economies as well. The usage of fiat currency in the United Kingdom, United States, and Germany are recorded as 48%, 55%, and 67% respectively [92]. The usage of physical fiat currencies is a major blocking point for the advancement of the IoT sector. The cost of producing, printing, and securing fiat currency, the inefficiency of payments, unsuitability to digital economic needs are some of the major concerns of physical fiat currencies.
- **Static agreements on payment rates** - IoT requires to perform dynamic micro-transactions [93]. Due to traditional business models that are prevailing in the industry, IoT platforms have to enter into static agreements with IoT data suppliers. But, the data requirements of IoT platforms are dynamic in nature. So, the latest IoT trends urge for solutions that has the capability to handle dynamic payment terms.

B. ROLE OF BLOCKCHAIN FOR IoT PAYMENTS

The key characteristics of blockchain include decentralization, immutability, and enhanced security. These characteristics make the blockchain technology ideal for IoT payments. Since the blockchains are distributed, direct P2P transactions can be performed without the need of a trusted third party. The IoT payments can be made unalterable due to the immutability provided by the consensus mechanism and smart contracts used by blockchains. Therefore, the IoT transaction history can not be modified or reversed.

Worldwide people have adopted electronic payments. The consumer identity theft attempts are common and current payment system ecosystems such as payment cards are vulnerable to such instances. The process of tokenization converts the sensitive data into non-sensitive tokens. Therefore, sensitive data can be secured as the original data gets replaced with an unrelated value. Blockchain-based distributed payment systems can protect the users from identity thefts as payment tokens can easily be used in the blockchain payment ecosystem [94].

The conventional fiat currency faces issues in currency issuance, payment methods, and currency storage requirements. Therefore, digital currency usage is ivolving and the acceptance of bitcoin by El-Salvador in June 2021 as legal tender, is an example for the possibility of world moving towards cryptocurrencies. Xuan Han et al [95] have analyzed some of the major cryptocurrencies and proposed an scheme to use digital currency during their research work.

The eco-system of blochkchain-based IoT payments is given in Figure 5. The blockchain-based decentralized IoT payment schemes will provide various benefits to IoT payment domain.

- **No dependency with third-party payment platforms** - The traditional business models rely on a trusted third party to proceed with payment transactions. The most widely used mechanism is to use a third-party such as a bank to proceed with transactions. Blockchain-based IoT payment options have enabled actual P2P transactions without any dependency on a third party.
- **Anonymous transactions** - When a third party such as a bank is involved in the transaction process, the users have to provide sensitive information such as credit card information to proceed with payments. If IoT data from multiple platforms is required, the users have to expose their sensitive payment information multiple times. Considering the security risks involved in the current digital era, this is not preferred by IoT data consumers. So, using blockchain, a certain amount of anonymity can be maintained.
- **Less transaction fee** - In traditional E-business models, the transaction fee is a major issue as micro-transactions are a unique characteristic of IoT. Blockchain-based solutions are improved and necessary research is being done to minimize the transaction fee. Also, IOTA-tangle-based payment approaches have introduced payment options without any transaction fee.

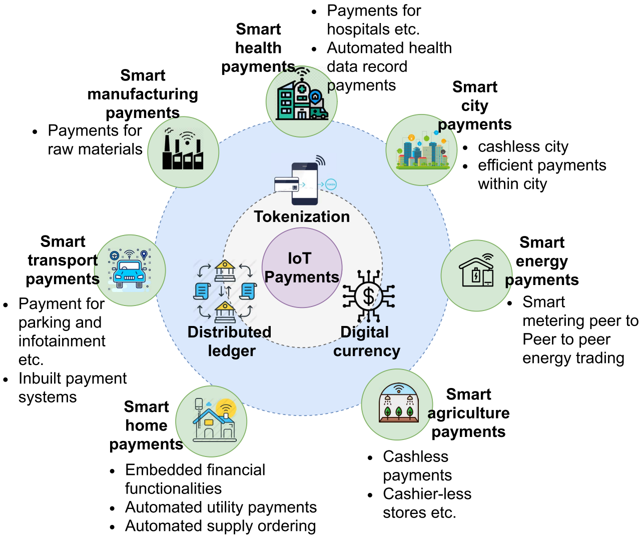

Smart health payments
Payments for hospitals etc.
Automated health data record payments
Smart manufacturing payments
Payments for raw materials
Smart city payments
cashless city
efficient payments within city
Tokenization
IoT Payments
Smart transport payments
Payment for parking and infotainment etc.
Inbuilt payment systems
Smart energy payments
Smart metering peer to Peer to peer energy trading
Distributed ledger
Digital currency
Smart home payments
Embedded financial functionalities
Automated utility payments
Automated supply ordering
Smart agriculture payments
Cashless payments
Cashier-less stores etc.

FIGURE 5. **Blockchain-based IoT payment.**

VI. TECHNICAL CHALLENGES OF IoT PAYMENT AND MARKETPLACES

The traditional IoT business models used for IoT payments and marketplaces rely on central authority. This has created technical challenges such as IoT data security and privacy issues, creation of data silos without any collaboration, requirement of a central payment systems, lack of anonymity and fradulent transaction attempts. Table 4 shows how the existing IoT payment and marketplace challenges are addressed by blockchain solutions and Table 5 highlights how IoT challenges are addressed by blockchain in real world implementations.

A. IoT DATA SECURITY

1) TECHNICAL CHALLENGE OF IoT DATA SECURITY

Most of the IoT devices are controlled remotely over the internet to achieve the desired functionality. These devices use standard communication protocols to share information among the devices in the IoT ecosystem via communication networks. The IoE concept highlights the smart connected things concept where each device is having some sensor module to collect data and a communication module to connect to the IoT application network. These IoT devices include home appliances, health monitoring devices, weather stations, tracking devices, and much other equipment based on the IoT application domain. The data acquired from the end devices need to be shared in real-time with the IoT application platforms. Considering the critical nature of the IoT ecosystem, enabling IoT data security is a critical factor for the development of all IoT fields.

The IoT deployment architectures need to be secure from privacy, integrity, and confidentiality-related security attacks. IoT ecosystem consists of inter-connected networks which inherit the security issues of computer networks. The heterogeneous devices are having power, memory and other resource constraints that make it further challenging to address the security issues through complex mechanisms [26].

2) ROLE OF BLOCKCHAIN IN SOLVING IoT DATA SECURITY ISSUE

Blockchain solutions are introduced for tracking and monitoring products, goods, and assets to increase trust and security. They maintain the integrity of the distributed transactions. Therefore, IoT devices can be registered with a defined set of attributes in a distributed ledger such as blockchain and resolve the existing security and trust issues of IoT platforms.

The Blockchain IoT (BIoT) concept in [39] explains how sensor data-related transactions can be included in a blockchain. This provides essential security features such as publishing sensor data in distributed ledgers, the immutability of the records, authentication, and non-repudiation of data. They are identified as solutions with protection from data tampering and usage of compromised IoT devices, secure communication, user authentication, and trustworthiness [96].

Even though blockchain-based solutions can establish IoT security, they are also vulnerable to security issues. If the randomness of private keys is limited, then they can easily be compromised by the attackers. Further, transaction privacy and other security threats such as double spending attacks need to be carefully analyzed when introducing a blockchain solution [27].

3) SUMMARY

Even though blockchain systems offer a robust approach for IoT security, they are also vulnerable. Based on the security threat, the research community has suggested different frameworks. But, a single framework that is resilient against many combined attacks and feasible to implement is a research challenge. The fate of blockchain-based security in the era of quantum computing is yet to be properly analyzed.

B. IoT DATA PRIVACY

1) TECHNICAL CHALLENGE OF IoT DATA PRIVACY

The IoT data produced within the IoT ecosystem need to be transmitted, processed, and stored securely without compromising privacy. It is common for IoT data to contain sensitive information including personal data. User data should not be disclosed without obtaining consent from the data owners. IoT ecosystems are complex, decentralized, and consist of heterogeneous system elements. Therefore, it is challenging to preserve the privacy of IoT data.

The privacy concerns related to IoT data negatively affect the adoption of it as users are reluctant to use a system that is not capable of respecting the privacy requirements of the users. The traditional authorization protocols such as Role Based Access Management (RBAC), OAuth 2.0, and OpenID are too complex to run in most of the resource constraints IoT environments. User privacy is considered a major concern by the regulators as well. Therefore, it is essential to guarantee the privacy of IoT data [26].

2) ROLE OF BLOCKCHAIN IN SOLVING IoT DATA PRIVACY ISSUE

Smart contracts can be executed in blockchains to provide IoT device authentication in the decentralized system and they are less complex compared to the traditional authentication protocols. Blockchain solutions have their own privacy-related concerns. One of the main issues that should be addressed to preserve data privacy is not letting and sensitive data be lost or erased from the system [97]. Mixing technique and anonymous solutions are the two existing solutions for privacy protection [98]. Both centralized mixing and decentralized mixing models have their own disadvantages. In centralized mixing, the transaction time is a major concern, and in decentralized mixing increased complexity is a major concern [98]. The use of cryptography-based techniques to preserve privacy and transaction time is a common approach to preserve the privacy.

Smart contracts can be used to define access rules, access time periods, or other required conditions to ensure data privacy and the user right levels can also be managed [26]. Tiffany Hyun-Jin Kim et al [99] developed a mechanism named Self-Sovereign Privacy (SSP) to protect the privacy and integrity of the data collected by IoT devices. This method removed the risk of having a single point of failure and minimized the cryptographic operations that must be performed on IoT devices. Fitwi *et al.* [100] Fitwi *et al.* [100] proposed a blockchain-based privacy protection scheme for surveillance cameras to perform surveillance activities by capturing videos without compromising user privacy.

3) SUMMARY

Privacy of IoT data needs to be preserved to enhance user trust in the IoT ecosystem. Blockchain solutions provide possible solutions to address IoT data-related privacy concerns. Even though blockchain is an ideal candidate to address many of the IoT-related technical challenges, widespread adoption of blockchain-based technologies is still hindered due to the privacy concerns of blockchain itself. In public blockchains, user information shared is disclosed to all nodes. Further, the other types of blockchains are also facing data privacy-related concerns where research community is trying to provide an ideal solution.

C. LACK OF COOPERATION AMONG IoT PLATFORMS

1) TECHNICAL CHALLENGE OF NOT HAVING COOPERATION AMOING IoT PLATFORMS

It is challenging to exchange data within the IoT ecosystem due to the decentralized nature and heterogeneity of IoT systems and it is challenging to achieve interoperability as well. The distributed IoT resources make it difficult to manage and the distribution of smart objects of multiple IoT applications at the same location makes it more complex. Therefore, the cooporation among IoT platforms is important to reduce complexity and deployment costs [101].

