sustainability

Review

Blockchain-Enabled Smart Grid Applications: Architecture, Challenges, and Solutions

Bhargav Appasani [1], Sunil Kumar Mishra [1], Amitkumar V. Jha [1], Santosh Kumar Mishra [1], Florentina Magda Enescu [2], Ioan Sorin Sorlei [3], Fernando Georgel Bîrleanu [4], Noureddine Takorabet [5], Phatiphat Thounthong [5,6] and Nicu Bizon [2,3,4,*]

[1] School of Electronics Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar 751024, India; bhargav.appasanifet@kiit.ac.in (B.A.); sunil.mishrafet@kiit.ac.in (S.K.M.); amit.jhafet@kiit.ac.in (A.V.J.); 2081108@kiit.ac.in (S.K.M.)

[2] Faculty of Electronics, Communication and Computers, University of Pitesti, 110040 Pitesti, Romania; florentina.enescu@upit.ro

[3] ICSI Energy, National Research and Development Institute for Cryogenic and Isotopic Technologies, 240050 Ramnicu Valcea, Romania; sorin.sorlei@icsi.ro

[4] Doctoral School, University Politehnica of Bucharest, Splaiul Independentei Street no. 313, 060042 Bucharest, Romania; birleanu.fernando@gmail.com

[5] Group of Research in Electrical Engineering of Nancy (GREEN), University of Lorraine, 2 Avenue de la Forêt de Haye, 54518 Vandeuvre lès Nancy, CEDEX, F-54000 Nancy, France; noureddine.takorabet@univ-lorraine.fr (N.T.); phatiphat.t@fte.kmutnb.ac.th (P.T.)

[6] Renewable Energy Research Centre (RERC), Department of Teacher Training in Electrical Engineering, Faculty of Technical Education, King Mongkut's University of Technology North Bangkok, 1518 Pracharat 1 Road, Wongsawang, Bangsue, Bangkok 10800, Thailand

[*] Correspondence: nicu.bizon@upit.ro

check for updates

Citation: Appasani, B.; Mishra, S.K.; Jha, A.V.; Mishra, S.K.; Enescu, F.M.; Sorlei, I.S.; Bîrleanu, F.G.; Takorabet, N.; Thounthong, P.; Bizon, N. Blockchain-Enabled Smart Grid Applications: Architecture, Challenges, and Solutions. *Sustainability* **2022**, *14*, 8801. https://doi.org/10.3390/su14148801

Academic Editor: Thanikanti Sudhakar Babu

Received: 11 April 2022
Accepted: 14 July 2022
Published: 18 July 2022

Abstract: The conventional electrical grid is undergoing substantial growth for reliable grid operation and for more efficient and sustainable energy use. The traditional grid is now metamorphosing into a smart grid (SG) that incorporates a diverse, heterogeneous blend of operating measures such as smart appliances, meters, and renewable energy resources. With better efficient results and dependability, the SG can be described as a modern electric power grid architecture. The SG is one of the greatest potential advances as a promising solution for the energy crisis. However, it is complex and its decentralization could be of tremendous benefit. Moreover, digitalization and integration of a large number of growing connections make it a target of cyber-attacks. In this sense, blockchain is a promising SG paradigm solution that offers several excellent features. There has been considerable effort put into using blockchains in the smart grid for its decentralization and enhanced cybersecurity; however, it has not been thoroughly studied in both application and architectural perspectives. An in-depth study was conducted on blockchain-enabled SG applications. Blockchain architectures for various applications, such as the synchrophasor applications, electric vehicles, energy management systems, etc., were proposed. The purpose of this article is to provide directions for future research efforts aimed at secure and decentralized SG applications using blockchain.

Keywords: smart grid; blockchain; smart contracts; cybersecurity; microgrids; electric vehicles; energy transactions; energy management; smart cities; advanced metering infrastructure; home automation; smart homes

1. Introduction

The power grid is a complex engineering marvel, which is undergoing rapid changes due to the proliferation of renewable energy resources, high-speed signal processors, and intelligent sensors, etc. The present requirement involves bi-directional flow energy and information between the power generators and the power consumers. So, the traditional power grid is evolving into a smart grid (SG), a grid that is capable of dynamically monitoring and controlling the flow of power, providing reliable power to the consumers [1].

The SG connects heterogeneous components that vary in their functionality and requirements. These components include renewable and non-renewable energy sources, intelligent sensors, controllers, etc. The statistics on research publications related to the SG are shown in Figure 1. These statistics were obtained from the Scopus database. The various applications that the SG caters to are shown in Figure 2. In Figure 2, the share of research publications from the application's perspective is shown. From this figure, it can be observed that the main applications in an SG are the energy management systems (EMS), electric vehicles (EVs), microgrids (MGs), smart cities (SCs), home automation (HA), advanced metering infrastructure (AMI), and synchrophasor applications (SPAs) [2].

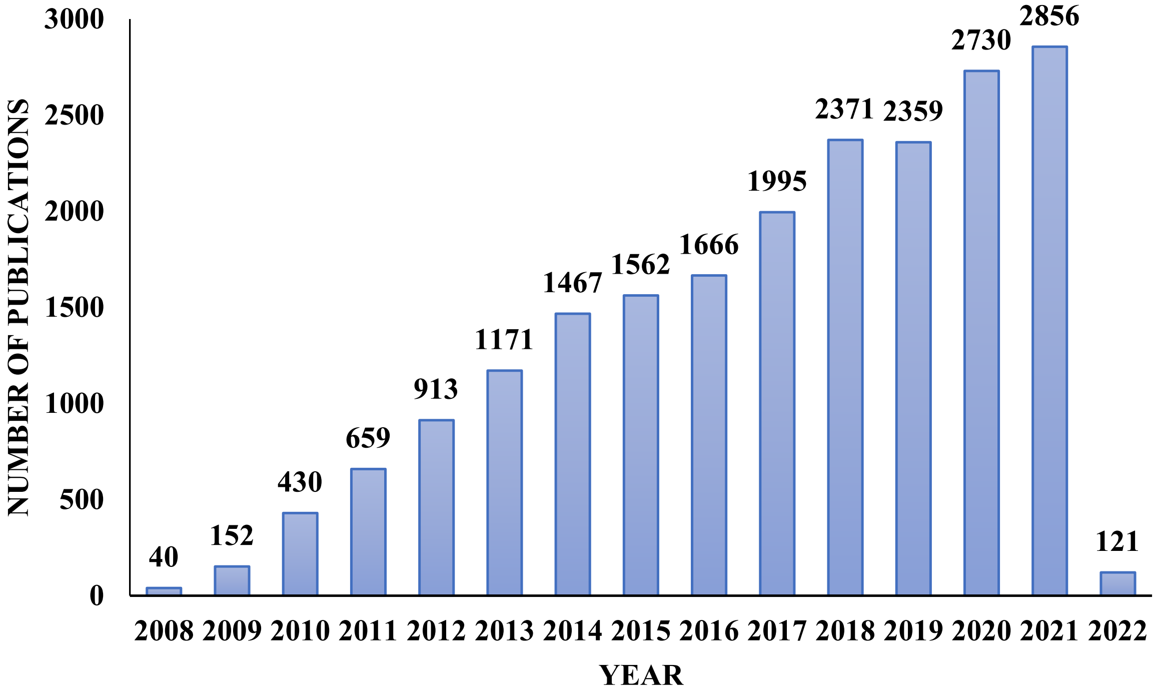

Figure 1. Publication statistics on SG.

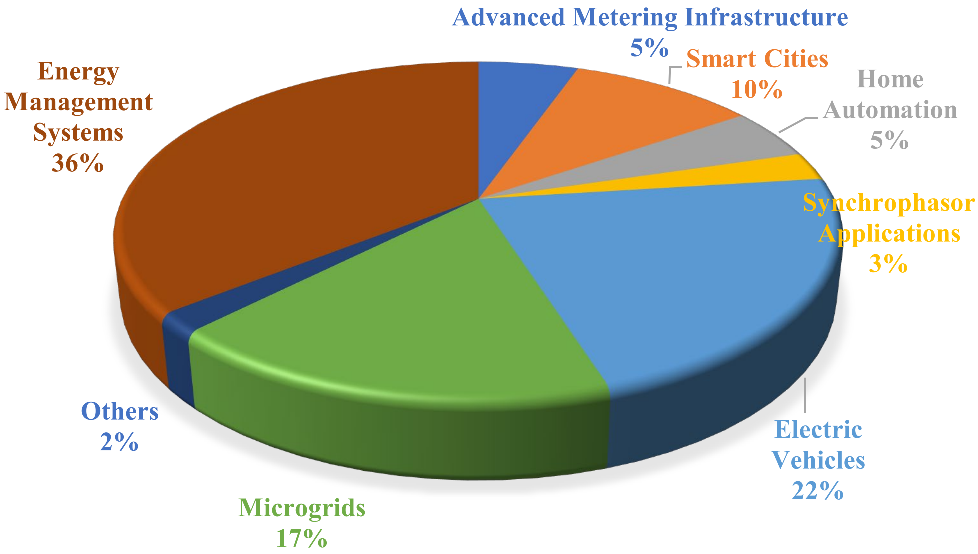

Figure 2. Distribution of research related to SG.

SG enhances the reliability of power supply and materializes several applications at the cost of increased complexity [3]. In this complex network, at a given instance, there are several entities in the grid that carry out transactions. An important concern is validating a transaction between the various entities involved in a particular SG application. A promising and secure solution for this problem is the use of Blockchain technology.

Blockchain technology, first introduced by Satoshi Nakamoto, helps achieve consensus about the authenticity of a particular transaction and helps maintain trust between various entities involved [4]. The number of papers published on blockchain technology every year is shown in Figure 3. Additionally, the corresponding number of papers published on Blockchain for SG is shown in this figure. The publication statistics were obtained from the Scopus database.

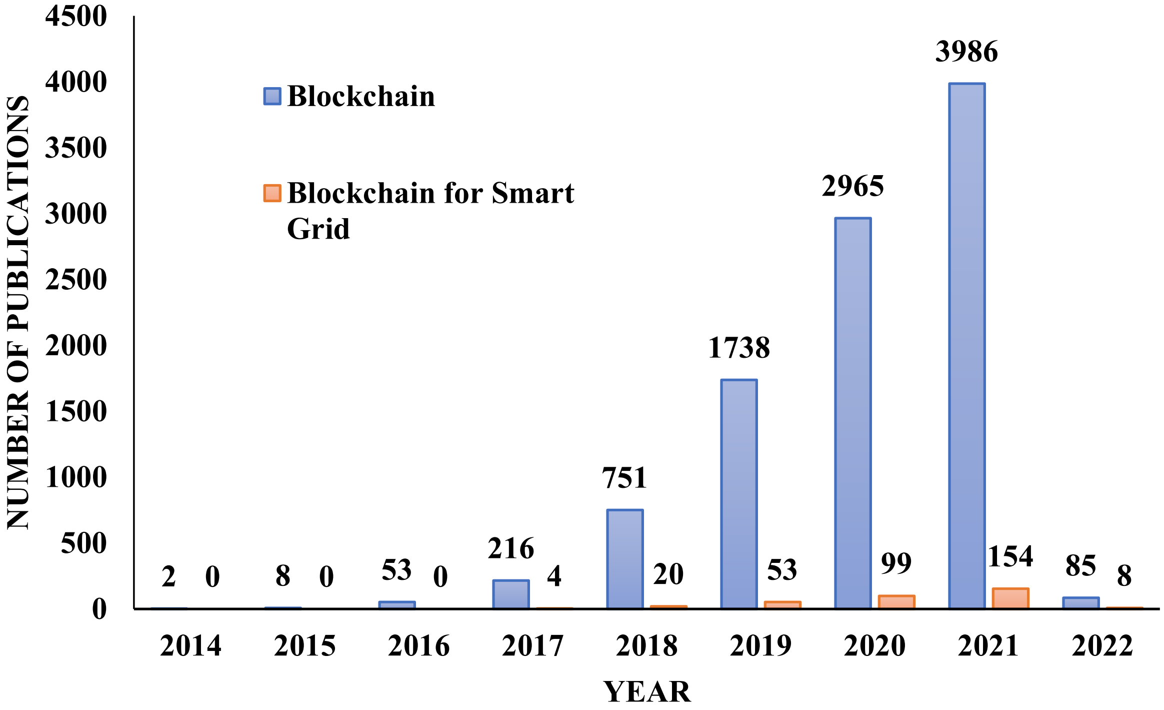

Figure 3. Publication statistics on blockchain and blockchain for SG.

The statistics indicate that blockchain technology is not being exploited for SG applications. Only 3.5% of publications on the blockchain are related to the SG applications. The motivation for this review was to explore the research available on the blockchain for SG, categorize it based on the application, propose the blockchain architectures for the various SG applications, identify the challenges in this regard, and suggest suitable solutions. The review papers and surveys on blockchain for SG are summarized in Table 1. Contrary to these works, the present work presents a boarder perspective on different SG applications with the blockchain. Moreover, the present work also describes the architecture of the blockchain-enabled SG applications. A wide range of potential applications of SG is considered, such as EV, AMI, SPA, MGs, SCs, HA, and EMS.

The paper is organized in the following sections, as represented in Figure 4. Section 2 discusses the basic concepts of a blockchain. It presents the terminology related to the blockchain and its general architecture. Section 3 presents a review of the blockchain-enabled SG applications. Different applications are discussed, and their architectures are presented. The security concerns pertaining to these applications are discussed in Section 4, and Section 5 is the conclusion of this review.

Table 1. Existing reviews on blockchain for SG. "✓" and "×" indicates "included" and "excluded" respectively in literature.

Reference	Blockchain from an SG Application Perspective			SG Applications Considered						
	Architecture	Security	General	EVs	AMI	SPA	MGs	SCs	HA	EMS
[4]	×	×	✓	×	×	×	✓	×	×	✓
[5]	×	×	✓	✓	×	×	×	×	×	×
[6]	×	×	×	×	×	×	×	×	×	✓
[7]	×	×	✓	×	×	×	×	×	✓	×
[8]	×	✓	×	✓	×	×	×	×	×	✓
[9]	×	✓	✓	×	×	×	×	×	×	×
[10]	×	✓	✓	×	×	×	×	×	×	×
[11]	×	×	✓	×	×	×	×	×	×	×
[12]	×	×	✓	×	×	×	×	×	×	✓
[13]	×	✓	✓	×	×	×	✓	×	×	✓
[14]	×	✓	✓	✓	×	×	✓	×	×	✓
[15]	×	×	✓	×	×	×	×	×	×	✓
[16]	✓	×	✓	×	×	×	✓	×	×	✓
[17]	×	×	✓	×	×	×	×	×	×	×
[18]	×	×	✓	×	×	×	×	×	×	✓
[19]	×	×	✓	×	×	×	×	×	×	×
[20]	×	×	✓	×	×	×	✓	×	×	×
[21]	×	✓	✓	×	×	×	×	×	×	×
[22]	×	×	✓	×	×	×	✓	×	×	✓
This survey	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

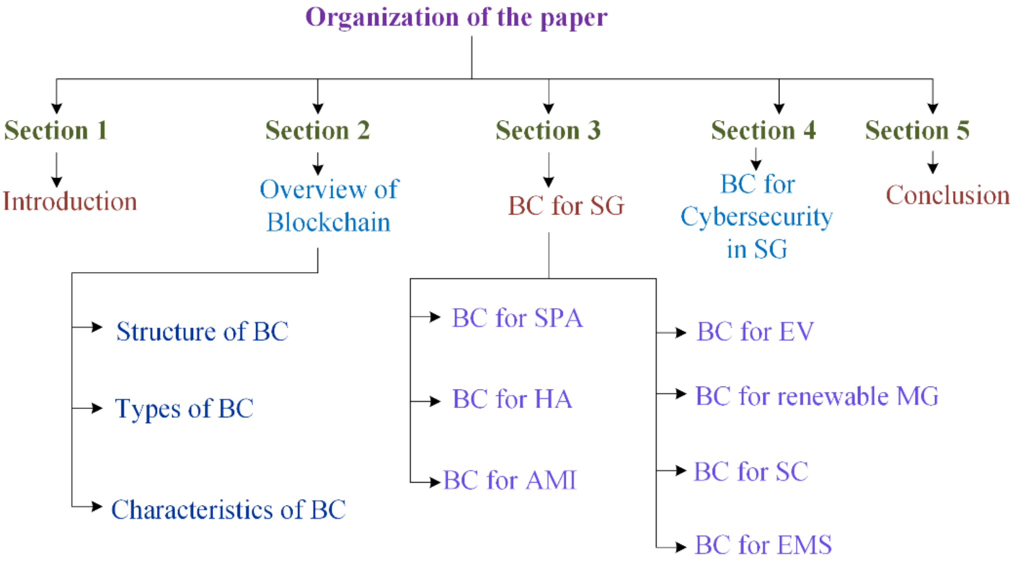

Figure 4. Organization of the paper.

2. Overview of Blockchain

In the past few years, blockchain technology has received tremendous attention worldwide. At the beginning of the technology's inception for application in digital currency, or cryptocurrency, blockchain was considered a cryptocurrency [23]. Bitcoin, the most popular cryptocurrency, was considered to be the blockchain. However, blockchain is the backbone of these cryptocurrencies. It is a distributed ledger for transactions in a decentralized network. Initially, the researchers were skeptical about this technology, but the popularity of Bitcoin changed their perception. This can be corroborated in the sudden growth in the number of published articles on the blockchain after 2016 as shown in Figure 3. Blockchain is being considered in various other domains such as banking, healthcare, healthcare, industries, etc. These various applications are depicted in Figure 5.