Let's consider an example: An agricultural IoT system needs weather data for analytical purposes. The weather stations established by the meteorology department independently collect weather data for weather predictions. Since the two IoT platforms are working independently without any cooperation, the agricultural IoT system will need to deploy a separate weather station. If there is a common IoT marketplace, agricultural IoT platform and weather station platform can exchange information and achieve resource optimization. The different IoT verticals need to cooperate with each other to prevent the issue of small silo networks without much use is getting created.

2) ROLE OF BLOCKCHAIN IN PROVIDING COOPERATION AMONG IoT PLATFORMS

Blockchains can keep the transactions in an immutable manner and the transaction records in the blockchain are transparent and reliable. Further, data monetization can be enabled via cryptocurrency-based transactions without the need for fiat currency. Therefore, the blockchain-based IoT data marketplace concept can deploy a platform for various IoT applications to coordinate with each other.

Let's consider an example: A smart health monitoring device fixed on an athlete can monitor the health conditions. Once the device owner advertises the data via an IoT marketplace, hospitals, AI-based training institutions, pharmaceutical companies, and any other third-party system can obtain the stream of data to be used in their IoT applications. This type of approach can allow the IoT platforms to coordinate with IoT platforms and fast track the IoT adoption.

Dai *et al.* [21] highlighted the convergence of blockchain and IoT and proposed an interoperable IoT platform architecture. Abou-Nassar *et al.* [109] introduced a decentralized and interoperable trust model based on blockchain for healthcare-based IoT.

3) SUMMARY

Due to the lack of cooperation among IoT platforms, small-scale silo networks are getting created. This is a major concern for the widespread adoption of IoT solutions. Blockchain provides a promising solution to the IoT platform interoperability issue via the blockchain-based IoT platforms. But, the integration challenges of blockchain such as performance and scalability issues observed with IoT platforms that generate a high volume of data need to be resolved with further research.

D. REQUIREMENT OF CENTRAL PAYMENT SYSTEMS

1) TECHNICAL CHALLENGE OF HAVING A CENTRAL PAYMENT SYSTEM

The conventional IoT business models rely on a trusted third party to act as an intermediary to perform monetary transactions. This is a major limiting factor to prevent the adoption of true P2P applications. The recent boom in IoT and the expected growth in the IoT ecosystem suggest that IoT applications and relevant monetary transactions will increase exponentially. In an IoT data marketplace, it is preferred to allow data suppliers and consumers to perform the transactions in a decentralized manner [33].

TABLE 5. How blockchain solutions can address IoT challenges.

Challenges	Importance of blockchain features to address them	Practical implementations	Possible limitations in blockchain system
IoT Data Security	• Allows to publish sensor data in distributed ledgers, the immutability of the records, authentication, and non-repudiation of data. • Therefore, data tampering will be avoided and secure communication, user authentication, and trustworthiness will be enabled.	• ArcTouch – DApps for smart, connected items; including voice assistants, wearables and smart TVs [102]. • Xage - A blockchain-protected security platform for IoT [103]	• Vulnerable to security issues including transaction privacy and other types of attacks such as double spending.
IoT Data Privacy	• Smart contracts can be executed to provide IoT device authentication in the decentralized system • Cryptography-based solutions can further enhance privacy.	• Chronicled - pharmaceutical and food supply industries related supply chain solutions [104]. • The stringent data privacy requirements in pharmaceutical industry are handled.	• Privacy of blockchain-based IoT systems is a major concern. • Especially, public ledgers, lack of awareness in data sharing and ability to track via personally identifiable information pose data privacy risks.
Lack of cooperation among IoT platforms	• The decentralized, immutable, transparent and crypto-currency-based IoT data marketplace. • A platform which the IoT applications can coordinate.	• NetObjex – IoTokens provides a secure platform for IoT devices in the same ecosystem [105]. • Helium - A decentralized wireless infrastructure solution to provide connectivity for IoT devices [106]	• The complexity of blockchain-based systems is a major concern for resource limited IoT applications.
Requirement of central payment systems	• Due to the distributed nature of blockchains, they allow direct P2P transactions without the need of a trusted third party.	• HYPR - decentralized networks to secure connected ATMs, cars, locks and homes [107]. • Grid+ - Provides consumers access to energy saving IoT devices.	• Transaction fee issue of blockchain.
Lack of anonymity	• Blockchain has the capability to provide anonymity via decentralized payment systems.	• NEBULA GENOMICS -Understanding human genome. All individual DNA data are kept anonymously in a blockchain [108].	• Due to the complete anonymity, they are vulnerable to criminal exploitation and regulatory resistance.

2) ROLE OF BLOCKCHAIN IN IMPLEMENTING DECENTRALIZED PAYMENT SOLUTION

Due to the distributed nature of blockchains, they allow direct P2P transactions without the need of a trusted third party. Blockchain technologies bring capabilities such as data tracking, coordinating, and allowing a large number of devices to be handled without a centralized approach. The parties in a blockchain might not trust each other. But, the immutability of blockchains has enabled the parties to trust each other without a central authority. From the past, there were proposals for decentralized P2P Wireless Sensor Networks (WSN) [24]

P2P transactions without third-party intervention can be allowed in a distributed payment system [110]. Chanthong *et al.* [111] designed and built an electronic payment system for electric vehicle (EV) charging using blockchain and smart contract technologies to control and manage payments and to decentralize the payment system. Dimitriou *et al.* [112] developed a data payment and transfer scheme that uses bitcoin payments to reward users for detailed electricity measurements they submit to a utility provider (UP) and other applications such as crowdsensing. Even though the technology is promising which has hindered the usage of blockchain as a decentralized payment platform. The technology has its own scalability issues. Payment channel networks have been proposed to increase transaction throughput and decrease transaction confirmation latency, [113].

3) SUMMARY

IoT deals with micro-transactions. Each transaction of cryptocurrency requires a certain amount of computation and attracts transaction fees. Therefore, the computation and transmission overheads are a major concern in blockchain-based decentralized payment systems.

E. LACK OF ANONYMITY

1) TECHNICAL CHALLENGE OF LACK OF ANONYMITY

Users do not want the IoT applications to store their payment and transaction history details. Eg: Imagine a farmer who's using third-party weather station data to control an irrigation system. This farmer has to pay for the weather station data, smart irrigation system, etc. So, the farmer's bank information data need to be shared with the third parties who are handling these IoT platforms. If the use case involves more IoT platforms, the number of times the bank information to be shared will also increase.

2) ROLE OF BLOCKCHAIN IN PROVIDING ANONYMITY

Blockchains excel in anonymity when compared to traditional centralized IoT platforms. Gordon *et al.* [114] used pseudonymization which consists of removing some of the information necessary to identify an entity. The research conducted by Kshetri *et al.* [115] proposed a blockchain-enabled e-voting (BEV) system to allow the eligible voters to anonymously cast their vote using a computer or smartphone. Lin *et al.* [116] introduced Decentralized Conditional Anonymous Payment (DCAP). It is difficult to regulate Decentralized Anonymous Payment (DAP) systems. Therefore, the anonymity feature of blockchain can be exploited by criminals for money laundering and other cybercrime.

3) SUMMARY

Blockchain has the capability to provide anonymous solutions via decentralized payment systems. But, complete anonymity can be criminally exploited. Therefore, the decentralized payment systems should be designed after carefully considering the level of anonymity to be allowed based on regulatory requirements to avoid criminal exploitation and reasonable privacy protection.

F. OTHER TECHNICAL CHALLENGES

1) TECHNICAL CHALLENGE OF HIGH TRANSACTION FEE

If a third-party organization is used in IoT solutions, a separate transaction fee should be paid for their service. Since IoT payments include many micropayments, the higher transaction fee is a major concern for IoT payments and market places [93]. Therefore, a payment that is both small and metered is required for IoT systems. We can use cryptocurrencies to remove the fiat currency usage requirement, Further, the decentralized solutions, remove the need for a third party to perform monetary transactions. Therefore, the merchant payment fees can be reduced and users can receive funds immediately via cryptocurrencies. The transaction fee is an issue in blockchain technologies as well, but there is multiple research that has been done to improve this significantly.

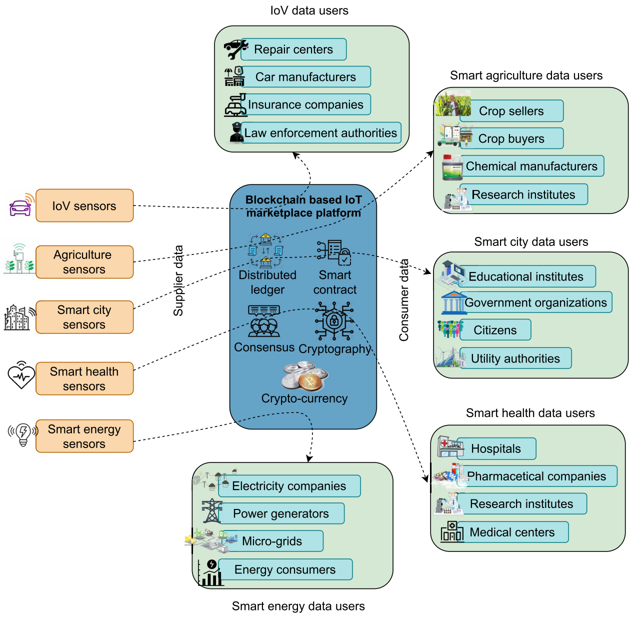


FIGURE 6. Blockchain-based IoT payment and marketplace application domains.

2) STATIC AGREEMENTS ISSUE

Due to the current static agreements, there is a possibility for the data owner to loose the ownership of data due to reselling possibility. An example scenario would be a small house generating sensor data and providing them to marketplace, then the data can be resold by-passing the owner.

VII. IoT APPLICATIONS

Blockchain technology can be applied in many IoT domain applications. Blockchain technologies can be applied in different IoT domains as shown in Figure 6. These IoT applications include autonomous vehicles, smart agriculture, smart cities, smart grid, and smart trading. A summary of related research work in IoT application domains are mentioned in Table 6.

A. AUTONOMOUS VEHICLES

1) INTRODUCTION

IoV is considered as an emerging concept in Intelligent Transportation Systems (ITS) which has integrated the Vehicular Adhoc Network (VANETs) to IoT [117]. The overall IoV ecosystem that consists of smart vehicles is interdependent with communication networks, and external environments including roads, traffic lights, road signs, pedestrians, and all relevant domains relevant to transportation. IoV is a major component in the concept of smart city as well [118].

2) ROLE OF BLOCKCHAIN-BASED SOLUTION

IoV has integrated smart vehicles with the internet. The overall IoV ecosystem includes smart vehicles with sensors, road network, pedestrians, other vehicles, and other infrastructure. Therefore, in order to guarantee road safety, a common information exchange platform is required among the IoV ecosystem. ITS needs this platform to be secure, trustworthy, and immutable to achieve the intended objectives [117]. IoV faces technical challenges such as effectively using the scare spectrum, allocating channels for communication, and utilizing transportation infrastructure appropriately based on the traffic conditions [119]. IoV applications can resolve these challenges by integrating blockchain with cryptographic techniques and edge computing. Innopolis University in Russia implemented a M2M billing service for electric autonomous vehicles. Their primary focus was to introduce a solution based on IOTA's tangle network for the M2M monetary transactions that need to be performed by the vehicles with charging stations for electricity consumption. The introduced payment framework acts as a meter to exchange IOTAs for the consumed power based on the number of kWh [25].

3) SUMMARY

IoV aims to establish a novel and secure smart vehicle ecosystem. IoV is still trying to resolve many security and privacy vulnerabilities. The blockchain-based solutions that are emerging in IoV are capable of resolving the technical challenges of IoV by enabling secure data communication. Secure IoV communications can utilize methodologies such as the High-Performance Blockchain Consensus (HPBC) algorithm. But, the number of transactions required to update blockchain ledgers poses serious issues for vehicles as these may consume the available energy.

B. SMART AGRICULTURE

1) INTRODUCTION

Smart agriculture is a revolutionary concept that has allowed farmers to access real-time crop data very easily and respond accordingly. Farmers can analyze data and make informed decisions rather than relying on their gut feeling. Efficiency in all aspects of farming is critical to get the maximum yield and meet the increasing demand. Smart agriculture expects to improve all food supply chain elements by eliminating the middleman and deploying a transparent and efficient system. The application requirements of agriculture supply chain include query efficiency, security and privacy, the authenticity and reliability of data [120].

2) ROLE OF BLOCKCHAIN-BASED SOLUTION

In the context of building an inter-organizational mechanism of data sharing and value creation, blockchain technology is believed to be the favorable candidate, compared to many other information and communication technologies (ICT). The need for a middleman can be eliminated by introducing transparent and efficient blockchain-based food supply chain solutions. This allows the buyers to track the origin of the product, product delivery time, and even the environmental conditions of the field as well [69]. Mohsin Ur Rahman *et al.* [44] proposed a distributed data sharing system for smart agriculture which consists of four main components namely smart agriculture, smart contract, Interplanetary File System (IPFS), and agriculture stakeholders. Lu *et al.* [70] designed a blockchain-based agricultural data sharing model and system architecture.

3) SUMMARY

Smart agriculture applications need systems that can guarantee query efficiency, security, and privacy, authenticity, and reliability of data. Blockchain-based smart agriculture platforms are capable of deploying a transparent and trusted ecosystem where farmers can have access to instant agriculture-related data such as the seed quality, climate environment-related data, payments, soil conditions, and crop market status.

C. SMART CITIES

1) INTRODUCTION

Smart cities are developed as a solution to the growing urbanization challenge to achieve sustainable development goals. They are a combination of smaller smart networks. These data-driven services are developed based on ICTs and the data is acquired via mechanisms such as sensors, cameras, human inputs, crowd-sourced data from mobile phones and vehicles. The data sources might be wholly owned by local authorities, a single organization, or any heterogeneous group of individuals and organizations. The data owners must be compensated by the data consumers in a smart city for sharing the data with them [84].

2) ROLE OF BLOCKCHAIN-BASED SOLUTION

A smart city consists of various parties that need to sell, find and buy data to function their applications. The data suppliers need to be compensated for sharing information. Therefore, the IoT data marketplace platforms are essential in smart cities. Blockchain's unique characteristics make it an ideal candidate for such an IoT marketplace.

El Majdoubi *et al.* [122] developed a smart blockchain-based solution to preserve privacy and security in a smart city environment. Stefano Loss et al [123] demonstrated how a blockchain-based platform can be used to handle land registration. Xie *et al.* [124] reviewed how blockchain technology is applied in various domains of smart cities including smart citizens, smart healthcare, smart grid, smart transportation, and supply chain management. Hakak *et al.* [125] did a case study on a conceptual blockchain-based architecture that can secure a smart city.

3) SUMMARY

A smart city is an ecosystem of various IoT applications such as transportation, healthcare, energy, manufacturing,

TABLE 6. Blockchain-based IoT payment and marketplace related research.

Ref.	Description of related work.	IoT Marketplace	IoT Payments	IoT Challenges					IoT Application						
				IoT Data Security	IoT Data Privacy	Lack of cooperated IoT platforms	Need of central payment systems	Lack of anonymity	Autonomous Vehicles	Smart Agriculture	Smart Cities	Smart Grid	Smart Healthcare	Content Trading	Common
[31]	A decentralized and trustless data marketplace platform for nonreal-time and non-critical IoT applications to store and access IoT data.	✓	✓			✓	✓								✓
[84]	A decentralized marketplace for smart cities.	✓	✓				✓				✓				
[85]	A three-tiered architecture consists of participants of the marketplace, facilitators to supervise service areas, and regulators to ensure that the facilitators are adhering to the privacy regulations.	✓	✓			✓	✓								✓
[33]	A blockchain-based IoT data monetization framework.	✓	✓			✓	✓								✓
[119]	A blockchain-based IoV scheme to ensure secure data sharing.		✓	✓	✓		✓		✓						
[76]	A blockchain-based consent model for health data sharing.	✓	✓				✓						✓		
[84]	A blockchain-based data market place for smart cities.	✓	✓		✓	✓	✓	✓			✓				
[85]	A three tier IoT marketplace consisting of data sellers, facilitators and regulators is proposed.	✓				✓	✓								✓
[121]	An integrated trading system named ArtChain, based on blockchain for trading artworks	✓	✓				✓							✓	
[78]	A decentralized health data trading platform with access control and smart contract.	✓	✓	✓		✓	✓	✓					✓		
[75]	A power trading market-based on blockchain and n VCG-auction-based transaction.	✓	✓			✓	✓					✓			
[74]	A blockchain implementation-based on Ethereum implementation for energy trading.		✓				✓					✓			
[44]	A blockchain-based data sharing platform for smart agriculture.	✓		✓			✓			✓					
[70]	A blockchain-based agricultural IoT data sharing system .	✓					✓			✓					

education, administration, and logistics. The characteristics of blockchain such as transparency, automation, decentralization, and immutability are helpful in achieving the ultimate smart city concept.

D. SMART GRID

1) INTRODUCTION

Smart grids are the core of smart energy solutions. It allows the power generation sources and the power consumers to exchange information and deliver energy in an automated and distributed network. Micro-grids are deployed within small communities using renewable energy and Energy Storage Systems (ESS). They act as a platform to trade locally generated energy with each other in the community [71].

2) ROLE OF BLOCKCHAIN-BASED SOLUTION

Dekhane *et al.* [72] presented a blockchain-based power distribution ecosystem for smart cities. This system used a wallet-based currency, called "Green Coin", for power transactions such as buying, selling, and lending. Hamouda *et al.* [73] presented the development and case-study validation of a comprehensive transactive energy market framework with linked blockchain and power system. Hussain *et al.* [74] developed an ethereum-based blockchain solution for energy trading. The research results are shown for a case where energy transactions are undertaken between the Distribution System Operator (DSO) and the smart meters of individual houses. Ha *et al.* [75] designed a power smart contract system based on blockchain for renewal energy trading market that consists of power producers and consumers (Prosumers).

3) SUMMARY

The concept of smart energy aims to integrate green and renewable energy technologies into the conventional power grids efficiently. The blockchain-based typical power trading markets consist of power producers and power consumers who are capable of producing renewable energy. Blockchain and smart contract technologies used in energy trading helps to implement a distributed network with transparency and immutability

E. SMART HEALTHCARE

1) INTRODUCTION

Rapid growth is observed in the usage of wearable bio-sensors and smart healthcare-related use cases. The enormous amount of data produced by the healthcare ecosystem need to be shared among the parties involved. This ecosystem will eventually improve the health condition of people by using their own data as it provides an overall better understanding of a patient rather than relying only on Electronic Health Records (EHR). In the current context, due to the hospital or specific patient-specific IoT solutions, only health data silos are getting created. Therefore, it is required to enable data sharing among both private and public healthcare sector applications to prevent the less useful data silos from getting created. [126].

2) ROLE OF BLOCKCHAIN-BASED SOLUTION

The main requirement of a health marketplace is to create a data-centric decentalized ecosystem and use AI applications to further improve the solutions. Decentralized marketplaces are implemented based on secure smart contracts and DLTs. This has enabled data producers to transact with data consumers while maintaining anonymity. Blockchain-based platforms can create a distributed and trusted user network for data sharing [76]. BCT has the potential to enhance data-sharing due to its properties such as transparency, traceability, and immutability [77].

Alsharif *et al.* [78] proposed a decentralized blockchain-based medical data marketplace for the medical record sellers to sell their data to interested buyers. Kumar *et al.* [79] established a hyperledger fabric-based blockchain network among patients and medical institutions to share patients' data securely and reliably. Jaiman *et al.* [76] developed a blockchain-based data-sharing consent model using smart contracts to access control the health data. Dubovitskaya *et al.* [77] presented a systematic literature review to analyze the motivations, advantages, limitations, and future challenges faced when applying the distributed ledger technology in oncology.

3) SUMMARY

Smart healthcare applications consisting of various elements such as health monitoring devices, research institutes, patients, and various other sections that need to share health-related information with each other. Considering the sensitive nature of health data, health data sharing should be allowed based on individual consent. But, resource limitation is a major bottleneck. Further, BCT uses crytographic techniques to guarantee data privacy and security.

F. CONTENT TRADING

1) INTRODUCTION

BitTorrent technology is an option for content data sharing. But, it infringes on the copyright, which taints its public perception [127]. The art market performs USD 200 billion worth annual trading, It is one of the largest unregulated markets in the world which is responsible for one-third of crimes committed [128].

2) ROLE OF BLOCKCHAIN-BASED SOLUTION

The blockchain-based digital content marketplace can resolve the issue of digital content trading issues that are observed in current market environments. The decentralized market which will be created using blockchain allows the users to engage in content publishing, hosting, accessing, downloading, and paying activities.

Heo *et al.* [129] proposed a new blockchain system named the Secret Block-based BlockChain (SBBC). This uses both off-chain and on-chain network components, to solve the issues observed with the blockchain system. Khan *et al.* [130] proposed a blockchain solution based on Ethereum to protect content and transactions. A blockchain-based art trading system named ArtChain was introduced as a pilot project in [121].

3) SUMMARY

Current content trading applications need solutions for the existing problems such as copyright violations, forgery, and falsification in the digital content trading environments. Even though blockchain is an ideal solution for the issues in the content trading domain, due to the scalability concerns, it is difficult to propagate digital content to the blockchain network. Therefore, blockchain-based content trading platforms consisting of off-chain and on-chain network components are introduced as a solution.