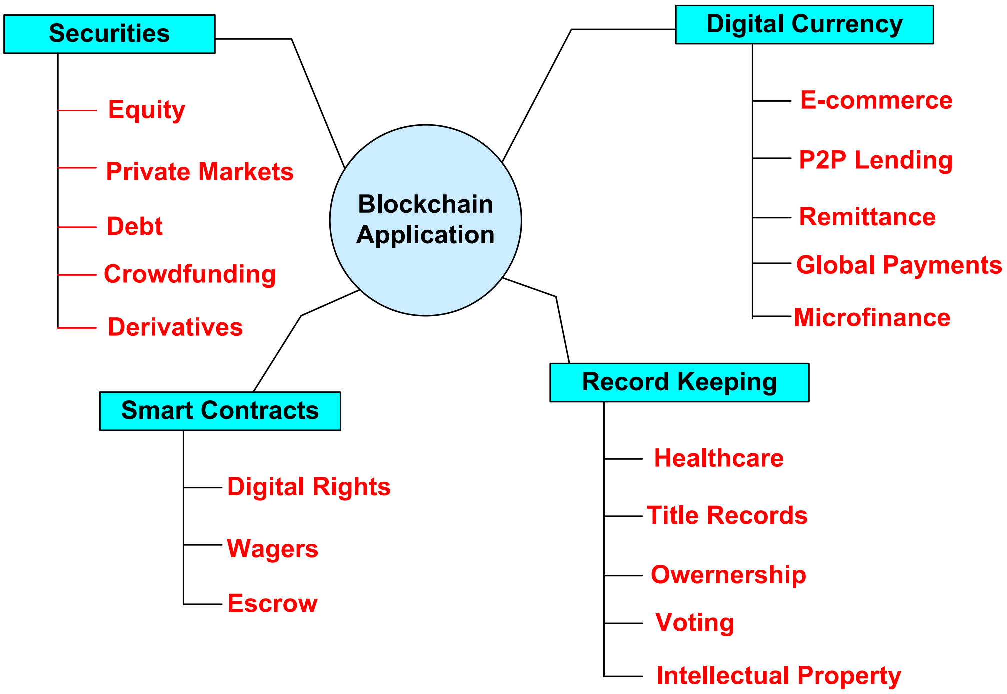

Figure 5. Applications of blockchain.

2.1. Structure of Blockchain

The blockchain comprises a series of blocks of transactions linked together in a chain, as shown in Figure 6. Client/server architecture is used in traditional client/server systems, and various administrators are in charge of them. On the other hand, blockchain is a distributed, decentralized peer-to-peer (P2P) network [24]. Each and every network participant can control the network. The network is made up of many connected computers or nodes, and the blocks in the chain cannot be changed without the network's approval. Each node in the network has its copy of the digital ledger.

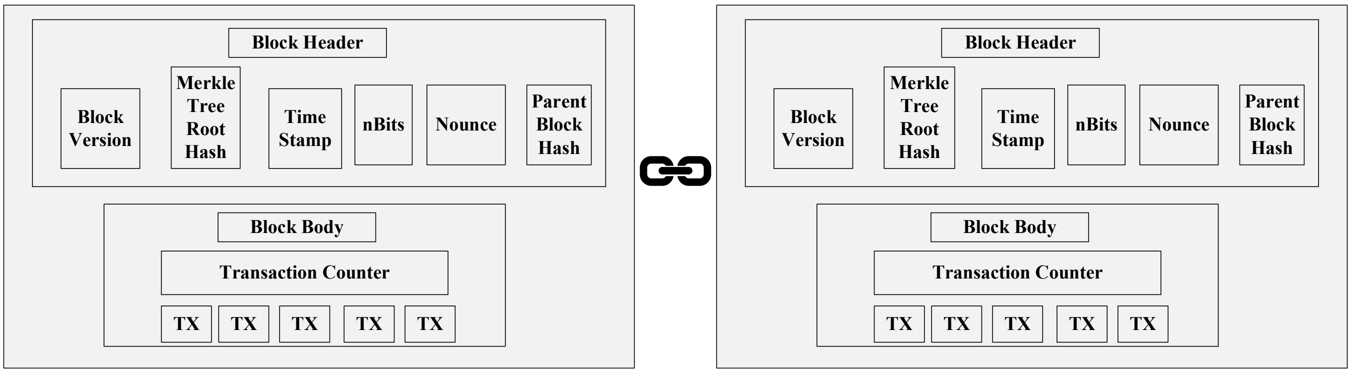

Figure 6. Structure of a blockchain.

The main constituents of a blockchain and the associated terminology are described as follows:

1. Block: In a blockchain, pointers and linked list data structures are utilized to represent blocks. Using a linked list, the blocks are sorted in a logical order and aligned up with one another. A block is a data set containing transaction information like timestamps and links to previous blocks and is produced using a secure hash technique.

The location of the next block is indicated via pointers. Every block is divided into two sections: the block header and the block body.

The block header has the following fields:

(i.) Block version: specifies which set of block validation criteria should be used.
(ii.) Merkle tree root hash: the sum of all transactions in the frame's hash value.
(iii.) Timestamp: from 1 January 1970, the current time is expressed in seconds in universal time.
(iv.) nBits: a valid block hash's goal threshold.
(v.) Nonce: a 4-byte field that starts with 0 and rises for each hash computation.
(vi.) Parent block hash: a 256-bit hash value that refers to the block before it.

A transaction counter and transactions make up the block body. The maximum number of transactions stored in a block is determined by the block size and the transaction size.

2. Public and Private keys: Blockchain is a constantly increasing network of interconnected and secured blocks using cryptographic processes [25]. To validate transactional authentication, blockchain employs an asymmetric key technique. The transactions in the block are encrypted using a private key. Every other node in the network can access these transactions. These nodes can decrypt the data using a public key available to all the nodes in the network.
3. Hash function: Every block has a cryptographic hash related to the previous block. Hashing creates a unique fixed-length string to identify a piece of data. The length of the string is independent of the size of the data.
4. Consensus process: A set of protocols and consensus from all network participants are used to validate new blocks. Consensus is needed to decide on the validity of the block. Several approaches are available for the consensus process, such as proof of work, proof of stake, practical byzantine fault tolerance, etc.
5. Smart Contracts: Smart contracts are programs that execute automatically and control the transactions between the distributed nodes in the blockchain network.

2.2. Types of Blockchain

The type of a blockchain depends on the nature of the application. There are three types of blockchains: public, private, and consortium [26]. These three types of blockchains are represented along with their properties in Figure 7.

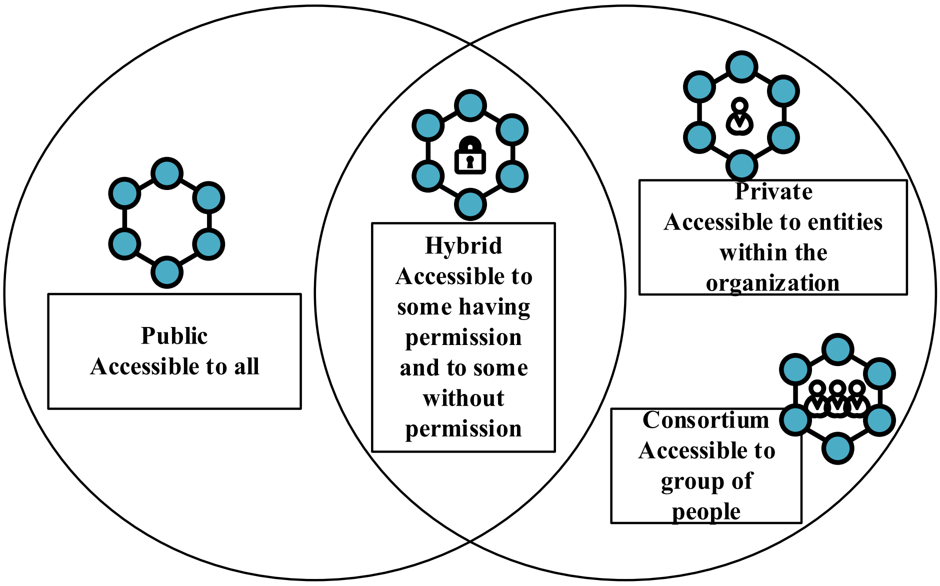
Public
Accessible to all
Hybrid
Accessible to some having permission and to some without permission
Private
Accessible to entities within the organization
Consortium
Accessible to group of people

Figure 7. Types of blockchains and their properties.

There is no control over a permissionless or public blockchain. Anyone may access the network and read or write data. Permissioned ledgers, on the other hand, are only accessible to network users who have been authenticated. Since they are encrypted with a private key, everyone cannot read the blocks. The properties of public and private blockchains are combined in consortium blockchains.

2.3. Characteristics of Blockchain

A blockchain is a decentralized network, and unlike a centralized system, the transactions are validated by the nodes in the network [27]. The identity of the nodes in the network remains unanimous, and once a transaction is validated by the nodes and added to the blockchain, it is impossible to reverse the transaction. Thus, the blockchain is immutable. The various other characteristics of a blockchain are depicted in Figure 8.

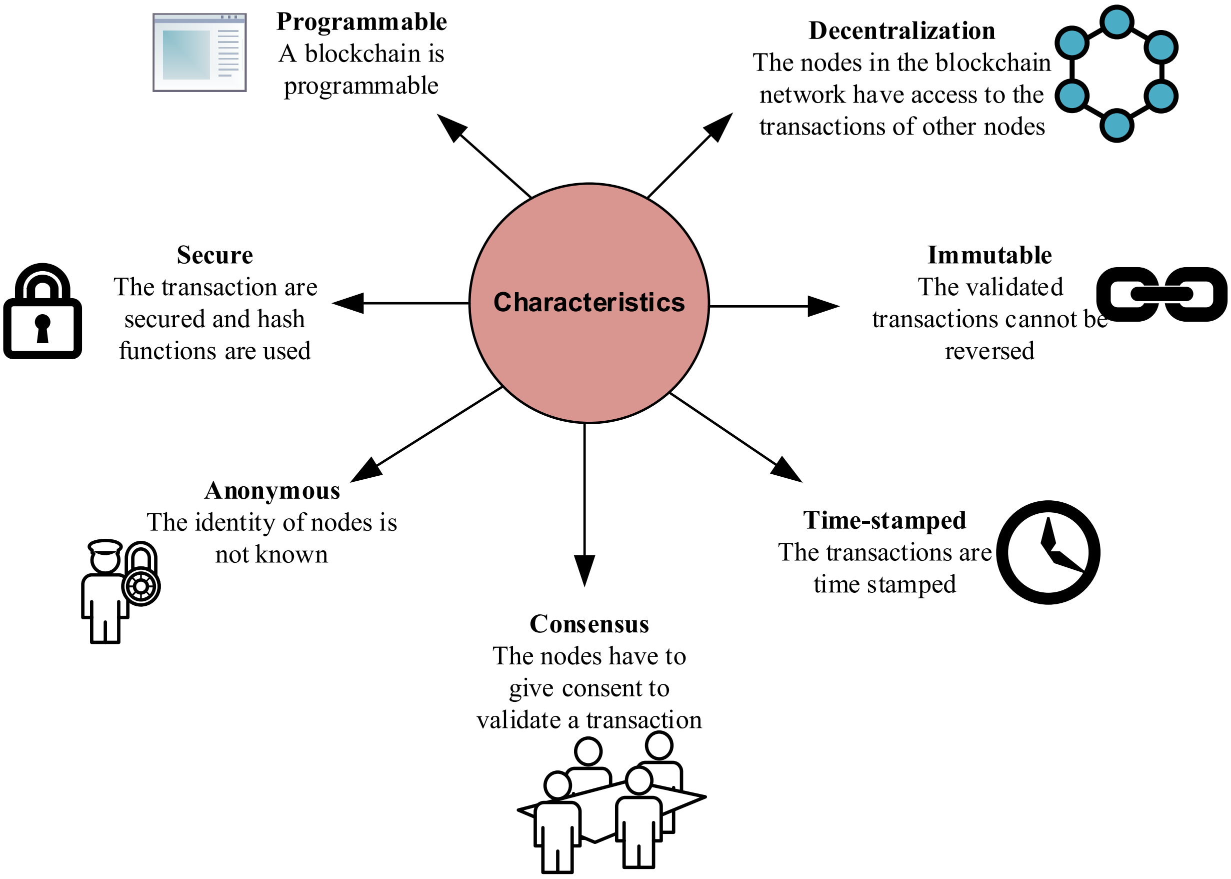
Characteristics
Programmable
A blockchain is programmable
Decentralization
The nodes in the blockchain network have access to the transactions of other nodes
Secure
The transaction are secured and hash functions are used
Immutable
The validated transactions cannot be reversed
Anonymous
The identity of nodes is not known
Time-stamped
The transactions are time stamped
Consensus
The nodes have to give consent to validate a transaction

Figure 8. Characteristics of a blockchain.

Although blockchain technology has gained traction in future Internet systems, several difficulties must be properly addressed. Expertise in blockchain technology is critical, as the technology is still in the nascent stages. Adoption of BCT provides promised benefits in various fields, but the high initial infrastructure costs are a big worry for businesses. The deployment of blockchain technology is also influenced by privacy and security concerns. Scalability and legal requirements are also significant obstacles to its implementation.

3. Blockchain for Smart Grid

Blockchain technology has much potential to transform applications by creating more trust and increasing decentralization. Despite its rapid growth, its advantages are not being aggressively exploited by the SG applications. The number of articles published on blockchain from the perspective of the various SG applications is shown in Figure 9. These statistics were taken from the Scopus database and considered only articles published in journals.

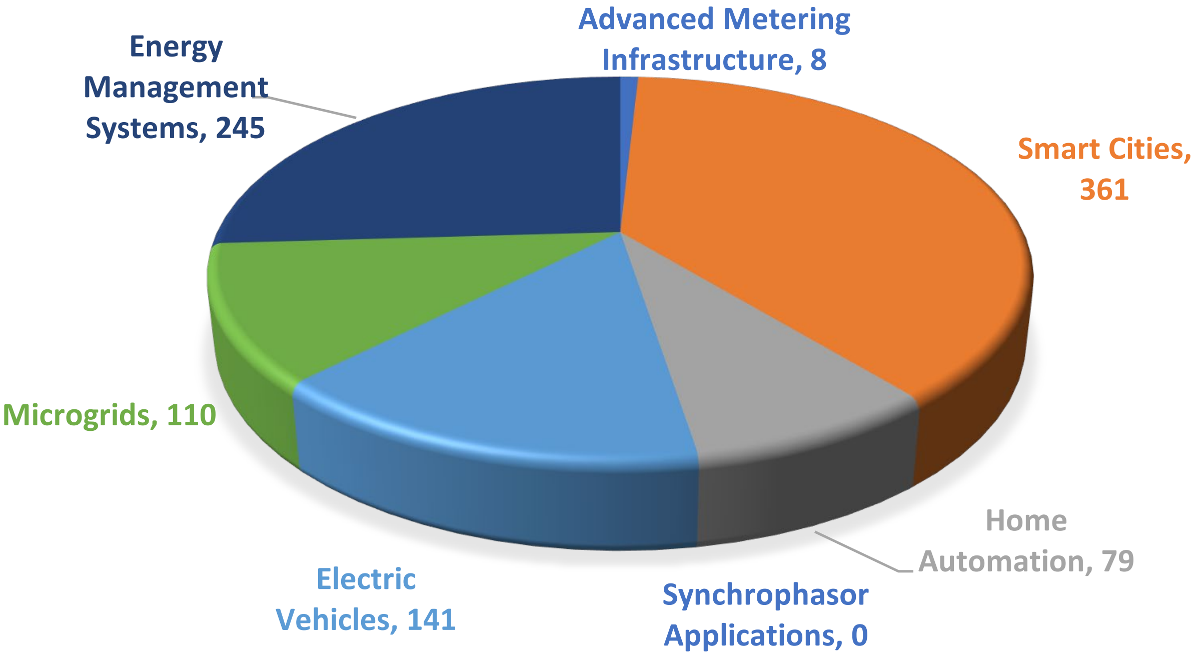

Figure 9. Publication statistics on blockchain for SG application.

Blockchain is widely adopted for energy management applications in an SG. Blockchain is also widely used for SCs, EVs, and MGs. SPAs, responsible for the wide area monitoring and control of the grid, are not employing blockchain technology for decentralizing the process. Only four conference articles reported the use of blockchain technology for SPA. In this section, blockchain technology will be explored from the perspective of these applications.

3.1. Blockchain for Synchrophasor Application

The major outages across the globe, such as those in Brazil in February 2011, the Pacific Southwest in September 2011, India in July 2012, Vietnam in May 2013, the Philippines in June 2013, Bangladesh in November 2014, etc., have necessitated the wide-area measurement system (WAMS) in the SG [28,29]. The WAMS is a comprehensive solution to monitor, control, and maintain the SG by incorporating the state-of-the-art infrastructure, emerging technology, and tools.

Recently, synchrophasor technology emerged as a viable solution for the WAMS. The synchrophasor technology enables WAMS to monitor, control, and coordinate the SG in real-time and precisely [30]. The fundamental architecture of the synchrophasor measurement system involves a phasor measurement unit (PMU), phasor data concentrator (PDC), and the communication network [31]. The PMUs are high-speed sensors that monitor the grid in real-time by measuring the grid voltages and currents. These measurements are time-synchronized using the global positioning system (GPS) and communicated to the PDC, which acts as an aggregator. The time-synchronized measurements of PMUs are referred to as synchrophasor data.

The communication network acts as a backbone since it provides the infrastructure for communicating synchrophasor data between PMUs and PDCs [32]. The more generic architecture of WAMS comprises decentralized architecture where the devices are hierarchically arranged. The decentralized hierarchical architecture of the WAMS with three levels of hierarchy is shown in Figure 10. A local PDC may be located close to the microgrids, aggregating synchrophasor data from several PMUs in a power grid. Further, there may be a master PDC that aggregates data from several local PDCs. Finally, the data from several master PDCs may be aggregated by a PDC known as a super PDC located at the regional level, which is the highest level in the proposed hierarchy.

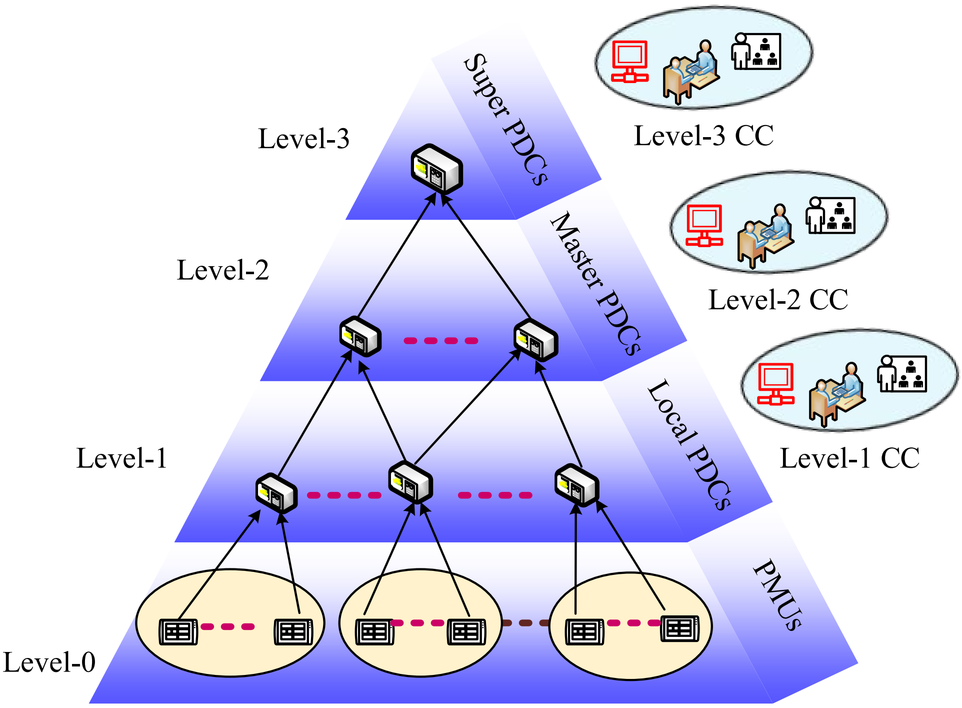

Figure 10. Hierarchy in a WAMS.

The data pertaining to the health of the grid can be used in WAMS for state estimation, stability analysis, situational awareness, etc., of the SG and its other operational-related functionalities. However, such data, typically referred to as synchrophasor data, can be exploited by cyber-attacks such as denial of service (DoS), distributed denial of service (DDoS), false data injection, spoofing, data tampering, etc. [33]. These attacks put the WAMS at risk, and its efficacy becomes questionable. The risk identification and assessment of smart grids is thoroughly discussed by Jha et al. in [34], where the authors considered risk assessment analysis of smart grid communication networks. The blockchain can be used with synchrophasor technology to mitigate the risk of cyber-attacks in a WAMS. Additionally, blockchain technology can simultaneously enhance the robustness, reliability, and integrity of the synchrophasor data by incorporating a decentralized peer-to-peer approach to communicate synchrophasor data in a WAMS.

3.1.1. Blockchain Architecture for SPA

The blockchain architecture for the SPA in an SG will consist of three fundamental components:

1. The member nodes, which are the PMUs or the PDC. Each node generates its synchrophasor data and shares it using the IEEE C37.118-2 [35].
2. A shared ledger containing the synchrophasor data collected by all the member nodes.
3. A peer-to-peer distributed network between the member nodes.

The architecture of a blockchain for SPAs is shown in Figure 11. As shown in the figure, the PMUs are connected in a fashion to create a distributed peer-to-peer network where all PMUs are enabled as member nodes. Each PMU is responsible for collectively updating the shared ledger. The synchrophasor data from a PMU is referred to as a synchrophasor transaction. The synchrophasor transactions are generated by PMUs which can be verified using authentication methods such as the elliptic curve digital signature algorithm. Despite this authentication, it is quite possible that the false identity of a PMU can be created to obtain access to the network causing danger to the resources. Such an attack can be mitigated using device identity validation methods such as the Bloom filter-based PMU identity validation approach.

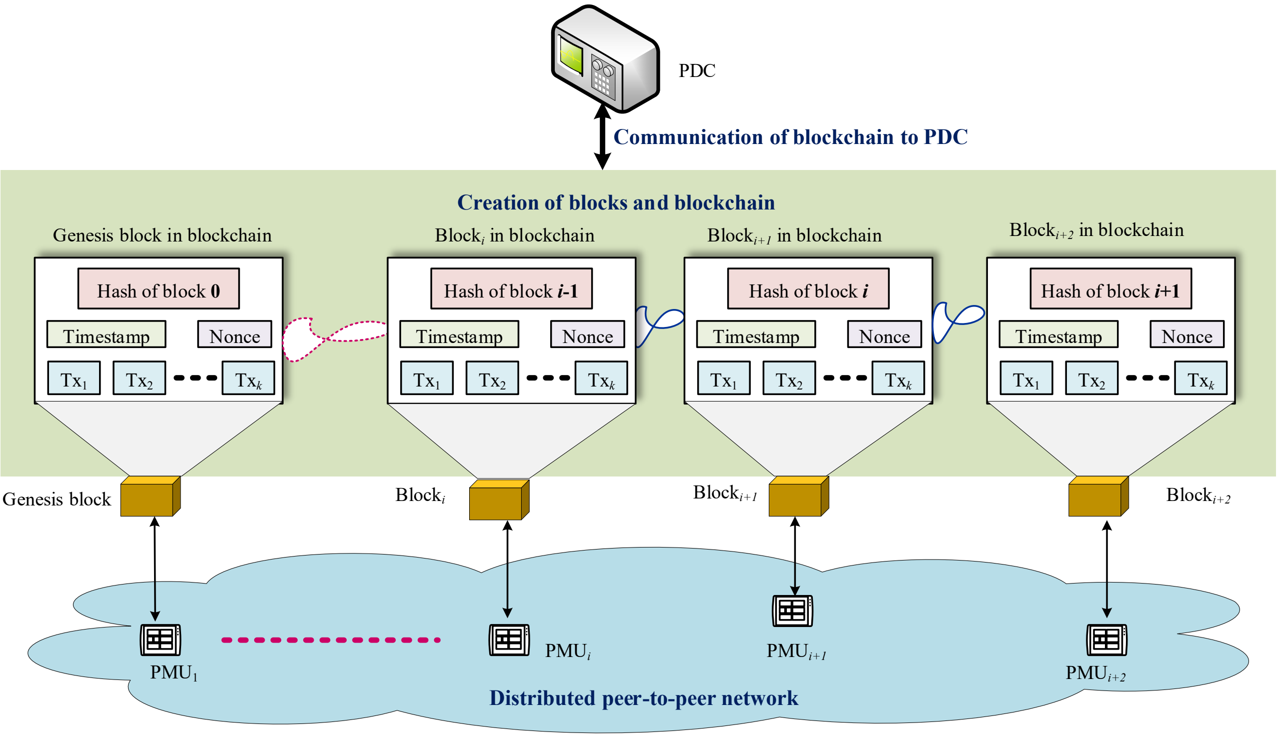

Figure 11. Blockchain architecture for SPA at the level of PMUs.

The PMUs are connected in a fashion to create distributed peer-to-peer network. Each PMU in the distributed peer-to-peer networks acts as a member which mines the block, where the synchrophasor transactions are included in a block. The contents of the block are shown in Figure 12.

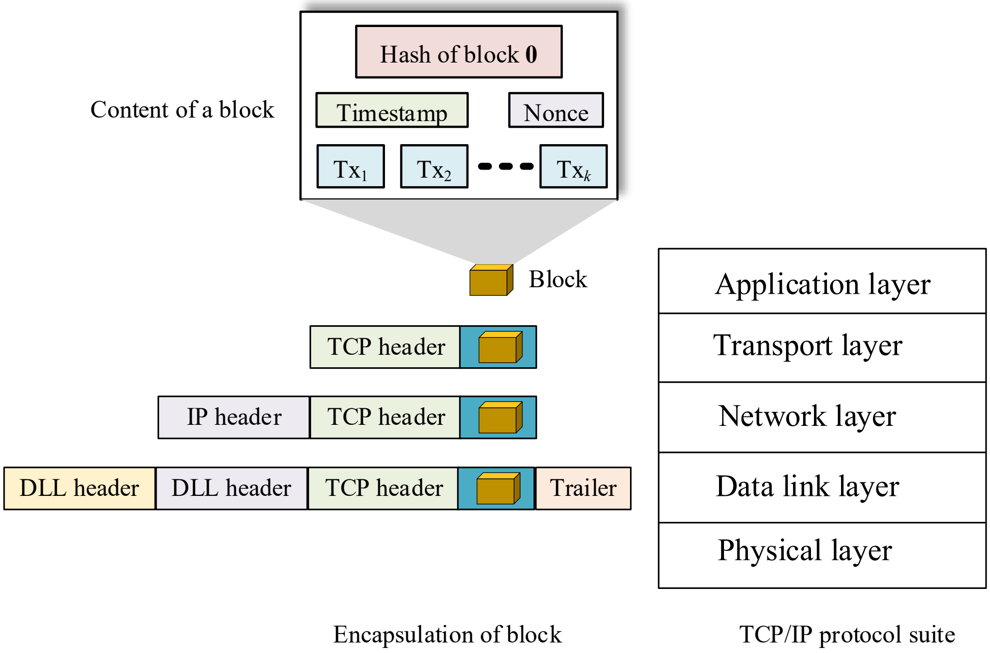

Figure 12. Contents of the block in a blockchain-based SPA.

Each block is generated using the IEEE C37.118-2 standard. The block is encapsulated with other protocols for communication over the TCP/IP network. The PMUs are responsible for consensus execution and block validation. There are several approaches for consensus execution and validation in blockchain technology. For SPA, the Markel tree-based approach can be used for consensus execution as it converges quickly without compromising the integrity of the synchrophasor transactions. Further, PMUs can follow consensus based on proof-of-work (PoW), where nonce is searched, which is a random number. When all the synchrophasor transactions grouped in a block are validated and PoW is completed, only a block is considered successfully mined by the PMU. On validating with PoW, the newly created block is appended to the existing chain to update the blockchain. The first block in the blockchain is a genesis block, which a PMU in the network can generate. It is imperative that any PMU can validate any number of blocks and receives the whole existing blockchain from executing the consensus and PoW. The decentralization can also help remove the PDC, and the PMUs themselves can take commensurate actions based on the measurements available from other PMUs.

3.1.2. Challenges and Solutions for the Implementation of Blockchain-Based SPA

PMUs operate at a very high rate, typically 30–60 samples per second in a time-synchronized manner. Hence, the additional functionalities of creating the blocks and validating burden the device and hampers the granularity of its measurements. An alternative solution to this problem is implementing the blockchain at a higher level in the hierarchy, i.e., at the local PDCs. The architecture for implementing the blockchain at the level of local PDCs is shown in Figure 13.

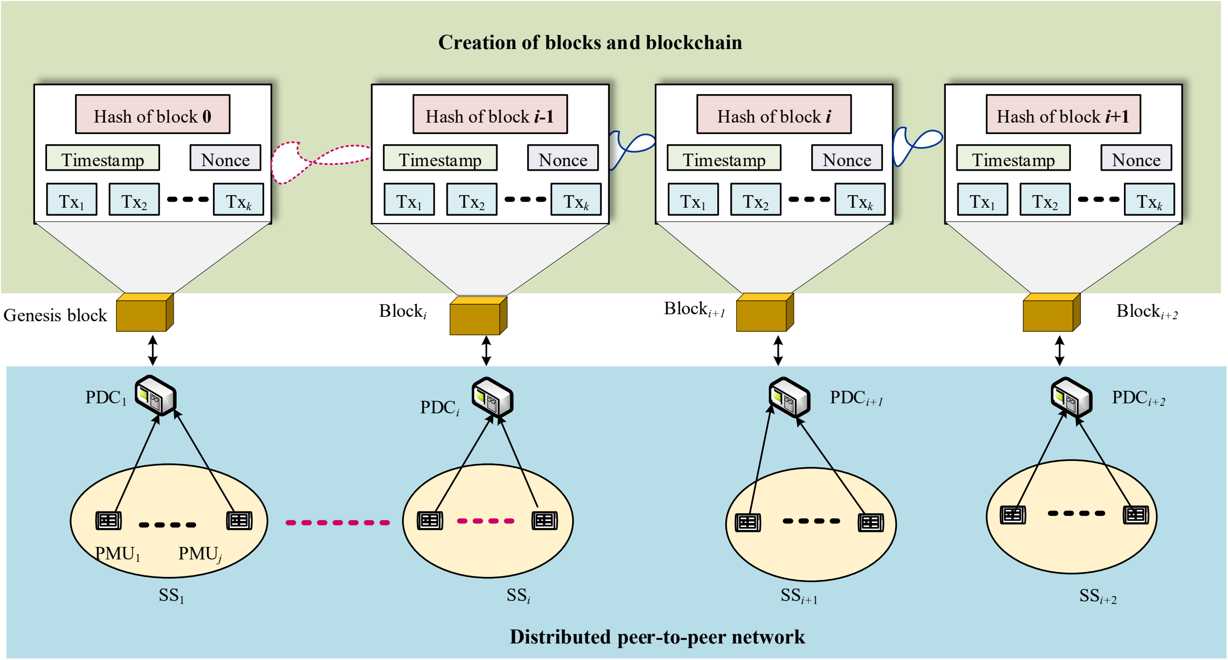

Figure 13. Blockchain architecture for SPA at the level of local PDCs.

SPAs are mission-critical, so it becomes computationally intensive to validate all the transactions. A solution to this problem is to terminate the chain at periodic intervals and start a new chain. This reduces the secureness of the chain, so additional measures will be needed to maintain the security. Because of the problems of the mission-critical nature of the application and the high data rate of the PMU, not many works are available on this topic.

3.2. Blockchain for Home Automation

A smart house is an integrated Internet of Things (IoT) domicile that provides users security, health, comfort, and a higher standard of life, among other benefits. People's life and independent living are made easier with smart home solutions. They provide valuable capabilities such as behavior tracking and safety evaluations, which have drawn the attention of consumers and device makers. Although intelligent homes provide significant benefits to homeowners and other interested parties, they are vulnerable to harmful cyber-attacks that risk users' safety and privacy [36]. Traditional solutions to such dangers exist, but they are extremely centralized and prone to large-scale attacks. As a result, the adaptability and scalability needed for effective utilization in the cutting-edge field of autonomous smart home applications and facilities are absent. Several clever technologies make life easier for individuals. Such programs generate enormous volumes of data. The archiving of this ever-changing material into repositories raises security problems. In cybersecurity technologies with remote connectivity and data transmission, blockchain has performed well. Thus, it is being employed for home automation applications.

3.2.1. Blockchain Architecture for HA

Home automation involves several smart devices, such as smart TVs, lights, etc. These devices monitor and control the various parameters of the house, which operate independently or are coordinated by a user. The interconnectivity of these smart devices is required to achieve the objective of HA. The interoperability challenges between the smart devices are handled using an IoT gateway. Users from one home cannot control the devices of another home to avoid a security breach. The service provider is responsible for providing necessary recommendations to the user for controlling smart devices based on prediction algorithms. The service provider can use machine learning algorithms for better recommendations or predictions. The blockchain network is used to connect different users and service providers to enhance security in the HA [37]. The blockchain network may be built using Ethereum or Hyperledger. The general architecture of blockchain for HA is shown in Figure 14.

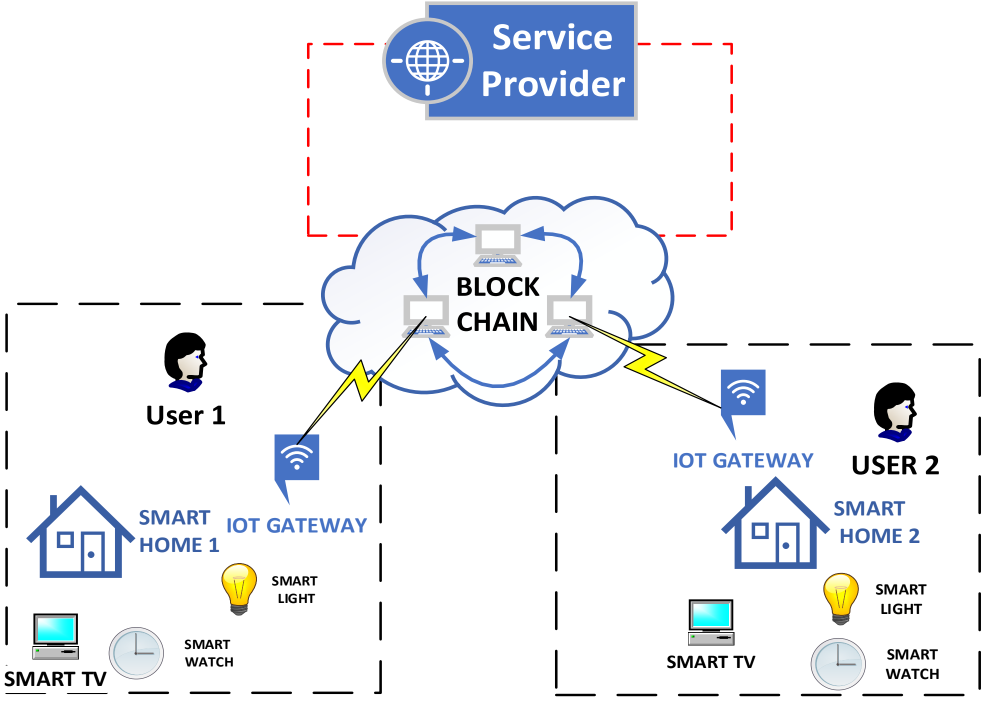

Figure 14. The architecture of blockchain for HA.