VIII. INTEGRATION CHALLENGES OF BLOCKCHAIN

The term blockchain is a leading buzzword in modern day tech world. But, the actual implementations of blockchain technologies are hindered due to various technical limitations mentioned in Table 7 which the research community has been trying to resolve for the last few years. The issues of transaction fee an transaction time are major challenges. The scalability issues of blockchain with respect to transactions and storage are also having a negative impact towards the blockchain adaption. Lack of standards, new security and privacy issues, latest quantum resistance related concerns, intermittent connection issues and other challenges such as regulatory resistance are challenges that should overcome for the widespread use of blockchain technologies in the real world applications such as IoT marketplaces.

A. ISSUE OF TRANSACTION FEE

1) INTRODUCTION

Micro-payments are an essential component in IoT applications as they constantly request data as a service from IoT devices. These transactions need to be compensated with some sort of small, metered, and anonymous payment option. The transaction fee is a major bottleneck in blockchain-based IoT application solutions. Some blockchain solutions require the transaction validators to be compensated. The transaction fees are market-based, which makes them quite expensive.

2) POSSIBLE SOLUTIONS

The on-chain solution is a method to increase scalability by modifying only elements within a blockchain. The transmission cost is lower than the conventional way in this method. But, increasing the block size is not a scalable solution. The off-chain solutions improve scalability by processing the transactions outside the blockchain and solve the transaction cost issues as they are handled outside the blockchain [131]. DAG-based approaches, aiming to provide cheap blockchain services with low latency and high throughput, are emerging as a solution to blockchain transaction fee issue [132].

Fehnker *et al.* [133] analyzes the Bitcoin Unlimited (BTU) in which the transmission limit is higher and the transmission cost is lower than the conventional way. Guo *et al.* [134] provided a detailed analysis of the Bitcoin Lightning Network (LN). The LNs use an off-chain mechanism to reduce transaction fees. Pierro *et al.* [135] analyzed the influence factors on Etherium transaction fee. Yang *et al.* [136] proposed a DAG-based blockchain for resource-constrained VSNs.

3) SUMMARY

In blockchain, once a transaction is created, the user must pay the transaction fee to the minor. This transaction fee is a major issue as light transactions such as micro-payments are a regular occurrence in IoT. On-chain and off-chain solutions are proposed as solutions to current blockchain scalability and transaction fee issues. But, handling the micro-transactions generated by various IoT systems is still an issue. Research community is using DAG-based solutions for various IoT applications as a latest solution.

B. SCALABILITY ISSUE: TRANSACTIONS

1) INTRODUCTION

The PoW concept introduced in initial blockchain applications has the core concept of competing for computation power [137].In PoW, the members in the blockchain need to solve complex problems, purely as a need for evidence, but not as a real requirement for a solution. The resource requirement of this process cannot be catered by IoT devices [138]. So, the transaction time is a problematic issue for many blockchain-based technologies.

2) POSSIBLE SOLUTIONS

Unlike PoW, PoS uses coin age i.e. the contribution to the blockchain network which doesn't require a high computational power [139]. Hafid *et al.* [140] did a comprehensive survey regarding the existing solutions to blockchain scalability. Hazari *et al.* [141] proposed a method using parallel mining which accelerated the process of PoW when compared with solo mining as the maximum of two miners will try to solve a specific block at a given time. Also, in literature, the solutions related to blockchain scalability can be classified into first layer solutions such as sharding, bigger blocks and DAGs and second-layer solutions such as payment channels and side chains [140].

Both PoW and PoS consensus mechanisms avoid forking and maintain a single version of blockchain ledger by slowing down the access rate of new blocks [138]. The use of DAGs is proposed as a solution to decrease transaction time and improve scalability [132]. Instead of arranging the nodes in linear chains, they are arranged as a directed graph in DAGs. The consensus in DAG-based solutions before creating a new node is usually reached by confirming a given number of previous transactions. Hence, it eliminates the requirement of complex consensus mechanisms, ultimately improving the scalability. Yang *et al.* [142] introduced CoDAG which improved the linear structure of traditional blockchain protocol using DAG. CoDAG achieved a throughput of 394 TPS, which is higher than Bitcoin and Ethereum.

3) SUMMARY

The blockchain scalability issue in terms of transactions is a major issue that the research community has been trying to resolve so it will be suitable for IoT applications. We can classify those solutions into two categories as first layer solutions which modify the structure of the blockchain and second layer solutions which include more transactions in a block to increase throughput. The main chain's structure is not changed in second-layer solutions. Therefore, network security is not sacrificed when compared with first-layer solutions. The research community is interested in combining both first and second-layer solutions to achieve higher throughput which is essential for adopting blockchain-based solutions for IoT applications.

C. SCALABILITY: STORAGE

1) INTRODUCTION

Storage capacity and scalability have been deeply questioned in the blockchain. The scalability of storage capacity is another major bottleneck in the blockchain. In typical blockchains, the chain continues to grow. Especially the full nodes need significant storage to store the complete chain. Nodes require more resources as they grow and this reduces the scalability of the system and it can impact the system performance. For example, when the Ethereum blockchain platform is considered, it requires all the nodes in a network to participate in the validation and if the data volume in the application is significant, this results in considerable processing delay [143].

2) POSSIBLE SOLUTIONS

Distributed storage systems can store a large amount of data off the chain. Therefore, it is proposed to combine blockchain with existing distributed storage systems [124]. Block compression techniques are used to reduce some redundant data of a block that has been already stored. Blockchain pruning is used to remove non-critical historical data from the blockchain while preserving the security [144].

The Storage Compression Consensus (SCC) algorithm used by Kim *et al.* [145] compresses a blockchain in each device to prevent storage capacity limitations in lightweight IoT devices. Kim *et al.* [146] proposed a selective compression scheme using a checkpoint-chain to prevent the limitation of accumulating the compression results which needs to validate the retained blocks. Sohan *et al.* [147] proposed a distributed storage system IPFS is used to bypass the storing liabilities and to increase throughput. Matzutt *et al.* [148] developed a scheme named Coin-Prune to prune old-blocks.

3) SUMMARY

Each node in a traditional blockchain needs to process and store the complete transactions to the genesis block. The IoT devices have limited computing and storage resources. Therefore, blockchains cannot be used with most IoT applications due to this limitation. Combining blockchains with existing storage systems allows the solutions to store a large amount of data off the chain.

D. LACK OF STANDARDS

1) INTRODUCTION

The term "blockchain" has been one of the most widely used tech buzzwords and it is evolving rapidly when compared with the attempts to introduce a standardization framework. So, the emerging blockchain technologies are used without proper standardization provided by a recognized international organization [149]. This is causing regulatory bodies not to accept blockchain-based technologies as they might not interoperate with each other and it will be difficult to integrate with traditional information systems as well [150].

2) POSSIBLE SOLUTIONS

A major standardization initiative was initiated on blockchain and distributed ledger technologies through a Technical Committee of the International Organization for Standardization, ISO/TC 307. Other organizations like IEEE1 and the International Telecommunication Union (ITU) have also established standardization efforts on blockchains to identify the needs and responsibilities of their members and stakeholders as users, developers, and operators of this new technology [150].

International Organization for Standardization (ISO) is currently working on 15 work programmes related to the standardization of blockchain technologies and distributed ledger technologies [151]. International Telecommunication Union (ITU) established Application of Distributed Ledger Technology (FG DLT) in May 2017 to identify and analyze DLT-based applications and services related to telecommunication use cases and concluded their work in August 2019 [152]. ITU-T work programme SG20 which is responsible for studies relating to the Internet of things (IoT) and its applications are currently working on blockchain-based applications and frameworks [153].König *et al.* [149] referred to local and international standardization organization's publications and provided a set of comparison criteria for future work and a comparison of the existing standards work.

3) SUMMARY

Standardization improves interoperability and provides a clear view of technical aspects for the industry. The existing issue of lack of standardization and clarity is a major obstacle to the adoption of the technology. Therefore, the standardization of blockchain technology is one of the major steps towards enabling interoperability and obtaining regulatory acceptance of the technology. But, introducing standards to an emerging technology can limit its advancement as well.

E. NEW SECURITY AND PRIVACY ISSUES

1) INTRODUCTION

Blockchain-based IoT systems use encryption and authentication strategies to ensure the security of data. Even though these strategies protect the transaction security of blockchains, the privacy of blockchain-based IoT systems has always been a major concern [154]. Some of the blockchain vulnerabilities are listed below.

- Liveness attack: The confirmation time of a target transaction is delayed in a liveness attack. The three phases of liveness attack are the preparation phase, transaction denial phase, and blockchain retarder phase [59].
- 51% vulnerability: 51% attack can be performed and the entire blockchain can be controlled when a single miner's hashing power is greater than 50% of the total hashing power of the entire blockchain [155], [156].
- Double Spending (DS) attack: When the proportion of computing power possessed by an attacker is higher than that of the honest network, DS attacks can be performed [157]
- Selfish mining: In selfish mining, malicious nodes don't immediately disclose their newly mined blocks and deflect their behavior from the standard pattern [158].
- Smart contract vulnerabilities: If an attack based on a smart contract is successfully executed, it will cause the smart contract to perform in an expected manner and result in losses to the parties involved [159].

2) POSSIBLE SOLUTIONS

The Conflux is a high throughput and fast confirmation blockchain platform which uses a novel consensus protocol to secure against double-spending attacks and liveness attacks [160]. Jang *et al.* [157] analyzed profitable DS attacks and guide how to set a block confirmation number for a safe transaction.

TABLE 7. Impact of blockchain integration challenges to IoT marketplace applications.

Blockchain Integration Challenges	Description	Smart Energy	Smart Agriculture	Smart Government	Smart Health	Smart Cities	Smart Manufacturing	IoV	Content Trading
Transaction fee	The market-based transaction fees required to compensate the validators are quite expensive	H	H	H	H	H	H	H	H
Scalability issue: transactions	The number of transactions that can be performed by most of the blockchain platforms are limited.	H	M	H	H	H	M	H	H
Scalability issue: storage	As the blockchain ledger grows, storage capacity requirement limits the scalability of the system.	H	H	H	H	H	H	H	H
Lack of standards	A well-defined standardized framework for blockchain is not available. Hence, the regulators are reluctant to accept it.	H	L	H	H	H	M	H	M
New security issues	Blockchains are vulnerable to security attacks similar to other ICT systems.	H	H	H	H	H	H	H	H
Privacy issues	The privacy of the data stored in the blocks are not always protected as the data stored in the ledger might be visible to all nodes.	M	L	H	H	H	H	H	H
Quantum resistance	Quantum computing has threatened to expose hash algorithms and other PKI systems.	H	H	H	H	H	H	H	H
Intermittent connections	Continuous network connectivity is not available all the time in all areas.	H	H	H	M	H	L	H	M

H High impact   M Medium impact   L Low impact

Singh *et al.* [27] did a comprehensive survey on the security attacks, challenges, and solutions for the distributed IoT networks. Li *et al.* [59] did a survey on the security of blockchain systems. Chicarino *et al.* [158] presented a simple heuristic to detect the presence of selfish mining attacks in PoW based blockchain networks. Sayeed *et al.* [159] proposed an attack categorization for smart contract vulnerabilities and highlighted the flaws in existing vulnerability detection methodologies. Li *et al.* [160] developed, high throughput and fast confirmation blockchain platform named the Conflux.