The user within the house can control the entities within his home; he cannot have access to the entities present in another smart home. The various devices in the home can be directly connected to the blockchain network through the gateway. The data from the devices can be placed into the blocks, which are then chained together using the hashing mechanism of the blockchain. The service provider can analyze the data and send suggestions to the users, but he cannot directly control the devices in the smart home. This architecture can be customized based on the user's specific requirements by the service provider. The various devices in the home can be directly connected to the blockchain network through the gateway. The data from the devices can be placed into the blocks, which are then chained together using the hashing mechanism of the blockchain.

3.2.2. State-of-the-Art on Blockchain for HA

The literature on blockchain for HA applications discusses access control mechanisms, homecare systems, utility payment services, etc. These works are summarized in Table 2.

Table 2. Review of the works on blockchain for HA applications.

Reference	Domain	Blockchain Mechanism Used	Summary
[38]	Access control	Private blockchain	For access control in smart homes, which is computationally fast and economical but is susceptible to malicious attacks.
[39]	Home care	Ethereum blockchain	Provides a secure means of sending healthcare data to the healthcare center, but has increased overhead.
[40]	Home care	Private blockchain	Reduces communication overhead for sending patient data but has more overhead.
[41]	EV charging bill payment	Lightweight basic blockchain	Reduces the size of block for payment of charging bill. This is also vulnerable to security attacks.
[42]	Home care	Consortium blockchain	Data of the aged people is stored efficiently with enhanced quality but is susceptible to DoS attack.
[43]	Authentication mechanism	Ethereum blockchain	A scalable but expensive mechanism for authentication of IoT devices.
[44]	Automated payment	Bitcoin blockchain	A highly scalable automated payment system that also allows off-chain transactions.
[45]	Lightweight payment system	NA	A low-power and fast payment system. This may be susceptible to malicious attacks.

3.2.3. Challenges and Solutions for the Implementation of Blockchain-Based HA

Various blockchain systems are being used for HA applications [46]. These systems have their specific data format, and their interoperability is challenging. Additionally, the consensus algorithms used by these systems are different. For seamless interaction, standardization of blockchain systems is required. Another challenge to implementing blockchain for HA applications is the real-time analytics of streaming data. The data have to be processed and analyzed in real-time. For example, an intruder detection system requires real-time face detection. Processing blockchains for real-time applications is challenging. A possible solution is to use a lightweight framework for this application.

3.3. Blockchain for Advanced Metering Infrastructure

The heart of the AMI is a smart meter used to collect, monitor, and communicate the data related to energy consumption corresponding to every user. The meter data are used differently by different entities. For example, the grid operator can use this data for load forecasting and planning, and the market operator can use smart meter data for dynamic pricing and billing. On the other hand, the users can use such data to manage their electricity usage. Whereas AMI provides ample advantages, secure AMI data transaction is challenging. The blockchain-based AMI plays an important role in achieving this objective. A generic framework for implementing AMI using blockchain is shown in Figure 15.

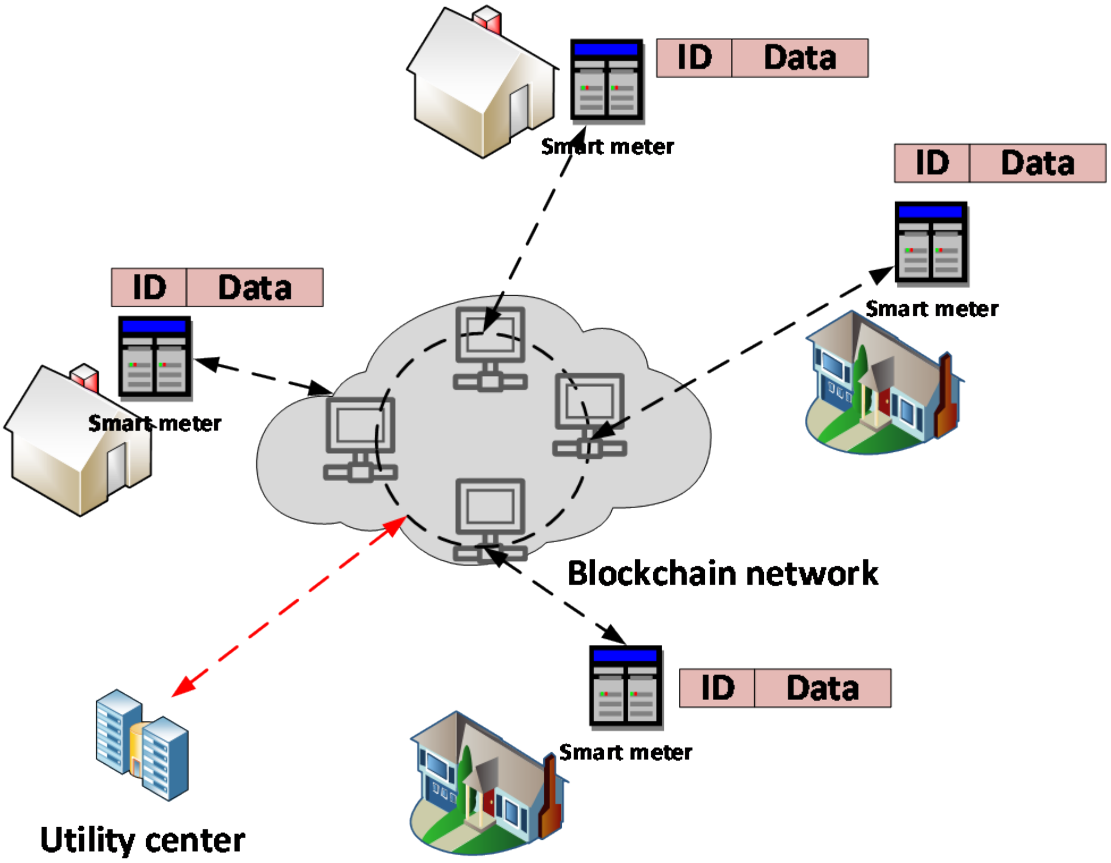

Figure 15. The architecture of blockchain for AMI.

The smart meters can be directly connected to the blockchain network through the gateway [47]. The data from the meters contains meter IDs and other utility-related information as per the IEC 62056 protocol. These meters are connected to the servers or nodes inside the blockchain network that create the blocks using the data received from the AMIs. These blocks are then shared with all other nodes inside the blockchain-enabled network. This network can only be accessed by the nodes related to the utility center and so should be a private blockchain network. The private blockchain can be used for smart contracts and validations to provide energy utilization transparency without compromising security and privacy.

Challenges for the Implementation of Blockchain for AMI

Blockchain has not been used widely for this SG application despite its utility. Researchers have used it to enhance the security of AMI applications. In ref. [48], a lightweight blockchain-based framework was proposed to enhance AMI's security. The framework was secure against attacks, and its energy consumption was low. In ref. [49], blockchain was used to preserve the integrity of the customers using AMI. As with the blockchain for HA applications, the blockchain for AMI is also plagued with interoperability and real-time constraints.

3.4. Blockchain for Electric Vehicles

The technological evolution of electric vehicles (EVs) and the rapid growth of the smart grid have led to the emergence of new connectivity structures—vehicle-to-grid (V2G) [50]. In the future, the importance of EVs using technologies such as the Internet of

Vehicles (IoV) [51] or the Internet of Things (IoT) [52] will increase, as it offers innumerable advantages, for example logistics companies provide fixed charging stations (CSs) for their fleet of vehicles.

Interconnectivity requirements with all technology systems in the real world have led to the emergence of vehicle-to-everything (V2X) technology [53], using integrated vehicle sensor platforms that use the centralization of various functions through an integrated EV server, connected by a series of connectivity devices such as CAN, LIN, Wi-Fi, and Bluetooth technology [54]. The results of V2X performances are based on a series of information on the collection and dissemination of multi-networks and technological capabilities between electric vehicles.

The security factor, the speed of data transfer between interconnected vehicles, and the wide coverage of telecommunications systems led to the emergence of 5G networks and their distribution very quickly in the world [55]. The infrastructure of multi-networks communication systems through 5G technology has the power to process applications at a superior level. The 5G network drives the V2X protocol, generating many scenarios for data management by promoting the development and integration of blockchain applications [56]. The implementation of blockchain systems in the vehicle-to-everything protocol tends to reinvent intelligent transport systems, leading to high efficiency of transport and road safety services [57].

3.4.1. Architecture of Blockchain for EVs

The general blockchain architecture for the EV application is shown in Figure 16. The blockchain-based EVs infrastructure requires regular nodes to capture mobile cars' dynamics. These nodes are responsible for smart contracts and block validations, forming the basis of the blockchain. The mobile cars send their data to such regularly placed blockchain nodes or access points. The interconnectivity between mobile electric vehicles and nodes is through WiFi. An ID number uniquely identifies each EV. The data that an EV sends to the access point involve the battery status, vehicle status, bill payment for charging, etc. The data are placed into the blockchain network by the access points as blocks. The various nodes in the blockchain validate the transactions. The blockchain network is also accessible to the transport authority, who can continuously monitor the status of the EVs and send personalized recommendations or warnings to the EV user. However, the transportation authority cannot change the parameters of the EV.

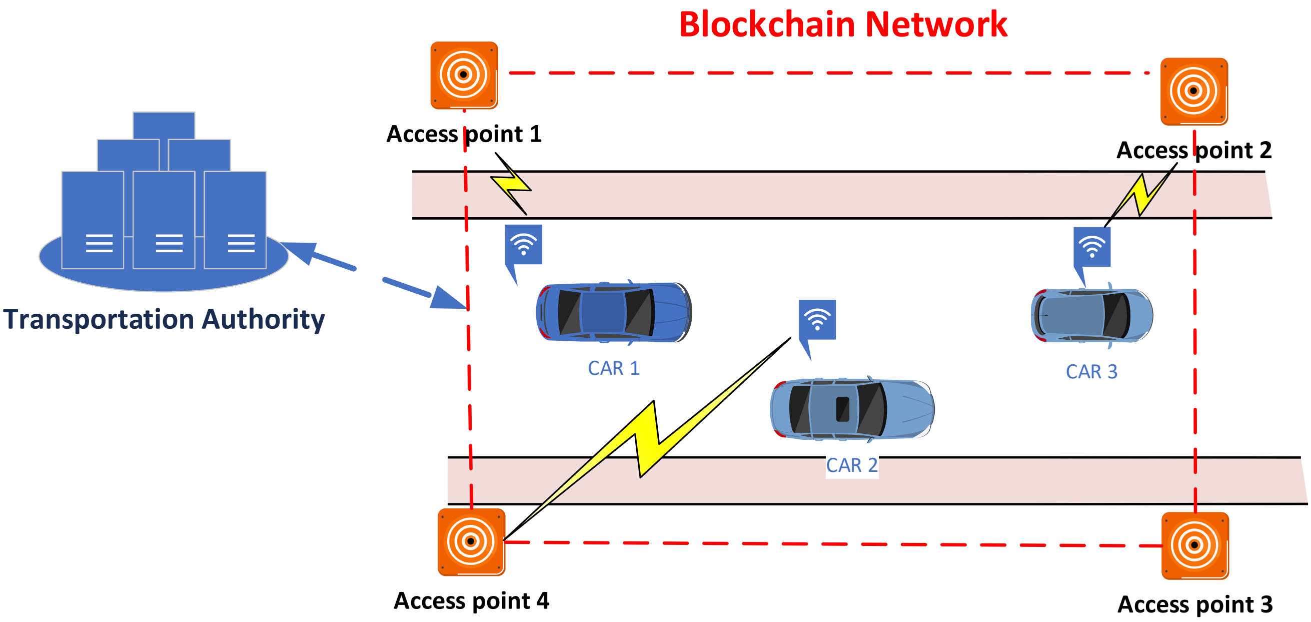

Figure 16. Architecture of blockchain for EV applications.

3.4.2. A panoramic Overview of Blockchain for EV

Despite abundant opportunities to incorporate blockchain in EV applications, some of the challenges are inherently present in the blockchain-enabled EV system, such as mining of the data, cybersecurity, handling of voluminous data, etc. Furqan Jameel et al. [58] provided a solution for unloading mining tasks in vehicle-to-everything cellular networks. A short block length transmission architecture has been proposed to meet the low-latency requirements for cybersecurity applications of EVs. In practice, finite block length architecture is a fairer approach to modeling blockchain networks. The inspiration for the theoretical application of adopting games defines a type of challenge for solving mining tasks and efficiently unloading them to clusters. The advantage of using blockchain databases ensures good data transfer rates and maintains the vehicles' fairness in the unloading process.

However, a significant disadvantage is the scalability of the data chains within the blockchain, which can be a design problem. Because data security is the main issue in conventional blockchain networks, the impact it has on the process of downloading data into electric vehicles is a real challenge. However, in ref. [59], the authors proposed a new coding sequence—Secure V2X—that capitalizes on the characteristics of the blockchain and the data networks protecting the confidentiality and security of the V2X protocol.

In addition to the benefits that blockchain initiates in low-security areas, confidentiality is the main issue in trading energy in a collective network type peer-to-peer (P2P) (E-trading). In recent years, electric vehicles have received worldwide recognition due to their potential in the green transportation system. The rapid development of technologies in smart communication networks has allowed EVs to relate to the environment. The electricity production costs are constantly decreasing through the implementation of renewable energy sources and smart grids [60]. Thus, the major challenge of peer-to-peer technology, E-trading and D-trading [61], and integration for electric vehicles is the development of a secure communication architecture that maintains data confidentiality and information anonymity. In addition, the objective of the blockchain is to mask trading relationships without compromising data integrity [62].

Various review papers in the literature focus on blockchain technologies applied in the Future Smart Grid [63,64]. Although the technology is considered one with a wide range of advantages, security needs to be assessed systematically to enhance reliability of the SG [65].

Motivated by previous development, Marina Dorokhova et al. [66] proposed integrating electric vehicle charging systems based on blockchain technology. The study is based on a popular blockchain platform, Ethereum, for interconnecting EV infrastructure and real-world infrastructure [67]. The advantage it offers is the crediting in the safety zone of the energy flows between the owners of electric vehicles and the companies that own charging stations. The only barriers that could be removed in the future are the limitations of the blockchain-high transaction costs due to network loads, high power consumption, or transactions that do not change in case of errors.

A case study by Shivam Saxena et al. [68] further demonstrated the need for techno-economic evaluation of residential energy trading systems. The EV is a part of such system, which can be enhanced through the blockchain. Using blockchain in EVs not only improves the household's participation in the electricity markets but also drastically reduces the negative impact on the energy distribution network [69]. These seminal works are comprehensively summarized in Table 3.

Table 3. Summary of works related to blockchain for EVs.

Reference	Subdomain	Objectives	Solutions/Results	Technologies	Advantages/Opportunities	Challenges
[58]	V2X Communications	Efficient solutions for unloading mining tasks in cellular vehicle-to-everything networks	Adopting a game-theoretic approach to efficiently unload the mining tasks to the mining clusters	Blockchain-based cellular V2X networks	Good data transfer rates and maintain the fairness of the vehicles in the unloading process	Scalability of the data chains within the blockchain and the impact of data security in the process of downloading data into EVs
[59]	Secure V2X Communications	Network performance	Deploying a novel framework (Secure V2X)	Blockchain and NDN (named data networking)	Protecting the confidentiality and security of the V2X protocol	Without the right cluster, the Secure V2X sequence do not helps to improve network performance
[61]	Energy trading and charging payment system for EVs	Employing blockchain technology to provide trust between users	Maintaining the data confidentiality and information anonymity	Private blockchain	Improves the distribution network and renewable energy network	Development of a secure communication architecture
[65]	Charging Management	Integration of EVs charging systems interconnected with real world infrastructure	Charging management framework	Ethereum blockchain platform	Crediting in the safety zone of the energy flows between the owners of electric vehicles and the companies that own charging stations	Limitations of the blockchain-high transaction costs and high power consumption
[67]	Residential communities	Technical -economic evaluation for residential energy trading systems	Residential energy trading systems	Blockchain platform	Reduces the impact on the energy distribution network	Peak energy demand is very high

3.4.3. Challenges and Solutions for the Implementation of Blockchain for EVs

The scalability of blockchain data chains, data security in the download process, and confidentiality are challenges that are yet to be addressed. The major challenge of peer-to-peer technologies is the processing of energy transactions and the anonymity of information. The high resource requirement and transaction cost in terms of energy consumption plagued the use of blockchain technology for EV applications with WSN infrastructure. Overcoming these limitations would make blockchain technology the main key factor for EVs. The development of lightweight blockchain algorithms for reaching consensus in real-time can be a probable solution.

3.5. Blockchain for Renewable Microgrids

With every day passing, there is a continuous transition and evolution to a renewable grid that is based on various distributed energy resources such as photovoltaics, fuel cells, microturbines, batteries, etc. These transitions rely on the successful deployment of blockchain technology.

3.5.1. Architecture of Blockchain for MGs

The generalized blockchain architecture for the MG application is shown in Figure 17. In general, the power grid of a zone is sprawled over a large geographical area where different MGs are considered. The different MGs are interconnected using the blockchain network. The blockchain network aims to enhance security and privacy in the MG operation without hampering transparency and data integrity. The data block carries information regarding the energy generated, energy to be shared with other microgrids, etc. The data pertaining to the MG are grouped into the blocks where each newly generated block is validated using a consensus algorithm. The block is then placed onto the blockchain network and is added to the blockchain after being validated. The nodes in the blockchain need proper algorithms to reach a consensus on the energy being traded, the price at which the electricity is being traded, etc.

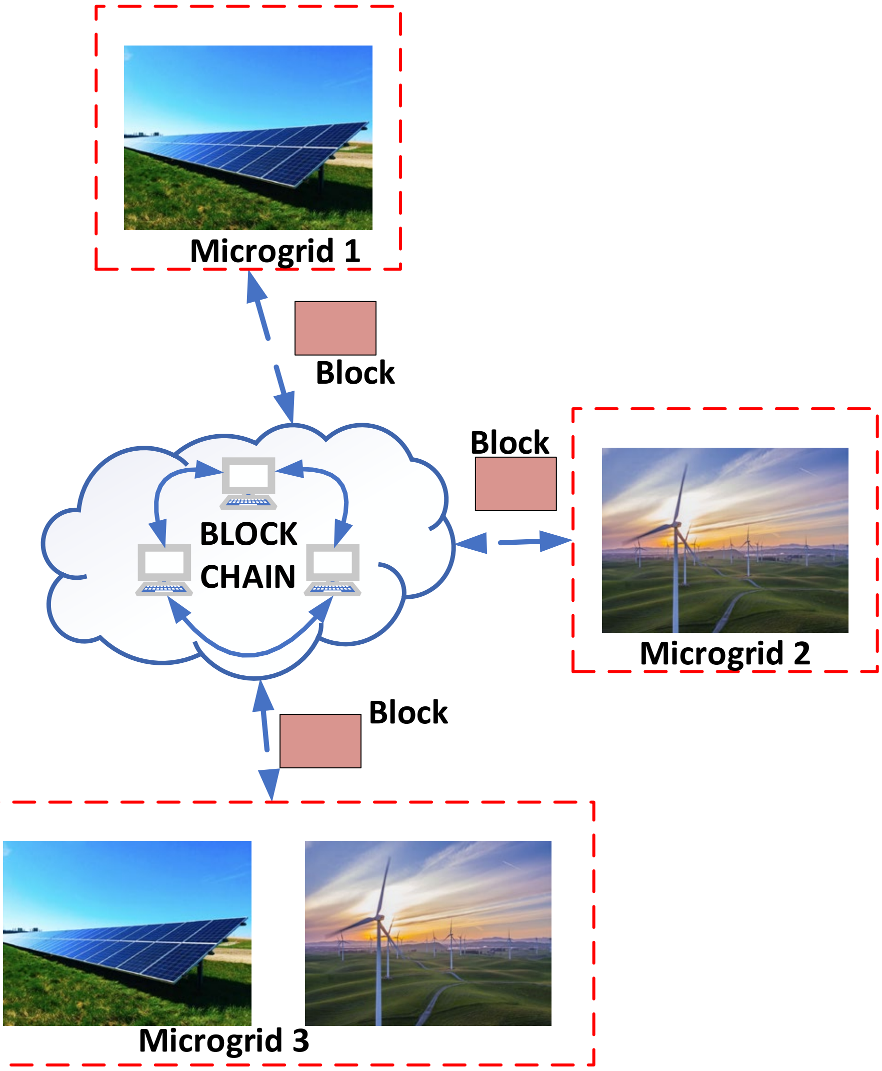

Figure 17. Blockchain for microgrids.

3.5.2. A Panoramic Overview of Blockchain for MG

Early inquiries about the energy sector with the accent on the smart grid and microgrids are mainly found in refs. [70–73], where different requirements, technologies, architectures, trends, and cyber security issues are largely debated.

With rising social, economic, political, and environmental concerns and strategies such as increasing power consumption, dealing with the middleman, market liberalization, pollution, etc., blockchain is seen as a promising solution in renewable microgrids for efficient operation such as complex point-to-point transactions between producers, traders, and users using elaborate algorithms in order to validate, secure, and record these transactions.

The different authors reviewed blockchain in the context of microgrids from several perspectives. In ref. [74], the need for blockchain, benefits, and challenges was reviewed. In ref. [11], real solutions such as the Brooklyn Micro Grid based on the blockchain environment with the Proof of Work (PoW) mechanism were presented. Other comprehensive reviews can be found in ref. [75] that can serve as quality background research for those who want to propose and implement feasible solutions and methodologies for renewable microgrids based on blockchain technology.

On the other hand, many works propose different solutions and approaches that use blockchain technology to enhance and improve microgrids and their applications. To start, ref. [76] proposed an approach for using blockchain on the Dominican Republic's electricity market, referred to as the main step in empowering automatic management of economic transfers with funds authenticating and supplier's guarantee. The approach presents an economic and energy blockchain-based flow to decentralize the current flows that involve total control through banking operations. Of course, such an approach must face serious economic interests, political regulations, and technological limitations to achieve its goals, but it is seen as a first step in applying blockchain in the electricity sector.

In ref. [77], a local energy market model using private blockchain via home energy management and demurrage mechanisms was presented. In the proposed model, there are three major actors: a small community (several microgrids) that uses photovoltaic systems as renewable energy as the prosumers; the consumers; and the main grid. Using Critical Peak Price (CPP) and Real-Time Price (RTP) schemes, simulations showed that costs were significantly reduced. Moreover, ref. [78] proposed a blockchain-based decentralized market mechanism to establish the price using auction methods. However, this is plagued with two limitations: difficulty in selling the oversupply of energy through auction and big challenges in ensuring privacy and security. Another solution for P2P energy trading was presented in ref. [79] by implementing the blockchain-based decentralized energy flexibility market for P2P transactions among prosumers. Two additional frameworks, first as decentralized blockchain-based and second as semi-decentralized, can be found in ref. [80], where the P2P energy trading subject was analyzed.

A more applied approach is in ref. [81], which proposed a method for an effective P2P blockchain-based energy market between a microgrid and the smart grid (IEEE 24-bus test system) where the function of distributed consensus algorithm was evaluated in the presence of Fault Data Injection Attack (FDIA). The main findings of this paper showed that the consensus process keeps running even if the case of a cyber-attack and the output response of the P2P market is very close to the centralized energy market. Maintaining the idea of the applied solution, the authors in ref. [82] suggested a model for an integrated energy management platform based on blockchain technology and, at the same time, implement a bilateral trading mechanism with simulation results showing significant optimization of the energy flow in a microgrid. Another model for blockchain-based energy management was suggested in ref. [83], where a Pythagorean fuzzy method was used in choosing the best solution for energy production, distribution, and waste control.

Further, in ref. [84], another P2P energy trading mechanism between microgrids based on the same technology using a fuzzy meta-heuristic approach as a pricing solution was presented with results showing increased profitability and reduced CO_2 emissions. Additionally, the fusion of the electricity market and blockchain was studied in ref. [85], where transactions were highlighted using multi-agent cooperation and sharing platform based on the Ethereum private blockchain, with results revealing several benefits such as transparent transactions and intelligent mutual trust.

Going deeper and deeper into the heart of the topic of this section, we arrive at the point where blockchain applications variates in terms of the constructive technology that microgrids are built on, this referring to AC microgrids, DC microgrids, or hybrid AC-DC MGs [86–90]. First, blockchain was used in ref. [86] to increase the security for interconnected hybrid AC-DC microgrids using a modified sine cosine algorithm to achieve the optimal decision in the shortest time and with high accuracy. The approaches in refs. [87] and [88] are based on the blockchain technology for energy management concerning DC and hybrid AC-DC microgrids using different strategies such as fuzzy logic control or the whale optimization algorithm. These seminal works are comprehensively summarized in Table 4.

Table 4. Material summary—blockchain for renewable microgrids.

Reference	Subdomain	Objectives	Solutions/Results	Technologies	Advantages/Opportunities	Challenges
[76]	Local energy market	Replacing transactions based on banking entities with cryptocurrency-based transactions	Economic and energy blockchain-based flow	Public blockchain	Funds authenticating and automatic control of transactions	Political regulations, economic interests and technological limitations
[77]	Local energy market/microgrid/smart grid	Optimizing energy consumption and minimizing electricity costs.	Reduced electricity cost and optimized energy consumption, especially at peak hours	Private blockchain with PoW mechanism	Optimal electricity cost for each time slot and local energy demand and generation balance	Implementing penalty policy
[78]	Microgrid/smart grid	Minimizing electricity costs	Decentralized market mechanism	Private blockchain	-	Selling oversupply
[79]	Local energy market/microgrid	P2P energy transactions	Electricity costs reduced	Public blockchain	Control of energy generation and flows and full ratio of self-consumption from renewable energy	Political regulations, economic interests, and technological limitations
[80]	Local energy market/microgrid	P2P energy transactions	Decentralized proposed framework and semi-centralized proposed framework	Solc, Mocha, React.js, Next.js, Ganachecli, Metamask, Ganache-cli, and Web3	Framework 1 uses more transactions, is less flexible and more secure/Framework 2 uses less transactions is more flexible and less secure	Smart contract limitations
[81]	Microgrid/smart grid	Ensure security and achieve consensus when cyber-attacks occur	Proposed architecture	Either public or private blockchain	Efficiency against attacks	Transaction security
[82]	Microgrid	Optimize the energy flow in a microgrid	Proposed model/optimized energy flow	Private blockchain	Reduced import costs	Security and communication efficiency
[83]	Renewable energy	Energy management	Proposed methodology and framework	Either public or private blockchain	-	Technological infrastructure and investment prices
[84]	Local energy market/microgrid	P2P energy transactions	Proposed fuzzy meta-heuristic approach	Either public or private blockchain	Encourage P2P energy transactions	Security and risks concerns
[85]	Local energy market/microgrid	P2P energy transactions	Proposed trading platform	Private blockchain	Transparent transactions	Political regulations, economic interests, and technological limitations
[86]	Hybrid AC-DC microgrid	Increase security	Proposed framework	Public blockchain	Increased security	Power injection limitations
[87]	DC microgrid	Energy management	Proposed framework	Either public or private blockchain	Maximum utilization of renewables	Political regulations, economic interests, and technological limitations
[88]	Hybrid AC-DC microgrid	Energy management	Proposed framework	Private blockchain	Optimal energy management and secured transactions	Political regulations, economic interests, and technological limitations

3.5.3. Challenges for Implementation of Blockchain for Microgrids

Like the numerous advantages, many challenges must be overcome in the blockchain-based renewable microgrids [91,92]. These challenges refer to technological constraints, economic aspects, social uncertainties, environmental concerns, political and institutional limitations, and law, regulations, norms, or end-to-end privacy and security.

A feasible and efficient balance between key features such as security, energy management, constraints, and costs is still challenging. Different consortiums operate different microgrids, so it is important to analyze and decide on the correct algorithm or methods to use, the best technology, the most suitable investor, and a very well-trained team.

3.6. Blockchain for Smart City

With the development and use of blockchain technology, the Internet of Things (IoT), and Cloud Computing, rapid evolution can be observed in the smart city paradigm.

3.6.1. A panoramic Overview on Blockchain for SC

In refs. [93,94], some of the problems related to smart city transportation were debated. These works demonstrated that there are concerns in rethinking the transformations of localities in terms of improvement of public transport and logistics [95,96], water supply [97], green energy [98], environment [99], health [100,101], education [102–105], and economics [106–109] by using the blockchain, which offers the possibility to use distributed stored data, and performs transactions without intermediaries between producers and beneficiaries [106,109] without data security problems [107]. The blockchain architecture [93,94] is the one that will strengthen the importance of using smart contracts in the development of transactions between the parties. These contracts are triggered by operations (agreements) between the parties or are determined by sensors, actuators, or IoT tags [97]. So, the blockchain and smart contracts are the ones that contribute to the transformation of localities into smart cities, finding the optimal adequacy in the development of logistics, energy, environment, water quality, health, etc. Some seminal results of the prospective of blockchain on health care are summarized in Table 5, whereas its applications in other smart city domains are summarized in Table 6.

Table 5. Summary of literature on blockchain for smart city health care system.

Reference	Objectives	Solutions/Results	Advantages/Opportunities
[93]	Smart village architecture	Blockchain in healthcare	Raising the standard of living of citizens
[94]	Application of BC in the health system	Implementation of BC in healthcare	Data storage security, privacy, and integrity in online consultation
[95]	Application of BC technology in the healthcare	How to apply BC technology in health to monitor the patient's health	Real-time patient monitoring, efficient data handling
[96]	Public health in the smart society	Prediction regarding the health status of the population using BC	Modernization of the healthcare system with enhanced data integrity, security, and privacy
[97]	Development of a BC based platform for healthcare	Model-based platform as a solution for healthcare information exchange	Enhanced privacy and security using a combined approach based on off-chain storage and on-chain verification

Table 6. Summary of literature on Blockchain for Smart City.

Reference	Objectives	Solutions/Results	Advantages/Opportunities
[98]	Green energy marketing	Utilization of photovoltaic parks	use of green energy, reduction of pollution, sale of surplus energy, decrease the production price
[99]	Energy management	Low-cost solution to the energy system	Efficient trading, production quality, capitalization of energy surplus
[100]	Incorporation of green energy in irrigation	Smart irrigation system based on photovoltaic parks	Efficient trading, management, and utilization of energy for irrigation systems
[101]	Scalable network of smart cities with hybrid architecture	Development of a model for real-time processing of the edge nodes	Enhanced resiliency of the system
[102]	Security issues for the smart city	Blockchain utility in smart communities	An in-depth survey covering various perspectives of blockchain in smart cities
[103]	Social issues	Solving social solutions through blockchain application	Applications and research opportunities in the paradigm of a smart city using BC
[104]	Supply chain data management	Implementation of salient features of BC, viz., immutability, transparency, decentralization, etc., to improve the efficacy of supply chain management in the industry	BC chain-based food traceability system as a case study with the deployment of BC in order to enhance the efficacy of supply chain management in the industry

Table 6. *Cont.*

Reference	Objectives	Solutions/Results	Advantages/Opportunities
[105]	Models and applications with secure transactions	Through surveys, they identified research opportunities	Creating new applications and interoperability between models
[106]	Carbon emissions monitoring	A three-step blockchain that uses smart contracting	Enhanced security with advanced features
[107]	Efficient urban mobility	Traffic decongestion	Data transparency, immutability for enhanced resilient traffic management
[108]	Augmented democracy	Involvement of citizens in decision making	Determination in real-time of the persons participating in the elections of the citizens in a decentralized and confidential way
[109]	Synergy of IoT and BC	Use of multilayer blockchain	The technology used ensures the competitive efficiency of cryptographic security and confidentiality
[110]	BC for industrial IoT	Improving the performance of industrial IoT devices by minimizing unfair, permissioned BC	Development of novel algorithms considering waiting time for packing of permissioned BC data

3.6.2. Architecture of Blockchain for SCs

The prospects of the IoT determine the smart city architecture, the multitude of sensors and smart objects that help collect data collected from public infrastructure, public access to data, increasing the quality of services and costs of environmental protection, and economic development. The general architecture of blockchain for SCs is shown in Figure 18.

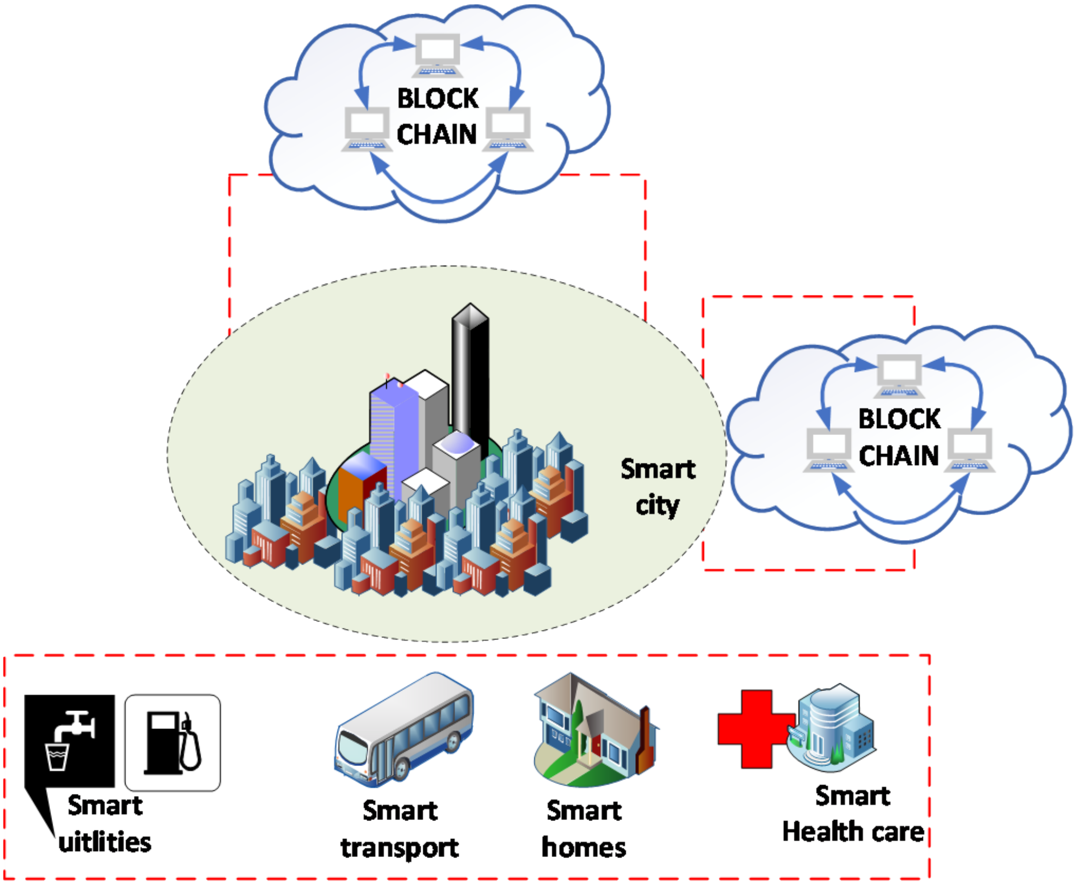

Figure 18. Blockchain architecture for SC applications.