3) SUMMARY

Blockchain solutions also face major security concerns. For example, transaction malleability is one of the main security issues and it is caused by delayed information in the hash transaction, DoS attacks are also a common phenomenon, there are attacks that affect privacy and confidentiality of data. A security attack on a critical IoT application can result in major losses. Therefore, when adopting blockchains for IoT applications, its security issues should be addressed properly after analyzing the similar solutions discussed in this research.

F. OTHER CHALLENGES

1) INTERMITTENT CONNECTION

In today's context, many of the services rely on continuous network connectivity. Therefore, communication infrastructure has become a crucial factor. However, 100% population coverage of networks is not available in all areas and even in the areas with coverage, intermittent connectivity is a common issue. Blockchain solutions require continuous network connectivity to constantly exchange data with its peer nodes [161].

A blockchain-based payment scheme can be built using smart contracts, a token-based admission control, account management, and mining rewards distribution for intermittently connected regions [161]. Yining *et al.* [161] proposed a blockchain-based digital payment scheme that can deliver reliable services on top of unreliable networks in remote regions using Etherium. Xiao *et al.* [155] proposed an analytical model which can assess the impact of network connectivity on the PoW blockchain and its impact on consensus security.

IX. LESSONS LEARNED AND FUTURE RESEARCH

In this section, We outline the lessons learned and future research challenges, along with available requirements to improve blockchain-based IoT payment and marketplace solutions.

A. TECHNICAL CHALLENGES

1) LESSONS LEARNED

The traditional e-business models used in IoT related payment and marketplaces have hindered the development of IoT applications. IoT data security and privacy are major concerns when transmiting and storing IoT data. A central payment system managed by a third party is required for IoT solutions and lack of anonymity, high transaction fee, fradulent transaction attempts and static agreements are some of the major technical challenges observed in such solutions.

2) OPEN RESEARCH PROBLEMS

- How to overcome IoT data security and privacy issue?
- What's the best solution to decentralize the IoT platform solutions?
- How to improve anonymity in IoT solutions ?

- How to resolve the transaction fee and scalability hurdles in IoT solutions?

3) PRELIMINARY SOLUTIONS

Data security and privacy can be provided to IoT solutions by using blockchain-based solutions with smart contract and cryptopraphic techniques. Blockchain is a DLT by nature, so central authority can be removed. So, the lack of anonymity and transaction fee related issues can also be overcome by blockchain-based solution which remove the third party from IoT solutions.

4) FUTURE RESEARCH DIRECTIONS

Research community have proposed various DLT and DAG based solutions to address the technical challenges that have limited the true potential of IoT. A single blockchain-based solution for all IoT technical challenges or introducing standardized blockchain-based solutions to resolve specific IoT technical challenges as a guideline will help the development of IoT domain immensely by overcoming its technical challenges. The right balance between blockchain and other cryptographic techniques to ensure data security and privacy need to be identified.

B. APPLICATIONS

1) LESSONS LEARNED

IoT systems connect various smart objects mounted with sensors actuators and software systems which can sense and collect information from the physical environment and then take necessary actions on them. The IoT ecosystem needs a way for sensors and devices to make monetary transactions in exchange for services. Therefore, IoT payment and marketplace requirements exist in various IoT application domain such as autonomous vehicles, smart agriculture, smart cities, smart grid, smart healthcare and content trading. Due to the characteristics such as decentralization, immutability, non-repudiation, traceability and trust of the BCT, they can be applied in all these IoT application domains.

2) OPEN RESEARCH PROBLEMS

- How can the blockchain technology along with modern cryptographic techniques, and edge computing be used in IoT applications ?
- What's the best blockchain-based platform for IoT marketplace requirement of various IoT applications?
- How can IoT application data silos be prevented ?

3) PRELIMINARY SOLUTIONS

Blockchain-based solutions such as HPBC are integrated into secure IoV communications. Various decentralized data marketplaces, focusing on the product smart contract and querying components are introduced in smart cities. Prosumer energy sharing applications use decentralized BCT solutions. Smart health applications use BCT-based data sharing approaches. Content trading is an emerging IoT application where BCT-based solutions were introduced.

4) FUTURE DIRECTIVES

The IoT domain mainly deals with micro-transactions and transaction fee and scalability issues of blockchain are major bottlenecks for IoT applications to use the BCT. Therefore, when developing an IoT marketplace solution for any IoT application domain, latest DLT-based plaforms such as hyperledger fabric or DAG-based platforms such as IOTA need to be considered. Since, IoT applications deal with sensitive information, ensuring privacy in blokchain-based solutions with right balance of BCT and typical cryptographic techniques is a must.

C. INTEGRATION CHALLENGES

1) LESSONS LEARNED

Even though blockchain is highly regarded by research community for IoT applications, the actual implementations of blockchain technologies are hindered due to various technical limitations. The transaction fee that has to be paid to miners is a major obstacle in blockchain-based IoT applications as micro-transactions are a common occurence in IoT domain. The scalability in terms of transactions and storage is another major concern for adopting blcokchain-based solutions. Emerging blockchain technologies are used without proper standardization and this has resulted in lack of trust regarding overall blockchain solutions. Privacy and latest security threats such as liveness attack, 51% vulnerability DS attack and smart contract vulnerabilities need to be addressed. The quantum resistance has threatened core blockchain security implementations which are based on cryptographic and has function related mechanisms. Intermittent connectivity issues observed in rural areas and regulatory concerns can also be considered as significant blockchain integration challenges.

2) OPEN RESEARCH PROBLEMS

- How to reduce the transaction fee required to reward the miners?
- How can the scalability issue of blockchain be resolved ?
- How to standardize the emerging blockchain technologies to gurantee interoperability ?
- How can blockchain survive the privacy and new security threat ?
- Can blockchain survive quantum resistance ?
- Will the rejection of blockchain based solutions by regulatory bodies hinder its development effort ?

3) PRELIMINARY SOLUTIONS

The proposed on-chain solutions tries to resolve the scalability issue by modifying only elements within a blockchain while the off-chain solutions improve the scalability by processing the transactions at outside the blockchain.

The emerging DAG-based approaches are suggested for IoT applications as a solution to blockchain transaction fee issue. ISO and ITU has initiated standardization related directives. Novel conses mechanisms are tested to address blockchain security and privacy issues. The post quantum schemes are adapted by blockchain-based solutions to face quantum resistance.

4) FUTURE DIRECTIVES

The blockchain solutions are vulnerable to various security threats and a standard framework need to be introduced for the application developers to follow, so the vulnerabilities can be minimized. The research community need to analyze the quantum resistance capability of their blockchain-based solutions and improve the solutions to face the inevitable future. The lack of standardization is a main reason for regulatory resistance and this is a major drawback for the widespread usage of blokchain-based IoT application solutions. Hence, a standardization approach similar to the mobile communication technology standards need to be followed for blockchain as well.

D. EMERGING DIRECTIONS

1) QUANTUM RESISTANCE

The cryptographic techniques such as Rivest, Shamir, Adleman (RSA), and Elliptic Curve (EC) are used to secure blockchains by protecting stored data [162]. The latest developments in the quantum computing domain can cause security issues that have never been considered before. For example, Shor's algorithm running on a powerful quantum computer can break the public-key algorithms in polynomial-time [163]. These public-key algorithms can be broken in polynomial-time with Shor's algorithm on a sufficiently powerful quantum computer [163]. Therefore, the usage of both public-key crypto systems and hash functions is threatened by the evolution of quantum computing.

pre-quantum and post-quantum cryptosystems are introduced to withstand the quantum attacks. For example, Code-based - to support error correction codes, multivariant-based - to solve the complex multivariate equations, lattice-based - rely on n-dimensional spaces with a periodic structure, Isogency-based - to withstand the quantum attacks on elliptic curves [163].

Gao *et al.* [164] defined post-quantum blockchain (PQB) and proposed a secure cryptocurrency scheme by combining the lattice-based signature scheme with blockchain together. Fernández-Caramès *et al.* [163] reviewed some of the post-quantum schemes and analyzed their application to the blockchain. A development framework for a scalable, quantum-secured permissioned blockchain named Logicontract (LC) was introduced by Sun *et al.* [165].

The use of blockchain and other DLTs for numerous applications has evolved significantly in the last few years. The main reason for the widespread research interest in blockchain is its characteristics that we discussed in section 2 due to public-key cryptography and hash functions. The fast progress of quantum computing which uses methodologies such as Grover's and Shor's algorithms will be an immense threat to core concepts of blockchain such as public-key cryptography and hash functions. Therefore, the research community needs to closely follow the developments in quantum computing and redesign blockchains to withstand quantum attacks.

2) AI ML INTEGRATION

IoT has been a most widely used technology in the recent past for various application domains. The IoT characteristics and its issues such as security concerns and micro-transactions have paved the way to utilize blockchain, AI and ML to introduce technological improvements in the IoT application domains [166]. Due to the rapid adoption of IoT, an exsessive amount of IoT data is getting generated. Therefore, big data and AI, along with blockchain is vital to accurately analyze IoT data in real-time [167]

Unal *et al.* [168] introduces how blockchain with Federated Learning (FL) can create a secure big data analytics service for IoT. Shahbazi *et al.* [169] applied an integrated methods of blockchain and ML to create a smart manufacturing system. Supriya *et al.* [170] reviewed how the utilization of ML, big data, and blockchain technology is important for the health sector advancements.

X. CONCLUSION

The adoption of IoT applications has hindered due to technical limitations inherited by IoT. These include data security and privacy issues, lack of cooperation among IoT platforms, the requirement of a central payment system, and lack of anonymity. Therefore, IoT applications require a platform with characteristics such as decentralization, immutability, enhanced security, and anonymity to handle their micro-transactions efficiently and cost-effectively. This paper analyzes the technical challenges faced by IoT applications and the suitability of blockchain-based solutions to address those challenges. Especially, the IoT payment transactions and data sharing marketplaces can be deployed by using blockchain-based technologies. In this research paper, we have identified the IoT application areas such as smart health, smart agriculture, IoVs, smart manufacturing, and content trading as some of the major IoT application domains that have shown promising results with blockchain-based solutions. Even though blockchain-based solutions and DAG-based solutions show promising results, they also have integration challenges such as the issue of the transaction fee, scalability issues in terms of transactions and storage, security and privacy issues, and the latest challenge: quantum resistance that needs to be addressed before being the next revolution of IoT to achieve its true potential.