Using the same blockchain network for all the services in the smart city is not feasible. Therefore, multiple blockchain networks have to be used depending on the size of the city and the nature of smart services provided. Each blockchain network may cater to the requirements of a single service. Smart devices, i.e., smart transport vehicles, smart sensors in homes, smart monitoring devices in hospitals, etc., generate data that is put into a blockchain related to its service. Proper protocols and blockchain frameworks will be needed to ensure the smooth operation of the services.

3.6.3. Challenges for Blockchain for SCs

SC has many different entities. The blockchain network used by the SCs' various entities varies with the application type. These applications have diverse requirements. For example, in the case of smart transportation, the devices are changing their locations, and in the case of smart lighting, the devices are static. The blockchain architecture must be planned according to the nature of the application. Additionally, the entities are spread over a large geographical area, and to meet the criterion for real-time analysis, the blockchain must be fast and secure. Additionally, interoperability between different blockchain networks in the SC is a challenge.

3.7. Blockchain for Energy Management System

Developing and implementing the distributed system, both in production and consumption and energy marketing, brought new benefits to producers and consumers. Moreover, the increasing energy use from wind turbines and photovoltaic panels necessitated changing the energy market's architecture and secure energy transactions. Blockchain technology can be used for this purpose.

3.7.1. Architecture of Blockchain for Energy Management System

The blockchain has enormous potential in the transaction related to energy marketing. EMS aims to ensure reliable energy trading in real-time, including all energy market entities such as generation systems (both renewable energy sources and non-renewable energy sources), customer systems, grid operators, etc. The blockchain architecture for EMS is shown in Figure 19.

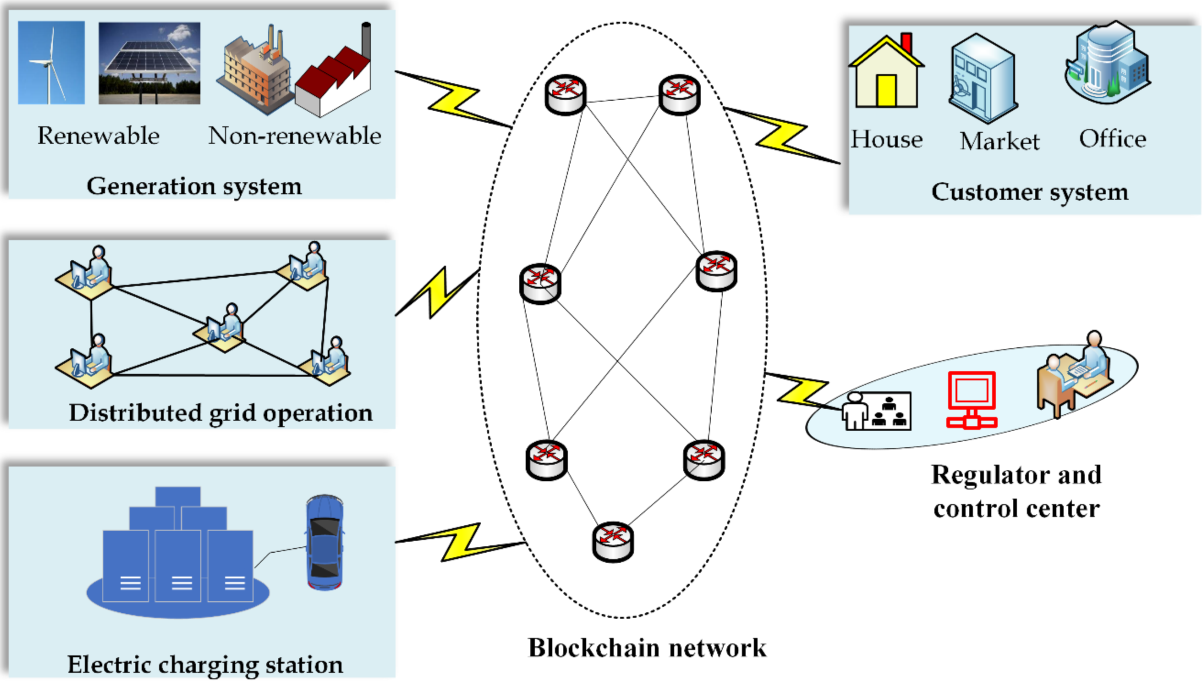

Figure 19. The architecture of blockchain-based EMS.

The SG envisioned integrating renewable energy sources with conventional energy sources as generation sources. On the consumer side, there are individual homes, residential buildings, offices, market complexes, etc. In addition to these, the EV charging stations also fall in the consumer domain of the SG. However, the consumer domain entities act not only as the electricity consumer but also as the electricity producer. Such consumers can be referred to as prosumers. When surplus electricity is available at prosumers, it is contributed to reducing the burden on the generation system.

On the one hand, it reduces the burden of the generation system, but on the other hand, it becomes vital to monitor the energy trading between users. Additionally, security and privacy in the energy trading market are equally important. To achieve this objective, blockchain can be integrated into the EMS.

The blockchain aims to integrate all domains of the SG, such as the generation system, operation system, the consumer system, regulator, and control center, using the blockchain network as shown in Figure 19. The blockchain-based EMS ensures the security and privacy of energy transactions through its distributed approach, interoperability, and smart contracts. The private blockchain can implement data permissions and selective consortium access to ensure security and privacy in energy trading. Due to distributed approach, blockchain-based EMS augments the transparency without compromising privacy in peer-to-peer energy trading.

3.7.2. A Panoramic Overview of Blockchain for EMS

The research on blockchain for EMS is gaining momentum and has been discussed in many recent works. As the amount of energy increases in trading, the greater the difficulties. So, this trading system needs to be controlled very carefully. An online energy transaction management model was proposed in ref. [111] where users can obtain information on their own trading and consumption through energetic transaction. For the transaction to be secure and fast, a payment plan was proposed based on the loan's value. Jiawei Yang et al., in ref. [112], propose a public pricing scheme based on the blockchain. The price is influenced by the share borne by the miners who are taxed with a part of the income for the power losses. The smart contract was created, although the testing was conducted with only 27 prosumers. The biggest problem when we talk about the price of energy in the trading process by using the blockchain is the high energy consumption used by this technology, which was resolved in ref. [113].

The security challenge was dealt with by Yi Zhang et al. in ref. [114] for users and energy flow. In ref. [115], S.N.G. Gourisetti et al. proposed an energy market framework using the online double auction. The authors explain the benefits and usefulness of blockchain technology and its use for transactional energy. The prognosis is that this technology and the implementation of smart contracts in stages can minimize and eliminate the challenge elements in key and certificate management. The authors stated that they expect that lower energy consumption will be achieved if users are more receptive.

Blockchain technology has allowed smart meters with enhanced security and privacy features. Further, a platform to monitor the energy generated from renewable sources by storing and trading energy between residents and network services of users was proposed in ref. [116]. The possibility of trading renewable energy generated by private producers using blockchain technology was shown in ref. [117]. The authors offer a high scalability solution based on smart contracts, which will not harm the decentralized system and data security. The costs of transactions made in this way will be lower compared with current blockchain costs. A cloud services platform for energy trading was proposed in ref. [118] by Lei Wang et al. Both users and suppliers participated in the platform, and the intelligent contract for trading between the parties was created. Antchain is used to make smart contracts, trade, and use the services offered by the cloud. The evolution over time of blockchain technology in the energy trading sector and the issues that stop the application of this technology were presented in ref. [119]. In ref. [120], the authors present the blockchain used by customers to pay for energy consumption. Some seminal work in this direction is comprehensively analyzed in Table 7.

Table 7. Summary of works on blockchain for EMS applications.

Reference	Subdomain	Objectives	Solutions/Results	Technologies	Advantages/Opportunities	Challenges

[111]	Secure energy transaction	Securing and controlling risks in energy transactions	Online transaction management is followed;
			Trading model;
			Smart contracts;
			Calculation of payment rates.
				Blockchain	Real-time verification of individual consumer transactions.	System security with: proxy re-encryption and homomorphic encryption;
						Improvement credit trading management.

[112]	Energy price	Establishing the public price of traded energy	Trading with *elecoin*	Blockchain	Supervision of transactions by network members.	The power supply system should be extended to applications.
[113]	Blockchain performance. Blockchain-based virtual electricity generation	Decreasing the cost of electricity to supply the process during the operation of the blockchain.	Reduction of energy consumption during the mining process.	Blockchain	Solutions to increase the energy efficiency of the technology	Applying and deepening the study of the reduction of energy consumption consumed by the network.
[114]	Smart contract trading	Securing energy flow and users.	Value calculation according to users and producers divided according to certain criteria (diversity).	Blockchain	Differentiated tariffs taking into account a classification of producers and consumers respectively.	Classifying users and establishing quotas according to the green energy produced and consumption; The approach methods for energy production to be planned according to the real conditions have not been studied; Improving the smart contract system.
[115]	Energy market	Energy architecture objectives.	Stage implementation of smart contracts.	Blockchain	Increased security.	Key and certificate management. Coverage in a larger area of more general market/industry.
[116]	Energy trading	Energy trading between residents	Decentralized optimization algorithm, energy distribution according to a predetermined program for energy trading to the user network.	Blockchain	Efficient trading without decentralized intermediaries.	Improving energy management. The platform will be tested on a larger community of residents, by improving the algorithm.
[117]	Renewable energy	Energy trading	A blockchain scalability solution.	Blockchain	Low transaction costs.	Development and widespread use of blockchain energy trading.
[118]	Smart contract	Cloud services platform design for energy	Realization of the trading platform with intelligent contract.	Blockchain	Trading without intermediaries	Improving cloud services, adding value green certificate, energy storage and other services, application and early service in the integrated energy market
[119]	Blockchain evolution and challenges	The widespread use of blockchain technology in the energy trading process.	Use of the decentralized system; Smart contract.	Blockchain	Trading through a secure decentralized system.	Secure, decentralized energy development
[120]	Energy management-household consumers	Energy trading management between customers.	Use of electric power inverters in the network; Energy-saving technique testing.	Blockchain	Distributes energy from one home user to another within the decentralized network; Management performed for the purpose of energy distribution planning for the client; Communication networks are independent.	Energy network development.
[121]	Energy trading in microgrids	Beneficial energy trading.	Interactive double auction and blockchain technology	Blockchain	Lower price set by consensus of both producers and buyers.	Controlling the marketing of the amount of energy produced. Study the problems that occur when a network node has problems.
[122]	Energy transaction	Shared network study	Trading platform. Encouraging the use of renewable energy	Blockchain	Blockchain with distributed trading energy storage, is efficient and reliable.	High flexibility and security of the power system and subsequent exploration to be done together.

4. Blockchain for Cybersecurity in SG

The immediate need to incorporate renewable energy sources has necessitated considering a more diversified and distributed structure for the SG. This objective was achieved through distributed generation system and DER [123]. However, this has increased the complexity of the SG. Further, the SG's complex infrastructure comprises several devices such as the PMUs, smart meters, home automation sensors, remote terminal unit, spanning generation, transmission, distribution, customer, operation, marketing, and utility domains, etc. [124]. Situational awareness is vital to ensure the resiliency of such a marvelous SG infrastructure. The communication infrastructure and the communication protocols needed to support these applications vary. The core of the communication network is a wide area network (WAN). In addition to this, there exist other types of communication networks such as local area networks (LAN), home area networks (HAN), wireless sensor networks (WSN), neighborhood area networks (NAN), etc. These communication networks mostly use TCP/IP protocol suite for data communication. TCP/IP is not a secure protocol. Hence, the communication network of the SG applications can be easily attacked by exploiting its vulnerability. Despite the basic security measures such as firewall, intrusion detection, encryption, authentication, etc., which are already implemented in the SG, though it is still vulnerable to several cyber-attacks. An excellent survey on various detection algorithms was provided on false data injection in ref. [125].

The SG is a typical cyber-physical system [126]. As a cyber-physical system, cybersecurity is a vital parameter with three features: availability, confidentiality, and integrity. Availability is characterized as the property in which all data are available promptly. The cyberattack can compromise availability by blocking, delaying, and corrupting the data or even losing the data. The impact of cyber-attack on the availability of SG applications is huge. Confidentiality is characterized as the property of the system to protect the privacy and proprietary information from unauthorized access. The cyberattack on confidentiality can compromise the privacy and proprietary information of the SG application. Such incidents can grant illegal access to the application by stealing password-related information, causing enormous loss to the operation of the application. Integrity is characterized as the application's property to protect the system from unauthorized access to avoid any modification, alternation, and destruction of the data. The cyberattacks on integrity can modify the data to configure the application, resulting in an enormous loss. For example, the modification data can lead to misconfiguration of the sensors leading to failure of the SG application.

Blockchain is a distributed ledger that is immutable and does not depend upon any third party for its execution. This makes blockchain a secure method for data transactions and thus plays a vital role in SG applications. The blockchain can explicitly be used to mitigate the cyberattacks to strengthen the SG application's security. Among the different blockchains, the public blockchain is highly secure compared with the consortium and private blockchain due to the nature of the members and the consensus mechanism. The members of the public blockchain can be anonymous, whereas only the trusted nodes can be members of the consortium and private blockchains. The consensus mechanism followed in the public blockchain is proof-of-work, whereas multi-party voting in the consortium blockchain and strictly pre-approved nodes in the private blockchain are followed as a consensus mechanism. However, computational complexity is very high in the public blockchain. Thus, when security threats are fewer, and computation complexity is low, consortium and private blockchains are preferable to the public blockchain. The architecture of the blockchain for cybersecurity in SG applications is shown in Figure 20.

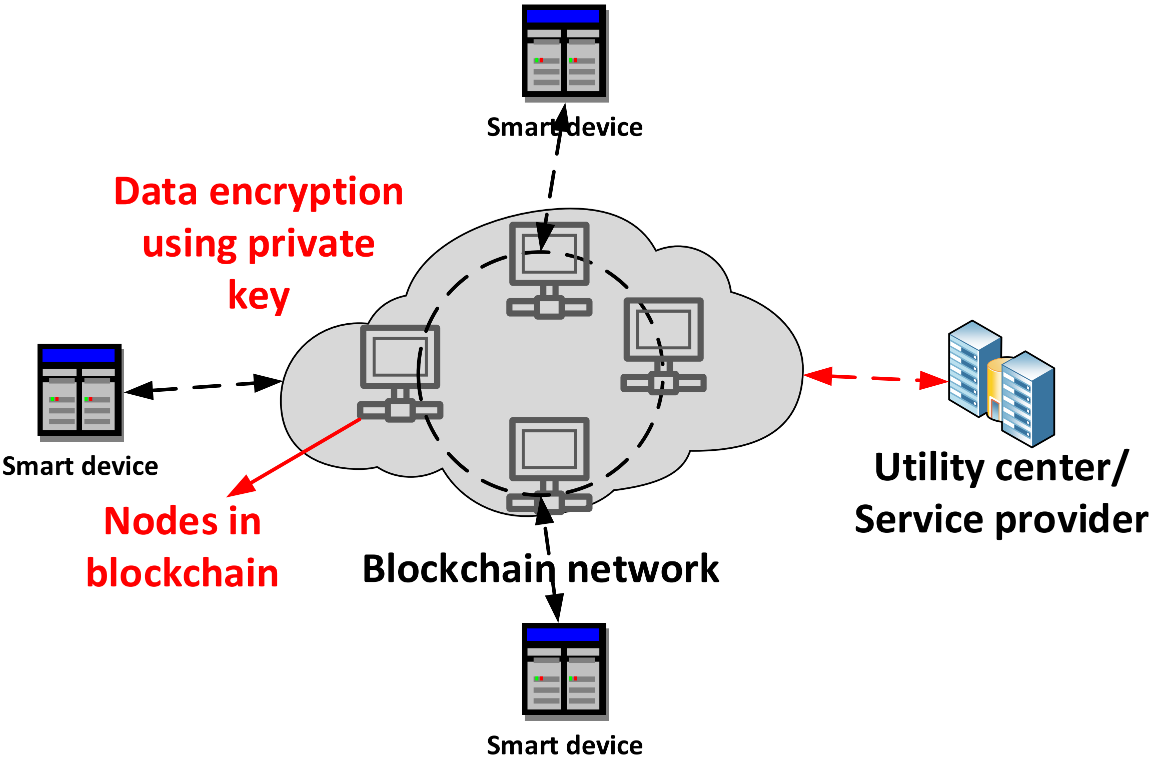

Figure 20. The architecture of SG cybersecurity using blockchain.

The smart devices generate data communicated to the blockchain network server using the TCP/IP protocol. If the devices are computationally powerful, the hashing of the data and its encryption can be performed at the device itself, thereby creating the block, which is then placed into the blockchain network. This is the most secure architecture, as any data tampering after it leaves the device results in a change in the has function, leading to the invalidation of the block. However, this puts much computational pressure on the end devices, which are already over-burdened by other tasks. The other alternative is to send the data to the servers/nodes in the blockchain using TCP/IP and generate the blocks in the blockchain. This is less secure, but it is not a computationally powerful smart devices. In the latter case, using private and public keys for extra authentication can be beneficial. This architecture envisions maximizing the security since all participants in the consortium blockchain are trusted, and the consensus mechanism is based on multi-party voting with no scope for anonymity. The administrative and management authorities select the member nodes acting as miners for the consortium and private blockchain. Next, the works related to blockchain for SG cybersecurity are comprehensively summarized in Table 8.

Table 8. Summary of works on blockchain for SG cybersecurity.

Reference	SG Application	Summary
[127]	AMI	A quantum key distribution-based secure key transmission is proposed for increasing the security of smart meters against cyber-attacks
[128]	Applicable to all	A multi-layer protocol is proposed to enhance the cyber-security of SG applications.
[81]	EMS and MG	A blockchain framework for P2P energy transactions is proposed, using a novel consensus algorithm for enhanced cyber security.
[129]	EMS and MG	A novel blockchain hyperledger is proposed for secure transactions on energy distribution.
[130]	MGs	A master-slave mechanism is proposed to protect the data against malicious attacks.
[131]	EMS	A novel rewarding scheme is presented for network security. Additionally, smart contracts are used for safe data storage.

Blockchain technology for SG applications is still in the research phase and is gradually finding practical utility. Secure mechanisms are needed that can be implemented at the device level before the data leave the device. These mechanisms should be light and can be implemented in real-time.

5. Conclusions

SG is evolving with the developments in storage and computational technologies. One such technology that can potentially transform the transactions amongst the various entities of the SG is the blockchain. The blockchain offers a decentralized and secure means of authorizing transactions, removing the need for a centralized authority. Despite its tremendous application in other domains, it has been underutilized for SG applications. This paper reviewed blockchain technology from a utility perspective for SG applications. General architectures were proposed for the important SG applications and identified challenges. The review is expected to enhance the research on developing novel technologies to meet the requirements of practical SG applications.

The blockchain-based applications are still in the nascent stage from various perspectives, which are seen as future research problems. Many SG applications operate in real-time, and the blockchain should not overburden the applications. The resource requirements for computation are a major challenge in blockchain-based systems. Blockchain must be developed to work on a lighter framework while retaining its security features. Additionally, regulatory bodies have to develop standardization procedures to make this technology interoperable and popular. Some of these research problems can be solved in the future, thoroughly revolutionizing blockchain-based applications.

Author Contributions: Conceptualization, B.A.; methodology, B.A.; software, S.K.M. (Sunil Kumar Mishra), S.K.M. (Santosh Kumar Mishra) and A.V.J.; validation, N.T., P.T. and N.B.; investigation, N.T., P.T., N.B. and B.A.; resources, S.K.M. (Sunil Kumar Mishra), S.K.M. (Santosh Kumar Mishra), A.V.J., I.S.S., F.M.E. and F.G.B.; data curation, F.M.E., N.B. and B.A.; writing—original draft preparation, S.K.M. (Sunil Kumar Mishra), S.K.M. (Santosh Kumar Mishra), A.V.J., I.S.S., F.M.E., B.A. and F.G.B.; supervision, N.B. and B.A.; project administration, N.B. and B.A.; formal analysis: N.T. and P.T.; funding acquisition: N.T. and P.T.; visualization: N.T., P.T., N.B. and B.A.; writing—review and editing: N.T., P.T., N.B. and B.A.; figures and tables: I.S.S. and A.V.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Framework Agreement between University of Pitesti (Romania) and King Mongkut's University of Technology North Bangkok (Thailand), in part by an International Research Partnership "Electrical Engineering—Thai French Research Center (EE-TFRC)" under the project framework of the Lorraine Université d'Excellence (LUE) in cooperation between Université de Lorraine and King Mongkut's University of Technology North Bangkok and in part by the National Research Council of Thailand (NRCT) under Senior Research Scholar Program under Grant No. N42A640328, and in part by National Science, Research and Innovation Fund (NSRF) under King Mongkut's University of Technology North Bangkok under Grant no. KMUTNB-FF-65-20.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jha, A.V.; Ghazali, A.N.; Appasani, B.; Ravariu, C.; Srinivasulu, A. Reliability Analysis of Smart Grid Networks Incorporating Hardware Failures and Packet Loss. *Rev. Roum. Sci. Tech. El.* **2021**, *65*, 245–252.
2. Mahmoud, M.A.; Nasir, N.R.; Gurunathan, M.; Raj, P.; Mostafa, S.A. The Current State of the Art in Research on Predictive Maintenance in Smart Grid Distribution Network: Fault's Types, Causes, and Prediction Methods—A Systematic Review. *Energies* **2021**, *14*, 5078. [CrossRef]
3. Appasani, B.; Jha, A.V.; Mishra, S.K.; Ghazali, A.N. Communication infrastructure for situational awareness enhancement in WAMS with optimal PMU placement. *Prot. Control Mod. Power Syst.* **2021**, *6*, 9. [CrossRef]

4. Yapa, C.; de Alwis, C.; Liyanage, M.; Ekanayake, J. Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research. *Energy Rep.* **2021**, *7*, 6530–6564. [CrossRef]
5. Kaltakis, K.; Polyzi, P.; Drosatos, G.; Rantos, K. Privacy-Preserving Solutions in Blockchain-Enabled Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 9792. [CrossRef]
6. Baidya, S.; Potdar, V.; Ray, P.P.; Nandi, C. Reviewing the opportunities, challenges, and future directions for the digitalization of energy. *Energy Res. Soc. Sci.* **2021**, *81*, 102243. [CrossRef]
7. Ma, Z.; Clausen, A.; Lin, Y.; Jørgensen, B.N. An overview of digitalization for the building-to-grid ecosystem. *Energy Inform.* **2021**, *4*, 36. [CrossRef]
8. Hasankhani, A.; Hakimi, S.M.; Bisheh-Niasar, M.; Shafie-Khah, M.; Asadolahi, H. Blockchain technology in the future smart grids: A comprehensive review and frameworks. *Int. J. Electr. Power Energy Syst.* **2021**, *129*, 106811. [CrossRef]
9. Liu, C.; Zhang, X.; Chai, K.K.; Loo, J.; Chen, Y. A survey on blockchain-enabled smart grids: Advances, applications and challenges. *IET Smart Cities* **2021**, *3*, 56–78. [CrossRef]
10. Guru, D.; Perumal, S.; Varadarajan, V. Approaches towards Blockchain Innovation: A Survey and Future Directions. *Electronics* **2021**, *10*, 1219. [CrossRef]
11. Wang, Q.; Li, R.; Zhan, L. Blockchain technology in the energy sector: From basic research to real world applications. *Comput. Sci. Rev.* **2021**, *39*, 100362. [CrossRef]
12. Yagmur, A.; Dedeturk, B.A.; Soran, A.; Jung, J.; Onen, A. Blockchain-Based Energy Applications: The DSO Perspective. *IEEE Access* **2021**, *9*, 145605–145625. [CrossRef]
13. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
14. Kumar, N.M.; Chand, A.A.; Malvoni, M.; Prasad, K.A.; Mamun, K.A.; Islam, F.; Chopra, S.S. Distributed energy resources and the application of AI, IoT, and blockchain in smart grids. *Energies* **2020**, *13*, 5739. [CrossRef]
15. Miglani, A.; Kumar, N.; Chamola, V.; Zeadally, S. Blockchain for Internet of Energy management: Review, solutions, and challenges. *Comput. Commun.* **2020**, *151*, 395–418. [CrossRef]
16. Zia, M.F.; Benbouzid, M.; Elbouchikhi, E.; Muyeen, S.M.; Techato, K.; Guerrero, J.M. Microgrid Transactive Energy: Review, Architectures, Distributed Ledger Technologies, and Market Analysis. *IEEE Access* **2020**, *8*, 19410–19432. [CrossRef]
17. Rathore, H.; Mohamed, A.; Guizani, M. A Survey of Blockchain Enabled Cyber-Physical Systems. *Sensors* **2020**, *20*, 282. [CrossRef]
18. Khajeh, H.; Laaksonen, H.; Gazafroudi, A.S.; Shafie-Khah, M. Towards Flexibility Trading at TSO-DSO-Customer Levels: A Review. *Energies* **2019**, *13*, 165. [CrossRef]
19. Alladi, T.; Chamola, V.; Rodrigues, J.J.P.C.; Kozlov, S.A. Blockchain in Smart Grids: A Review on Different Use Cases. *Sensors* **2019**, *19*, 4862. [CrossRef]
20. Nezamabadi, H.; Vahidinasab, V. Microgrids Bidding Strategy in a Transactive Energy Market. *Sci. Iran.* **2019**, *26*, 3622–3634. [CrossRef]
21. Erturk, E.; Lopez, D.; Yu, W.Y. Benefits and Risks of Using Blockchain in Smart Energy: A Literature Review. *Contemp. Manag. Res.* **2019**, *15*, 205–225. [CrossRef]
22. Abdella, J.; Shuaib, K. Peer to Peer Distributed Energy Trading in Smart Grids: A Survey. *Energies* **2018**, *11*, 1560. [CrossRef]
23. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
24. Lim, M.K.; Li, Y.; Wang, C.; Tseng, M.-L. A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Comput. Ind. Eng.* **2021**, *154*, 107133. [CrossRef]
25. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A Survey on Blockchain for Information Systems Management and Security. *Inf. Process. Manag.* **2020**, *58*, 102397. [CrossRef]
26. Meng, T.; Zhao, Y.; Wolter, K.; Xu, C.-Z. On Consortium Blockchain Consistency: A Queueing Network Model Approach. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1369–1382. [CrossRef]
27. Bhattacharjee, A.; Badsha, S.; Shahid, A.R.; Livani, H.; Sengupta, S. Block-Phasor: A Decentralized Blockchain Framework to Enhance Security of Synchrophasor. In Proceedings of the 2020 IEEE Kansas Power and Energy Conference (KPEC), Manhattan, KS, USA, 13–14 July 2020; pp. 1–6. [CrossRef]
28. Appasani, B.; Mohanta, D.K. A review on synchrophasor communication system: Communication technologies, standards and applications. *Prot. Control Mod. Power Syst.* **2018**, *3*, 37. [CrossRef]
29. Jha, A.; Appasani, B.; Ghazali, A.; Bizon, N. A Comprehensive Risk Assessment Framework for Synchrophasor Communication Networks in a Smart Grid Cyber Physical System with a Case Study. *Energies* **2021**, *14*, 3428. [CrossRef]
30. Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D.K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. *Wirel. Netw.* **2021**, *27*, 2595–2613. [CrossRef]
31. Appasani, B.; Mohanta, D.K. Co-Optimal Placement of PMUs and Their Communication Infrastructure for Minimization of Propagation Delay in the WAMS. *IEEE Trans. Ind. Inform.* **2018**, *14*, 2120–2132. [CrossRef]
32. Jha, A.V.; Appasani, B.; Ghazali, A.N. Analytical Channel Modelling of Synchrophsor Communication Networks in a Smart Grid Cyber Physical System. In Proceedings of the 2021 3rd Global Power, Energy and Communication Conference (GPECOM), Antalya, Turkey, 5–8 October 2021; pp. 257–262. [CrossRef]

33. Krishna, R.R.; Priyadarshini, A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. *Sustainability* **2021**, *13*, 9463. [CrossRef]
34. Jha, A.V.; Ghazali, A.N.; Appasani, B.; Mohanta, D.K. Risk Identification and Risk Assessment of Communication Net-works in Smart Grid Cyber-Physical Systems. In *Security in Cyber-Physical Systems: Foundations and Applications*; Studies in Systems, Decision and Control; Awad, A.I., Furnell, S., Paprzycki, M., Sharma, S.K., Eds.; Springer: Cham, Switzerland, 2021; Volume 339, pp. 217–253. [CrossRef]
35. Jha, A.V.; Appasani, B.; Ghazali, A.N. Performance Evaluation of Routing Protocols in Synchrophasor Communication Networks. In Proceedings of the 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India, 19–21 December 2019; pp. 132–136.
36. Wazid, M.; Das, A.K.; Shetty, S.; Jo, M. A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things. *IEEE Access* **2020**, *8*, 88700–88716. [CrossRef]
37. Arif, S.; Khan, M.A.; Rehman, S.U.; Kabir, M.A.; Imran, M. Investigating Smart Home Security: Is Blockchain the Answer? *IEEE Access* **2020**, *8*, 117802–117816. [CrossRef]
38. Xue, J.; Xu, C.; Zhang, Y. Private Blockchain-Based Secure Access Control for Smart Home Systems. *KSII Trans. Internet Inf. Syst.* **2018**, *12*, 6057–6078. [CrossRef]
39. Tantidham, T.; Aung, Y.N. Emergency Service for Smart Home System Using Ethereum Blockchain: System and Architecture. In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 888–893. [CrossRef]
40. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef]
41. Monrat, A.A.; Schelen, O.; Andersson, K. Blockchain Mobility Solution for Charging Transactions of Electrical Vehicles. In Proceedings of the 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC), Leicester, UK, 7–10 December 2020; pp. 253–348. [CrossRef]
42. Rupasinghe, T.; Burstein, F.; Rudolph, C.; Strange, S. Towards a Blockchain based Fall Prediction Model for Aged Care. In Proceedings of the PervasiveHealth: Pervasive Computing Technologies for Healthcare, Sydnet, Australia, 29–31 January 2019; pp. 1–10. [CrossRef]
43. Almadhoun, R.; Kadadha, M.; Alhemeiri, M.; Alshehhi, M.; Salah, K. A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–8. [CrossRef]
44. Decker, C.; Wattenhofer, R. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Cham, Switzerland, 2015; Volume 9212, pp. 3–18. [CrossRef]
45. Zhong, L.; Wu, Q.; Xie, J.; Li, J.; Qin, B. A secure versatile light payment system based on blockchain. *Futur. Gener. Comput. Syst.* **2018**, *93*, 327–337. [CrossRef]
46. Majeed, R.; Abdullah, N.A.; Ashraf, I.; Bin Zikria, Y.; Mushtaq, M.F.; Umer, M. An Intelligent, Secure, and Smart Home Automation System. *Sci. Program.* **2020**, *2020*, 4579291. [CrossRef]
47. El Houda, Z.A.; Hafid, A.; Khoukhi, L. Blockchain Meets AMI: Towards Secure Advanced Metering Infrastructures. In Proceedings of the IEEE International Conference on Communications, Dublin, Ireland, 7–11 June 2020.
48. Kamal, M.; Tariq, M. Light-Weight Security and Blockchain Based Provenance for Advanced Metering Infrastructure. *IEEE Access* **2019**, *7*, 87345–87356. [CrossRef]
49. Khalid, R.; Javaid, N.; Almogren, A.; Javed, M.U.; Javaid, S.; Zuair, M. A Blockchain-Based Load Balancing in Decentralized Hybrid P2P Energy Trading Market in Smart Grid. *IEEE Access* **2020**, *8*, 47047–47062. [CrossRef]
50. Sovacool, B.K.; Kester, J.; Noel, L.; de Rubens, G.Z. Actors, business models, and innovation activity systems for vehicle-to-grid (V2G) technology: A comprehensive review. *Renew. Sustain. Energy Rev.* **2020**, *131*, 109963. [CrossRef]
51. Islam, M.; Shahjalal; Hasan, M.K.; Jang, Y.M. Blockchain-based Energy Transaction Model for Electric Vehicles in V2G Network. In Proceedings of the 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 19–21 February 2020; pp. 628–630. [CrossRef]
52. Rehman, A.; Hassan, M.F.; Yew, K.H.; Paputungan, I.; Tran, D.C. State-of-the-art IoV trust management a meta-synthesis systematic literature review (SLR). *PeerJ Comput. Sci.* **2020**, *6*, e334. [CrossRef] [PubMed]
53. Pal, R.; Chavhan, S.; Gupta, D.; Khanna, A.; Padmanaban, S.; Khan, B.; Rodrigues, J.J.P.C. A comprehensive review on IoT-based infrastructure for smart grid applications. *IET Renew. Power Gener.* **2021**, *15*, 3761–3776. [CrossRef]
54. Gschwendtner, C.; Sinsel, S.R.; Stephan, A. Vehicle-to-X (V2X) implementation: An overview of predominate trial configurations and technical, social and regulatory challenges. *Renew. Sustain. Energy Rev.* **2021**, *145*, 110977. [CrossRef]
55. Khan, M.A.; Ghosh, S.; Busari, S.A.; Huq, K.M.S.; Dagiuklas, T.; Mumtaz, S.; Iqbal, M.; Rodriguez, J. Robust, Resilient and Reliable Architecture for V2X Communications. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4414–4430. [CrossRef]
56. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for 5G and beyond networks: A state of the art survey. *J. Netw. Comput. Appl.* **2020**, *166*, 102693. [CrossRef]
57. Xu, C.; Wu, H.; Liu, H.; Li, X.; Liu, L.; Wang, P. An Intelligent Scheduling Access Privacy Protection Model of Electric Vehicle Based on 5G-V2X. *Sci. Program.* **2021**, *2021*, 1198794. [CrossRef]