REFERENCES

[1] Statista. *Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025*. Accessed: Nov. 10, 2020. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[2] Y. Cao, T. Jiang, and Z. Han, "A survey of emerging M2M systems: Context, task, and objective," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1246–1258, Dec. 2016.

[3] H. Hejazi, H. Rajab, T. Cinkler, and L. Lengyel, "Survey of platforms for massive IoT," in *Proc. IEEE Int. Conf. Future IoT Technol. (Future IoT)*, Jan. 2018, pp. 1–8.

[4] K. Routh and T. Pal, "A survey on technological, business and societal aspects of Internet of Things by Q3, 2017," in *Proc. 3rd Int. Conf. Internet Things, Smart Innov. Usages (IoT-SIU)*, Feb. 2018, pp. 1–4.

[5] S. Chaudhary, R. Johari, R. Bhatia, K. Gupta, and A. Bhatnagar, "CRAIoT: Concept, review and application(s) of IoT," in *Proc. 4th Int. Conf. Internet Things, Smart Innov. Usages (IoT-SIU)*, Apr. 2019, pp. 1–4.

[6] J. M. Khurpade, D. Rao, and P. D. Sanghavi, "A survey on IoT and 5G network," in *Proc. Int. Conf. Smart City Emerg. Technol. (ICSCET)*, Jan. 2018, pp. 1–3.

[7] A. Raj and S. Prakash, "Internet of everything: A survey based on architecture, issues and challenges," in *Proc. 5th IEEE Uttar Pradesh Sect. Int. Conf. Electr., Electron. Comput. Eng. (UPCON)*, Nov. 2018, pp. 1–6.

[8] Z. Nezami and K. Zamanifar, "Internet of Things/internet of everything: Structure and ingredients," *IEEE Potentials*, vol. 38, no. 2, pp. 12–17, Mar. 2019.

[9] S. Higginbotham and M. Pesce, "Internet of everything: Macro & micro," *IEEE Spectr.*, vol. 58, no. 2, pp. 20–21, Dec. 2021.

[10] E. S. Jung, "4th industrial revolution and boundry: Challenges and opportunities," in *IEDM Tech. Dig.*, Dec. 2018, p. 1.

[11] H. Jung, "Practical approach and applications to the 4th industrial revolution," in *Proc. Int. Conf. Knowl. Smart Technol.*, 2020, p.12.

[12] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[13] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[14] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. M. Leung, "Enabling massive IoT toward 6G: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 15, pp. 11891–11915, Aug. 2021.

[15] T. M. Hewa, A. Kalla, A. Nag, M. E. Ylianttila, and M. Liyanage, "Blockchain for 5G and IoT: Opportunities and challenges," in *Proc. IEEE 8th Int. Conf. Commun. Netw. (ComNet)*, Oct. 2020, pp. 1–8.

[16] Worldometer. *World Population*. Accessed: Feb. 28, 2021. [Online]. Available: https://www.worldometers.info/world-population/

[17] Statista. *Internet of Things (IoT) and Non-IoT Active Device Connections Worldwide From 2010 to 2025*. Accessed: Mar. 6, 2021. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[18] S. Khare and M. Totaro, "Big data in IoT," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, 2019, pp. 1–7.

[19] S. A. Goswami, B. P. Padhya, and K. D. Patel, "Internet of Things: Applications, challenges and research issues," in *Proc. 3rd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Dec. 2019, pp. 47–50.

[20] M. R. M. Kassim, "IoT applications in smart agriculture: Issues and challenges," in *Proc. IEEE Conf. Open Syst. (ICOS)*, Nov. 2020, pp. 19–24.

[21] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[22] CISION. *Internet of Things (IoT) Market Worth USD 1319.08 Billion, Globally, by 2026 at 25.68 Percent CAGR*. Accessed: Nov. 20, 2020. [Online]. Available: https://cutt.ly/cbyrEvu

[23] C. Perera, C. H. Liu, and S. Jayawardena, "The emerging Internet of Things marketplace from an industrial perspective: A survey," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 4, pp. 585–598, Dec. 2015.

[24] 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.

[25] A. Ensor, S. Schefer-Wenzl, and I. Miladinovic, "Blockchains for IoT payments: A survey," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.

[26] 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.

[27] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021.

[28] Datum.org. *Blockchain Data Storage and Monetization*. Accessed: May 23, 2021. [Online]. Available: https://datum.org/

[29] D. Georgakopoulos, P. P. Jayaraman, and A. Dawod, "SenShaMart: A trusted loT marketplace for sensor sharing," in *Proc. IEEE 6th Int. Conf. Collaboration Internet Comput. (CIC)*, Dec. 2020, pp. 8–17.

[30] R. M. Haris and S. Al-Maadeed, "Integrating blockchain technology in 5G enabled IoT: A review," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 367–371.

[31] K. R. Ozyilmaz, M. Dogan, and A. Yurdakul, "IDMoB: IoT data marketplace on blockchain," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2018, pp. 11–19.

[32] S. Bajoudah, C. Dong, and P. Missier, "Toward a decentralized, trust-less marketplace for brokered IoT data trading using blockchain," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 339–346.

[33] W. Badreddine, K. Zhang, and C. Talhi, "Monetization using blockchains for IoT data marketplace," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 1–9.

[34] S. S. Sabry, N. A. Qarabash, and H. S. Obaid, "The road to the Internet of Things: A survey," in *Proc. 9th Annu. Inf. Technol., Electromechanical Eng. Microelectron. Conf. (IEMECON)*, Mar. 2019, pp. 290–296.

[35] D. Choudhary, "Security challenges and countermeasures for the heterogeneity of IoT applications," *J. Auton. Intell.*, vol. 1, no. 2, pp. 16–22, 2019.

[36] H. Rahman and M. I. Hussain, "A comprehensive survey on semantic interoperability for Internet of Things: State-of-the-art and research challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 12, 2020, Art. no. e3902.

[37] U. Khalil, A. Ahmad, A.-H. Abdel-Aty, M. Elhoseny, M. W. A. El-Soud, and F. Zeshan, "Identification of trusted IoT devices for secure delegation," *Comput. Electr. Eng.*, vol. 90, Mar. 2021, Art. no. 106988.

[38] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Appl. Sci.*, vol. 10, no. 12, p. 4102, Jun. 2020.

[39] P. Urien, "Blockchain IoT (BIoT): A new direction for solving Internet of Things security and trust issues," in *Proc. 3rd Cloudification Internet Things (CIoT)*, Jul. 2018, pp. 1–4.

[40] Hyperledger. *Hyperledger-Powered Internet of Things Applications*. Accessed: Apr. 6, 2021. [Online]. Available: https://www.hyperledger.org/blog/2020/07/27/hyperledger-powered-internet-of-things-applications

[41] L. Franke, M. Schletz, and S. Salomo, "Designing a blockchain model for the Paris Agreement's carbon market mechanism," *Sustainability*, vol. 12, no. 3, p. 1068, Feb. 2020.

[42] Allerin. *Your Ultimate Guide to the Quorum Blockchain*. Accessed: Oct. 23, 2021. [Online]. Available: https://www.allerin.com/blog/your-ultimate-guide-to-the-quorum-blockchain

[43] I. T. News. *Will EOS Platform Distrupt the Gaming Industry? A Real Use Case: Hidden Fighters*. Accessed: Jul. 5, 2021. [Online]. Available: https://bit.ly/3mbGBh4

[44] M. Ur Rahman, F. Baiardi, and L. Ricci, "Blockchain smart contract for scalable data sharing in IoT: A case study of smart agriculture," in *Proc. IEEE Global Conf. Artif. Intell. Internet Things (GCAIoT)*, Dec. 2020, pp. 1–7.

[45] BTCManager. *How Ardor Leverages Blockchain Technology for Real-World Use Cases*. Accessed: Jun. 23, 2021. [Online]. Available: https://btcmanager.com/ardor-leverages-blockchain-technology-real-world/

[46] IOTA. *Building Industrial IoT With IOTA: Introduction and How IOTA Works*. Accessed: Apr. 1, 2021. [Online]. Available: https://www.simform.com/industrial-iot-iota-part-1/

[47] F. A. Abadi, J. Ellul, and G. Azzopardi, "The blockchain of things, beyond bitcoin: A systematic review," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1666–1672.

[48] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.

[49] H. S. Kim and K. Wang, "Immutability measure for different blockchain structures," in *Proc. IEEE 39th Sarnoff Symp.*, Sep. 2018, pp. 1–6.

[50] A. Draper, A. Familrouhani, D. Cao, T. Heng, and W. Han, "Security applications and challenges in blockchain," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–4.

[51] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.

[52] *ETSI Executive Briefing—Mobile Edge Computing (MEC) Initiative*, Eur. Telecommun. Standards Inst. (ETSI), 2014. [Online]. Available: https://portal.etsi.org/portals/0/tbpages/mec/docs/mec%20executive%20brief%20v1%2028-09-14.pdf

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

[54] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, ''Recent advances in smart contracts: A technical overview and state of the art,'' *IEEE Access*, vol. 8, pp. 117782–117801, 2020.

[55] A. Manimuthu, R. V. Sreedharan, and D. Marwaha, ''A literature review on bitcoin: Transformation of crypto currency into a global phenomenon,'' *IEEE Eng. Manage. Rev.*, vol. 47, no. 1, pp. 28–35, 1st Quart., 2019.

[56] W. Li and M. He, ''Comparative analysis of bitcoin, ethereum, and libra,'' in *Proc. IEEE 11th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Oct. 2020, pp. 545–550.

[57] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, ''Bitcoin and blockchain: Security and privacy,'' *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10288–10313, Oct. 2020.

[58] Ethereum.org. *Consensus Mechanisms*. Accessed: May 30, 2021. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/

[59] D. Li, W. E. Wong, and J. Guo, ''A survey on blockchain for enterprise using hyperledger fabric and composer,'' in *Proc. 6th Int. Conf. Dependable Syst. Appl. (DSA)*, Jan. 2020, pp. 71–80.

[60] Hyperledger.org. *What is Hyperledger?* Accessed: Jun. 20, 2021. [Online]. Available: https://www.hyperledger.org/

[61] Hyperledger.org. *Hyperledger Fabric*. Accessed: Jun. 20, 2021. [Online]. Available: https://www.iota.org/get-started/what-is-iota

[62] Iota.org. *Hyperledger Fabric*. Accessed: Jun. 20, 2021. [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2020/03/hyperledger_fabric_whitepaper.pdf

[63] Eos.io. *EOSIO for developers*. Accessed: Jun. 21, 2021. [Online]. Available: https://eos.io/for-developers/

[64] S. Benahmed, I. Pidikseev, R. Hussain, J. Lee, S. M. A. Kazmi, A. Oracevic, and F. Hussain, ''A comparative analysis of distributed ledger technologies for smart contract development,'' in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–6.

[65] Cardano.org. *Discover Cardano*. Accessed: Jun. 21, 2021. [Online]. Available: https://cardano.org/discover-cardano/

[66] A. Pouraghily and T. Wolf, ''A lightweight payment verification protocol for blockchain transactions on IoT devices,'' in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 617–623.

[67] Y. Zhang, X. Xu, A. Liu, Q. Lu, L. Xu, and F. Tao, ''Blockchain-based trust mechanism for IoT-based smart manufacturing system,'' *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 6, pp. 1386–1394, Dec. 2019.

[68] J. Leng, S. Ye, M. Zhou, J. L. Zhao, Q. Liu, W. Guo, W. Cao, and L. Fu, ''Blockchain-secured smart manufacturing in Industry 4.0: A survey,'' *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 1, pp. 237–252, Jan. 2021.

[69] S. Umamaheswari, S. Sreeram, N. Kritika, and D. R. J. Prasanth, ''BIoT: Blockchain based IoT for agriculture,'' in *Proc. 11th Int. Conf. Adv. Comput. (ICoAC)*, Dec. 2019, pp. 324–327.

[70] S. Lu, X. Wang, and J. Zheng, ''Research on agricultural Internet of Things data sharing system based on blockchain,'' in *Proc. 35th Youth Acad. Annu. Conf. Chin. Assoc. Autom. (YAC)*, Oct. 2020, pp. 221–225.

[71] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, ''A blockchain-based energy trading platform for smart Homes in a microgrid,'' in *Proc. 3rd Int. Conf. Comput. Commun. Syst. (ICCCS)*, Apr. 2018, pp. 472–476.

[72] S. Dekhane, K. Mhalgi, K. Vishwanath, S. Singh, and N. Giri, ''Green-Coin: Empowering smart cities using blockchain 2.0,'' in *Proc. Int. Conf. Nascent Technol. Eng. (ICNTE)*, Jan. 2019, pp. 1–5.

[73] M. R. Hamouda, M. E. Nassar, and M. M. A. Salama, ''A novel energy trading framework using adapted blockchain technology,'' *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2165–2175, May 2021.

[74] S. M. S. Hussain, S. M. Farooq, and T. S. Ustun, ''Implementation of blockchain technology for energy trading with smart meters,'' in *Proc. Innov. Power Adv. Comput. Technol. (i-PACT)*, Mar. 2019, pp. 1–5.

[75] T. Ha, D. Lee, C. Lee, and S. Cho, ''VCG auction mechanism based on block chain in smart grid,'' in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2021, pp. 465–468.

[76] V. Jaiman and V. Urovi, ''A consent model for blockchain-based health data sharing platforms,'' *IEEE Access*, vol. 8, pp. 143734–143745, 2020.

[77] A. Dubovitskaya, P. Novotny, Z. Xu, and F. Wang, ''Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review,'' *Oncology*, vol. 98, no. 6, pp. 403–411, 2020.

[78] A. Alsharif and M. Nabil, ''A blockchain-based medical data marketplace with trustless fair exchange and access control,'' in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.

[79] N. Kumar S. and M. Dakshayini, ''Secure sharing of health data using hyperledger fabric based on blockchain technology,'' in *Proc. Int. Conf. Mainstreaming Block Chain Implement. (ICOMBI)*, Feb. 2020, pp. 1–5.

[80] S. M. Hatim, S. J. Elias, R. M. Ali, J. Jasmis, A. A. Aziz, and S. Mansor, ''Blockchain-based internet of vehicles (BIoV): An approach towards smart cities development,'' in *Proc. 5th IEEE Int. Conf. Recent Adv. Innov. Eng. (ICRAIE)*, Dec. 2020, pp. 1–4.

[81] Accenture. *Value of Data: The Dawn of the Data Marketplace*. Accessed: Mar. 6, 2021. [Online]. Available: https://www.accenture.com/us-en/insights/high-tech/dawn-of-data-marketplace

[82] BDEX. *BDEX*. Accessed: Dec. 8, 2020. [Online]. Available: https://www.bdex.com

[83] DAWEX. *DAWEX*. Accessed: Dec. 8, 2020. [Online]. Available: https://www.dawex.com/en

[84] G. S. Ramachandran, R. Radhakrishnan, and B. Krishnamachari, ''Towards a decentralized data marketplace for smart cities,'' in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Sep. 2018, pp. 1–8.

[85] P. Gupta, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, ''Towards a blockchain powered IoT data marketplace,'' in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2021, pp. 366–368.

[86] A. Oleksiuk. *IoT Payments: What's Ahead for Contextual Commerce?* Accessed: Dec. 20, 2020. [Online]. Available: https://www.intellias.com/iot-payments-what-s-ahead-for-contextual-commerce/

[87] Visa. *Cashless Cities*. Accessed: Dec. 21, 2020. [Online]. Available: https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-cashless-cities-report.pdf

[88] Vox. *Amazon's Cashierless Go Stores Could be a USD 4 Billion Business by 2021, New Research Suggests*. Accessed: Dec. 22, 2020. [Online]. Available: https://www.vox.com/2019/1/4/18166934/amazon-go-stores-revenue-estimates-cashierless

[89] I. Colak, R. Bayindir, and S. Sagiroglu, ''The effects of the smart grid system on the national grids,'' in *Proc. 8th Int. Conf. Smart Grid (icSmartGrid)*, Jun. 2020, pp. 122–126.

[90] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, ''A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes,'' *IEEE Access*, vol. 8, pp. 118433–118471, 2020.

[91] A. S. Sangeetha, S. Shunmugan, and G. Murugan, ''Blockchain for IoT enabled supply chain management—A systematic review,'' in *Proc. 4th Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Oct. 2020, pp. 48–52.

[92] A. Said, ''The economic impact of digital fiat currency (DFC): Opportunities and challenges,'' in *Proc. 2nd Eur. Middle East, North African Regional Conf. Int. Telecommun. Soc. (ITS)*, 2019, pp. 1–12. [Online]. Available: http://hdl.handle.net/10419/201744

[93] S. El-Hage and G. Holst, ''Micropayments between IoT devices: A qualitative study analyzing the usability of DLT: s in an IoT environment,'' KTH Roy. Inst. Technol., Stockholm, Sweden, Tech. Rep., 2018. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1272048/FULLTEXT01.pdf

[94] M. Zouina and B. Outtai, ''Towards a distributed token based payment system using blockchain technology,'' in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Apr. 2019, pp. 1–10.

[95] X. Han, Y. Yuan, and F.-Y. Wang, ''A blockchain-based framework for central bank digital currency,'' in *Proc. IEEE Int. Conf. Service Operations Logistics, Informat. (SOLI)*, Nov. 2019, pp. 263–268.

[96] M. Singh, A. Singh, and S. Kim, ''Blockchain: A game changer for securing IoT data,'' in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 51–55.

[97] M. B. Yassein, F. Shatnawi, S. Rawashdeh, and W. Mardin, ''Blockchain technology: Characteristics, security and privacy; issues and solutions,'' in *Proc. IEEE/ACS 16th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2019, pp. 1–8.

[98] T. T. Huynh, T. D. Nguyen, and H. Tan, ''A survey on security and privacy issues of blockchain technology,'' in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, Jul. 2019, pp. 362–367.

[99] T. H.-J. Kim and J. Lampkins, ''SSP: Self-sovereign privacy for Internet of Things using blockchain and MPC,'' in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 411–418.

[100] A. Fitwi, Y. Chen, and S. Zhu, "A lightweight blockchain-based privacy protection for smart surveillance at the edge," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 552–555.

[101] S. Soursos, I. P. Žarko, P. Zwickl, I. Gojmerac, G. Bianchi, and G. Carrozzo, "Towards the cross-domain interoperability of IoT platforms," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2016, pp. 398–402.

[102] ARCTOUCH. *A Blockchain Consulting and Development Company With a Track Record of Digital Leadership*. Accessed: Jun. 30, 2021. [Online]. Available: https://arctouch.com/services/blockchain-developers/

[103] Xage. *Zero Trust Security for the Real World*. Accessed: Oct. 1, 2021. [Online]. Available: https://xage.com/

[104] CRONICLED. *Automating Transactions Between Trading Partners in the Life Sciences Industry Through the MediLedger Network*. Accessed: Jul. 1, 2021. [Online]. Available: https://www.chronicled.com/

[105] NetObjex. *Digital Twin Automation on Demand Using AI, IoT and Blockchain*. Accessed: Jul. 1, 2021. [Online]. Available: https://www.netobjex.com/

[106] Helium. *People Powered Networks*. Accessed: Sep. 11, 2021. [Online]. Available: https://www.helium.com/

[107] Coindesk. *Blockchain Biometrics Startup Raises $3 Million in New Funding*. Accessed: Jul. 1, 2021. [Online]. Available: https://www.coindesk.com/blockchain-biometrics-startup-new-funding

[108] NebulaGenomics. *Technology at Nebula Genomics*. Accessed: Jul. 1, 2021. [Online]. Available: https://nebula.org/technology/

[109] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[110] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT data management using BlockChain and trusted execution environment," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Jul. 2018, pp. 15–22.

[111] N. Chanthong, T. Ruangsakorn, and S. Glomglome, "Blockchain and smart contract payment for electric vehicle charging," in *Proc. 17th Int. Conf. Electr. Eng., Electron., Comput., Telecommun. Inf. Technol. (ECTI-CON)*, Jun. 2020, pp. 161–164.

[112] T. Dimitriou and A. Mohammed, "Fair and privacy-respecting bitcoin payments for smart grid data," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10401–10417, Oct. 2020.

[113] N. Papadis and L. Tassiulas, "Blockchain-based payment channel networks: Challenges and recent advances," *IEEE Access*, vol. 8, pp. 227596–227609, 2020.

[114] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Structural Biotechnol. J.*, vol. 16, pp. 224–230, Sep. 2018.

[115] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Softw.*, vol. 35, no. 4, pp. 95–99, Jul./Aug. 2018.

[116] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K.-R. Choo, "DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2440–2452, 2020.

[117] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[118] P. K. Lahiri, D. Das, W. Mansoor, S. Banerjee, and P. Chatterjee, "A trustworthy blockchain based framework for impregnable IoV in edge computing," in *Proc. IEEE 17th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Dec. 2020, pp. 26–31.

[119] S. Sharma, K. K. Ghanshala, and S. Mohan, "Blockchain-based internet of vehicles (IoV): An efficient secure ad hoc vehicular networking architecture," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 452–457.

[120] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, "A trusted blockchain-based traceability system for fruit and vegetable agricultural products," *IEEE Access*, vol. 9, pp. 36282–36293, 2021.

[121] Z. Wang, L. Yang, Q. Wang, D. Liu, Z. Xu, and S. Liu, "ArtChain: Blockchain-enabled platform for art marketplace," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 447–454.

[122] D. E. Majdoubi, H. El Bakkali, and S. Sadki, "Towards smart blockchain-based system for privacy and security in a smart city environment," in *Proc. 5th Int. Conf. Cloud Comput. Artif. Intelligence: Technol. Appl. (CloudTech)*, Nov. 2020, pp. 1–7.

[123] S. Loss, N. Cacho, J. M. D. Valle, and F. Lopes, "Orthus: A blockchain platform for smart cities," in *Proc. IEEE Int. Smart Cities Conf. (ISC)*, Oct. 2019, pp. 212–217.

[124] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, Sep. 2019.

[125] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 8–14, Jan. 2020.

[126] F. Firouzi, B. Farahani, M. Barzegari, and M. Daneshmand, "AI-driven data monetization: The other face of data in IoT-based smart and connected health," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5581–5599, Apr. 2022.

[127] J. Li, A. Grintsvayg, J. Kauffman, and C. Fleming, "LBRY: A blockchain-based decentralized digital content marketplace," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures (DAPPS)*, Aug. 2020, pp. 42–51.

[128] M. Zeilinger, "Digital art as 'Monetised graphics': Enforcing intellectual property on the blockchain," *Philosophy Technol.*, vol. 31, no. 1, pp. 15–41, Mar. 2018.

[129] G. Heo, D. Yang, I. Doh, and K. Chae, "Efficient and secure blockchain system for digital content trading," *IEEE Access*, vol. 9, pp. 77438–77450, 2021.

[130] U. Khan, Z. Y. An, and A. Imran, "A blockchain ethereum technology-enabled digital content: Development of trading and sharing economy data," *IEEE Access*, vol. 8, pp. 217045–217056, 2020.

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

[132] T. Wang, Q. Wang, Z. Shen, Z. Jia, and Z. Shao, "Understanding intrinsic characteristics and system implications of DAG-based blockchain," in *Proc. IEEE Int. Conf. Embedded Softw. Syst. (ICESS)*, Dec. 2020, pp. 1–6.

[133] A. Fehnker and K. Chaudhary, "Twenty percent and a few days–optimising a bitcoin majority attack," in *Proc. NASA Formal Methods Symp.* Cham, Switzerland: Springer, 2018, pp. 157–163.

[134] Y. Guo, J. Tong, and C. Feng, "A measurement study of bitcoin lightning network," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 202–211.

[135] G. A. Pierro and H. Rocha, "The influence factors on ethereum transaction fees," in *Proc. IEEE/ACM 2nd Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, May 2019, pp. 24–31.

[136] W. Yang, X. Dai, J. Xiao, and H. Jin, "LDV: A lightweight DAG-based blockchain for vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5749–5759, Jun. 2020.

[137] P. R. Nair and D. R. Dorai, "Evaluation of performance and security of proof of work and proof of stake using blockchain," in *Proc. 3rd Int. Conf. Intell. Commun. Technol. Virtual Mobile Netw. (ICICV)*, Feb. 2021, pp. 279–283.

[138] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, "When Internet of Things meets blockchain: Challenges in distributed consensus," *IEEE Netw.*, vol. 33, no. 6, pp. 133–139, Nov./Dec. 2019.

[139] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities," *IEEE Access*, vol. 7, pp. 85727–85745, 2019.

[140] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125244–125262, 2020.

[141] S. Shahriar Hazari and Q. H. Mahmoud, "Improving transaction speed and scalability of blockchain systems via parallel proof of work," *Future Internet*, vol. 12, no. 8, p. 125, Jul. 2020.

[142] S. Yang, Z. Chen, L. Cui, M. Xu, Z. Ming, and K. Xu, "CoDAG: An efficient and compacted DAG-based blockchain protocol," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 314–318.

[143] 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.

[144] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.

[145] T. Kim, J. Noh, and S. Cho, "SCC: Storage compression consensus for blockchain in lightweight IoT network," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2019, pp. 1–4.

[146] T. Kim, S. Lee, Y. Kwon, J. Noh, S. Kim, and S. Cho, "SELCOM: Selective compression scheme for lightweight nodes in blockchain system," *IEEE Access*, vol. 8, pp. 225613–225626, 2020.

[147] M. S. H. Sohan, M. Mahmud, M. A. B. Sikder, F. S. Hossain, and M. R. Hasan, "Increasing throughput and reducing storage bloating problem using IPFS and dual-blockchain method," in *Proc. 2nd Int. Conf. Robot., Electr. Signal Process. Techn. (ICREST)*, Jan. 2021, pp. 732–736.

[148] R. Matzutt, B. Kalde, J. Pennekamp, A. Drichel, M. Henze, and K. Wehrle, "CoinPrune: Shrinking bitcoin's blockchain retrospectively," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 3, pp. 3064–3078, Sep. 2021.

[149] L. König, Y. Korobeinikova, S. Tjoa, and P. Kieseberg, "Comparing blockchain standards and recommendations," *Future Internet*, vol. 12, no. 12, p. 222, Dec. 2020.

[150] V. Gramoli and M. Staples, "Blockchain standard: Can we reach consensus?" *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 16–21, Sep. 2018.

[151] ISO. *ISO/TC 307, Blockchain and Distributed Ledger Technologies*. Accessed: May 23, 2021. [Online]. Available: https://www.iso.org/committee/6266604.html

[152] ITU. *Focus Group on Application of Distributed Ledger Technology*. Accessed: May 24, 2021. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

[153] ITU. *ITU-T Work Programme*. Accessed: May 24, 2021. [Online]. Available: https://www.itu.int/itu-t/workprog/wp_search.aspx?isn_sp=3925&isn_sg=3937&isn_status=-1,1,3,7&title=blockchain

[154] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019.

[155] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "Modeling the impact of network connectivity on consensus security of proof-of-work blockchain," in *Proc. IEEE IEEE Conf. Comput. Commun.*, Jul. 2020, pp. 1648–1657.

[156] S. Lee and S. Kim, "Short selling attack: A self-destructive but profitable 51% attack on PoS blockchains," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 19, Sep. 2020.

[157] J. Jang and H. N. Lee, "Profitable double-spending attacks," *Appl. Sci.*, vol. 10, no. 23, p. 8477, 2020.

[158] V. Chicarino, C. Albuquerque, E. Jesus, and A. Rocha, "On the detection of selfish mining and stalker attacks in blockchain networks," *Ann. Telecommun.*, vol. 75, no. 3, pp. 1–10, 2020.

[159] S. Sayeed, H. Marco-Gisbert, and T. Caira, "Smart contract: Attacks and protections," *IEEE Access*, vol. 8, pp. 24416–24427, 2020.

[160] C. Li, P. Li, D. Zhou, Z. Yang, M. Wu, G. Yang, W. Xu, F. Long, and A. C.-C. Yao, "A decentralized blockchain with high throughput and fast confirmation," in *Proc. Annu. Tech. Conf. (USENIX)*, 2020, pp. 515–528.

[161] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "A delay-tolerant payment scheme based on the ethereum blockchain," *IEEE Access*, vol. 7, pp. 33159–33172, 2019.

[162] J. J. Kearney and C. A. Perez-Delgado, "Vulnerability of blockchain technologies to quantum attacks," 2021, *arXiv:2105.01815*.

[163] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

[164] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.

[165] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, "Towards quantum-secured permissioned blockchain: Signature, consensus, and logic," *Entropy*, vol. 21, no. 9, p. 887, Sep. 2019.

[166] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100227.

[167] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.

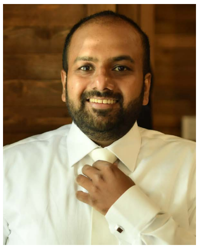
[168] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, and R. Hamila, "Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things," *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102393.

[169] Z. Shahbazi and Y.-C. Byun, "Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing," *Sensors*, vol. 21, no. 4, p. 1467, Feb. 2021.

[170] S. M. and V. K. Chattu, "A review of artificial intelligence, big data, and blockchain technology applications in medicine and global health," *Big Data Cognit. Comput.*, vol. 5, no. 3, p. 41, Sep. 2021.

AMILA SAPUTHANTHRI (Member, IEEE) received the B.Sc. degree (Hons.) in electronic and telecommunication engineering and the M.Sc. degree in telecommunications from the University of Moratuwa, Moratuwa, Sri Lanka, in 2014 and 2019, respectively. He is currently pursuing the Ph.D. degree in electrical and electronic engineering with the University of Sri Jayewardenepura, Ratmalana, Sri Lanka. He is also working as a Lead Engineer at Dialog Axiata PLC. His research interests include telecommunication, cloud computing, the IoT, and blockchain.

CHAMITHA DE ALWIS (Senior Member, IEEE) received the B.Sc. degree (Hons.) in electronic and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2009, and the Ph.D. degree in electronic engineering from the University of Surrey, U.K., in 2014. He is currently a Senior Lecturer and the Head of the Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Sri Jayewardenepura, Sri Lanka. He also provides consultancy services in the areas of telecommunication, 4G, 5G, IoT, and network security. He has published over 20 peer-reviewed articles, contributed to various national and international projects related to ICT, and served as a reviewer and a TPC member in several international journals and conferences. He has also worked as a Consultant at the Telecommunication Regulatory Commission of Sri Lanka, an Advisor in IT services with the University of Surrey, and a Radio Network Planning and Optimization Engineer at Mobitel, Sri Lanka. His research interests include 5G, 6G, the IoT, blockchain, and network security.



MADHUSANKA LIYANAGE (Senior Member, IEEE) received the B.Sc. degree (Hons.) in electronics and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Thailand, in 2011, the M.Sc. degree from the University of Nice Sophia Antipolis, France, in 2011, and the Doctor of Technology degree in communication engineering from the University of Oulu, Finland, in 2016. From 2011 to 2012, he worked a Research Scientist at the I3S Laboratory and Inria, Shopia Antipolis, France. He is currently an Assistant Professor/an Ad Astra Fellow at the School of Computer Science, University College Dublin, Ireland. He is also acting as an Adjunct Processor at the Center for Wireless Communications, University of Oulu. From 2015 to 2018, he was a Visiting Research Fellow at CSIRO, Australia, the Infolabs21, Lancaster University, U.K., the Department of Computer Science and Engineering, The University of New South Wales, Australia, the School of IT, University of Sydney, Australia, the LIP6, Sorbonne University, France, and the Department of Computer Science and Engineering, University of Oxford, U.K. His research interests include 5G/6G, SDN, the IoT, blockchain, MEC, mobile, and virtual network security. He was also a recipient of Prestigious Marie Skłodowska-Curie Actions Individual Fellowship, from 2018 to 2020. He has received "2020 IEEE ComSoc Outstanding Young Researcher" Award by IEEE ComSoc EMEA and "2022 The Tom Brazil Excellence in Research Award" by SFI CONNECT Center. For more information visit the link (http://www.madhusanka.com).