58. Bhattacharya, P.; Tanwar, S.; Bodkhe, U.; Kumar, A.; Kumar, N. EVBlocks: A Blockchain-Based Secure Energy Trading Scheme for Electric Vehicles underlying 5G-V2X Ecosystems. *Wirel. Pers. Commun.* **2021**, 1–41. [CrossRef]
59. Jameel, F.; Javed, M.A.; Zeadally, S.; Jantti, R. Efficient Mining Cluster Selection for Blockchain-Based Cellular V2X Communications. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4064–4072. [CrossRef]
60. Rawat, D.B.; Doku, R.; Adebayo, A.; Bajracharya, C.; Kamhoua, C. Blockchain Enabled Named Data Networking for Secure Vehicle-to-Everything Communications. *IEEE Netw.* **2020**, *34*, 185–189. [CrossRef]
61. Rasheed, M.B.; Javaid, N.; Ahmad, A.; Awais, M.; Khan, Z.A.; Qasim, U.; Alrajeh, N. Priority and delay constrained demand side management in real-time price environment with renewable energy source. *Int. J. Energy Res.* **2016**, *40*, 2002–2021. [CrossRef]
62. Khan, P.; Byun, Y.-C. Blockchain-Based Peer-to-Peer Energy Trading and Charging Payment System for Electric Vehicles. *Sustainability* **2021**, *13*, 7962. [CrossRef]
63. Sadiq, A.; Javed, M.U.; Khalid, R.; Almogren, A.; Shafiq, M.; Javaid, N. Blockchain Based Data and Energy Trading in Internet of Electric Vehicles. *IEEE Access* **2020**, *9*, 7000–7020. [CrossRef]
64. Musleh, A.S.; Yao, G.; Muyeen, S.M. Blockchain Applications in Smart Grid–Review and Frameworks. *IEEE Access* **2019**, *7*, 86746–86757. [CrossRef]
65. Kim, M.; Park, K.; Yu, S.; Lee, J.; Park, Y.; Lee, S.-W.; Chung, B. A Secure Charging System for Electric Vehicles Based on Blockchain. *Sensors* **2019**, *19*, 3028. [CrossRef] [PubMed]
66. Dorokhova, M.; Vianin, J.; Alder, J.-M.; Ballif, C.; Wyrsch, N.; Wannier, D. A Blockchain-Supported Framework for Charging Management of Electric Vehicles. *Energies* **2021**, *14*, 7144. [CrossRef]
67. Buterin, V. Ethereum Platform Review—Opportunities and Challenges for Private and Consortium Blockchains. Available online: http://www.smallake.kr/wp-content/uploads/2016/06/314477721-Ethereum-Platform-Review-Opportunities-and-Challenges-for-Private-and-Consortium-Blockchains.pdf (accessed on 10 January 2022).
68. Saxena, S.; Farag, H.E.Z.; Brookson, A.; Turesson, H.; Kim, H. A Permissioned Blockchain System to Reduce Peak Demand in Residential Communities via Energy Trading: A Real-World Case Study. *IEEE Access* **2020**, *9*, 5517–5530. [CrossRef]
69. Huang, Z.; Li, Z.; Lai, C.S.; Zhao, Z.; Wu, X.; Li, X.; Tong, N.; Lai, L.L. A Novel Power Market Mechanism Based on Blockchain for Electric Vehicle Charging Stations. *Electronics* **2021**, *10*, 307. [CrossRef]
70. Birleanu, G.F.; Bizon, N. Control and Protection of the Smart Microgrids Using Internet of Things: Technologies, Architecture and Applications. In *Microgrid Architectures, Control and Protection Methods*, 1st ed.; Tabatabaei, N.M., Kabalci, E., Bizon, N., Eds.; Springer: Cham, Switzerland, 2020; pp. 749–770. [CrossRef]
71. Birleanu, G.F.; Anghelescu, P.; Bizon, N.; Pricop, E. Cyber Security Objectives and Requirements for Smart Grid. In *Smart Grids and Their Communication Systems*, 1st ed.; Kabalci, E., Kabalci, Y., Eds.; Springer: Singapore, 2019; pp. 607–634. [CrossRef]
72. Birleanu, G.F.; Anghelescu, P.; Bizon, N. Malicious and Deliberate Attacks and Power System Resiliency. In *Power Systems Resiliency: Modeling, Analysis and Practice*, 1st ed.; Tabatabaei, N.M., Ravadanegh, S.N., Bizon, N., Eds.; Springer: Cham, Switzerland, 2018; pp. 223–246. [CrossRef]
73. Ahmethodzic, L.; Music, M. Comprehensive review of trends in microgrid control. *Renew. Energy Focus* **2021**, *38*, 84–96. [CrossRef]
74. Foti, M.; Vavalis, M. What blockchain can do for power grids? *Blockchain Res. Appl.* **2021**, *2*, 100008. [CrossRef]
75. Valdivia, A.D.; Balcell, M.P. Connecting the grids: A review of blockchain governance in distributed energy transitions. *Energy Res. Soc. Sci.* **2021**, *84*, 102383. [CrossRef]
76. Aybar-Mejía, M.; Rosario-Weeks, D.; Mariano-Hernández, D.; Domínguez-Garabitos, M. An approach for applying blockchain technology in centralized electricity markets. *Electr. J.* **2021**, *34*, 106918. [CrossRef]
77. Yahaya, A.S.; Javaid, N.; Alzahrani, F.A.; Rehman, A.; Ullah, I.; Shahid, A.; Shafiq, M. Blockchain Based Sustainable Local Energy Trading Considering Home Energy Management and Demurrage Mechanism. *Sustainability* **2020**, *12*, 3385. [CrossRef]
78. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A blockchain-based smart grid: Towards sustainable local energy markets. *Comput. Sci. Res. Dev.* **2017**, *33*, 207–214. [CrossRef]
79. Antal, C.; Cioara, T.; Antal, M.; Mihailescu, V.; Mitrea, D.; Anghel, I.; Salomie, I.; Raveduto, G.; Bertoncini, M.; Croce, V.; et al. Blockchain based decentralized local energy flexibility market. *Energy Rep.* **2021**, *7*, 5269–5288. [CrossRef]
80. Vieira, G.; Zhang, J. Peer-to-peer energy trading in a microgrid leveraged by smart contracts. *Renew. Sustain. Energy Rev.* **2021**, *143*, 110900. [CrossRef]
81. Kavousi-Fard, A.; Almutairi, A.; Al-Sumaiti, A.; Farughian, A.; Alyami, S. An effective secured peer-to-peer energy market based on blockchain architecture for the interconnected microgrid and smart grid. *Int. J. Electr. Power Energy Syst.* **2021**, *132*, 107171. [CrossRef]
82. van Leeuwen, G.; AlSkaif, T.; Gibescu, M.; van Sark, W. An integrated blockchain-based energy management platform with bilateral trading for microgrid communities. *Appl. Energy* **2020**, *263*, 114613. [CrossRef]
83. Yildizbasi, A. Blockchain and renewable energy: Integration challenges in circular economy era. *Renew. Energy* **2021**, *176*, 183–197. [CrossRef]
84. Tsao, Y.-C.; Thanh, V.-V. Toward sustainable microgrids with blockchain technology-based peer-to-peer energy trading mechanism: A fuzzy meta-heuristic approach. *Renew. Sustain. Energy Rev.* **2020**, *136*, 110452. [CrossRef]
85. Wang, X.; Liu, P.; Ji, Z. Trading platform for cooperation and sharing based on blockchain within multi-agent energy internet. *Glob. Energy Interconnect.* **2021**, *4*, 384–393. [CrossRef]

86. Li, Q.; Li, A.; Wang, T.; Cai, Y. Interconnected hybrid AC-DC microgrids security enhancement using blockchain technology considering uncertainty. *Int. J. Electr. Power Energy Syst.* **2021**, *133*, 107324. [CrossRef]
87. Mahesh, G.S.; Babu, G.D.; Rakesh, V.; Mohan, S.; Ranjit, P. Energy management with blockchain technology in DC microgrids. *Mater. Today Proc.* **2021**, *47*, 2232–2236. [CrossRef]
88. Wang, S.; Xu, Z.; Ha, J. Secure and decentralized framework for energy management of hybrid AC/DC microgrids using blockchain for randomized data. *Sustain. Cities Soc.* **2021**, *76*, 103419. [CrossRef]
89. Fineberg, S.J.; Nandyala, S.V.; Marquez-Lara, A.; Oglesby, M.; Patel, A.A.; Singh, K. Incidence and risk factors for postoperative delirium after lumbar spine surgery (Phila Pa 1976). *Spine* **2013**, *38*, 1790–1796. [CrossRef]
90. Wang, T.; Hua, H.; Wei, Z.; Cao, J. Challenges of blockchain in new generation energy systems and future outlooks. *Int. J. Electr. Power Energy Syst.* **2021**, *135*, 107499. [CrossRef]
91. Ahl, A.; Yarime, M.; Goto, M.; Chopra, S.S.; Kumar, N.M.; Tanaka, K.; Sagawa, D. Exploring blockchain for the energy transition: Opportunities and challenges based on a case study in Japan. *Renew. Sustain. Energy Rev.* **2019**, *117*, 109488. [CrossRef]
92. Perez-DeLaMora, D.; Quiroz-Ibarra, J.E.; Fernandez-Anaya, G.; Hernandez-Martinez, E. Roadmap on community-based microgrids deployment: An extensive review. *Energy Rep.* **2021**, *7*, 2883–2898. [CrossRef]
93. Enescu, F.M.; Bizon, N.; Ionescu, V.M. Blockchain—A new tehnology for the smart village. In Proceedings of the 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 1–3 July 2021; pp. 1–6. [CrossRef]
94. Enescu, F.M.; Bizon, N.; Cirstea, A.; Stirbu, C. Blockchain Technology Applied in Health the Study of Blockchain Application in the Health System (I). In Proceedings of the 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018; pp. 1–4. [CrossRef]
95. Cirstea, A.; Enescu, F.M.; Bizon, N.; Stirbu, C.; Ionescu, V.M. Blockchain Technology Applied in Health the Study of Blockchain Application in the Health System (II). In Proceedings of the 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018; pp. 1–4. [CrossRef]
96. Gul, M.J.; Subramanian, B.; Paul, A.; Kim, J. Blockchain for public health care in smart society. *Microprocess. Microsyst.* **2020**, *80*, 103524. [CrossRef]
97. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.D.; He, J. BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Italy, 18–20 June 2018; pp. 49–56. [CrossRef]
98. Enescu, F.M.; Bizon, N.; Onu, A.; Răboacă, M.S.; Thounthong, P.; Mazare, A.G.; Șerban, G. Implementing Blockchain Technology in Irrigation Systems That Integrate Photovoltaic Energy Generation Systems. *Sustainability* **2020**, *12*, 1540. [CrossRef]
99. Raboaca, M.S.; Bizon, N.; Trufin, C.; Enescu, F.M. Efficient and Secure Strategy for Energy Systems of Interconnected Farmers' Associations to Meet Variable Energy Demand. *Mathematics* **2020**, *8*, 2182. [CrossRef]
100. Enescu, F.M.; Bizon, N.; Ionescu, V.M. Use of Blockchain Technology in Irrigation Systems of small farmers' association. In Proceedings of the 2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 27–29 June 2019; pp. 1–6. [CrossRef]
101. Sharma, P.K.; Park, J.H. Blockchain based hybrid network architecture for the smart city. *Futur. Gener. Comput. Syst.* **2018**, *86*, 650–655. [CrossRef]
102. Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* **2020**, *61*, 102360. [CrossRef]
103. Mora, H.; Mendoza-Tello, J.C.; Varela-Guzmán, E.G.; Szymanski, J. Blockchain technologies to address smart city and society challenges. *Comput. Hum. Behav.* **2021**, *122*, 106854. [CrossRef]
104. Wu, H.; Cao, J.; Yang, Y.; Tung, C.L.; Jiang, S.; Tang, B.; Liu, Y.; Wang, X.; Deng, Y. Data Management in Supply Chain Using Blockchain: Challenges and a Case Study. In Proceedings of the 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 29 July–1 August 2019; pp. 1–8. [CrossRef]
105. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.-K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *144*, 13–48. [CrossRef]
106. Al Sadawi, A.; Madani, B.; Saboor, S.; Ndiaye, M.; Abu-Lebdeh, G. A comprehensive hierarchical blockchain system for carbon emission trading utilizing blockchain of things and smart contract. *Technol. Forecast. Soc. Chang.* **2021**, *173*, 121124. [CrossRef]
107. Zia, M. B-DRIVE: A blockchain based distributed IOT network for smart urban transportation. *Blockchain Res. Appl.* **2021**, *2*, 100033. [CrossRef]
108. Pournaras, E. Proof of witness presence: Blockchain consensus for augmented democracy in smart cities. *J. Parallel Distrib. Comput.* **2020**, *145*, 160–175. [CrossRef]
109. Paul, R.; Ghosh, N.; Sau, S.; Chakrabarti, A.; Mohapatra, P. Blockchain based secure smart city architecture using low resource IoTs. *Comput. Netw.* **2021**, *196*, 108234. [CrossRef]
110. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-Based Packing of Industrial IoT Data in Permissioned Blockchains. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7639–7649. [CrossRef]
111. Hu, W.; Li, H. A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things. *Alex. Eng. J.* **2020**, *60*, 491–500. [CrossRef]

112. Yang, J.; Paudel, A.; Gooi, H.B.; Nguyen, H.D. A Proof-of-Stake public blockchain based pricing scheme for peer-to-peer energy trading. *Appl. Energy* **2021**, *298*, 117154. [CrossRef]
113. Nair, R.; Gupta, S.; Soni, M.; Shukla, P.K.; Dhiman, G. An approach to minimize the energy consumption during blockchain transaction. *Mater. Today Proc.* **2020**. [CrossRef]
114. Zhang, Y.; Shi, Q. An intelligent transaction model for energy blockchain based on diversity of subjects. *Alex. Eng. J.* **2020**, *60*, 749–756. [CrossRef]
115. Gourisetti, S.N.G.; Sebastian-Cardenas, D.J.; Bhattarai, B.; Wang, P.; Widergren, S.; Borkum, M.; Randall, A. Blockchain smart contract reference framework and program logic architecture for transactive energy systems. *Appl. Energy* **2021**, *304*, 117860. [CrossRef]
116. Yang, Q.; Wang, H.; Wang, T.; Zhang, S.; Wu, X.; Wang, H. Blockchain-based decentralized energy management platform for residential distributed energy resources in a virtual power plant. *Appl. Energy* **2021**, *294*, 117026. [CrossRef]
117. Wongthongtham, P.; Marrable, D.; Abu-Salih, B.; Liu, X.; Morrison, G. Blockchain-enabled Peer-to-Peer energy trading. *Comput. Electr. Eng.* **2021**, *94*, 107299. [CrossRef]
118. Wang, L.; Ma, Y.; Zhu, L.; Wang, X.; Cong, H.; Shi, T. Design of integrated energy market cloud service platform based on blockchain smart contract. *Int. J. Electr. Power Energy Syst.* **2021**, *135*, 107515. [CrossRef]
119. Choobineh, M.; Arab, A.; Khodaei, A.; Paaso, A. Energy innovations through blockchain: Challenges, opportunities, and the road ahead. *Electr. J.* **2021**, *35*, 107059. [CrossRef]
120. Mathew, R.; Mehbodniya, A.; Ambalgi, A.P.; Murali, M.; Sahay, K.B.; Babu, D.V. RETRACTED: In a virtual power plant, a blockchain-based decentralized power management solution for home distributed generation. *Sustain. Energy Technol. Assess.* **2021**, *49*, 101731. [CrossRef]
121. Zhang, C.; Yang, T.; Wang, Y. Peer-to-Peer energy trading in a microgrid based on iterative double auction and blockchain. *Sustain. Energy Grids Netw.* **2021**, *27*, 100524. [CrossRef]
122. Xie, Y.-S.; Lee, Y.; Chang, X.-Q.; Yin, X.; Zheng, H. Research on the transaction mode and mechanism of grid-side shared energy storage market based on blockchain. *Energy Rep.* **2021**, *8*, 224–229. [CrossRef]
123. Rafique, Z.; Khalid, H.M.; Muyeen, S.M. Communication Systems in Distributed Generation: A Bibliographical Review and Frameworks. *IEEE Access* **2020**, *8*, 207226–207239. [CrossRef]
124. Jha, A.V.; Appasani, B.; Ghazali, A.N. A Comprehensive Framework for the Assessment of Synchrophasor Communication Networks from the Perspective of Situational Awareness in a Smart Grid Cyber Physical System. *Technol. Econ. Smart Grids Sustain. Energy* **2022**, *7*, 20. [CrossRef]
125. Musleh, A.S.; Chen, G.; Dong, Z.Y. A Survey on the Detection Algorithms for False Data Injection Attacks in Smart Grids. *IEEE Trans. Smart Grid* **2019**, *11*, 2218–2234. [CrossRef]
126. Mahmoud, M.S.; Khalid, H.M.; Hamdan, M.M. *Cyberphysical Infrastructures in Power Systems: Architectures and Vulnerabilities*; Elsevier: Amsterdam, The Netherlands, 2021. [CrossRef]
127. Alkhiari, A.M.; Mishra, S.; AlShehri, M. Blockchain-Based SQKD and IDS in Edge Enabled Smart Grid Network. *Comput. Mater. Contin.* **2022**, *70*, 2149–2169. [CrossRef]
128. Chen, J.; Mohamed, M.A.; Dampage, U.; Rezaei, M.; Salmen, S.H.; Al Obaid, S.; Annuk, A. A Multi-Layer Security Scheme for Mitigating Smart Grid Vulnerability against Faults and Cyber-Attacks. *Appl. Sci.* **2021**, *11*, 9972. [CrossRef]
129. Khan, A.A.; Laghari, A.A.; Liu, D.-S.; Shaikh, A.A.; Ma, D.-D.; Wang, C.-Y.; Wagan, A.A. EPS-Ledger: Blockchain Hyperledger Sawtooth-Enabled Distributed Power Systems Chain of Operation and Control Node Privacy and Security. *Electronics* **2021**, *10*, 2395. [CrossRef]
130. Xu, W.; Li, J.; Dehghani, M.; GhasemiGarpachi, M. Blockchain-based secure energy policy and management of renewable-based smart microgrids. *Sustain. Cities Soc.* **2021**, *72*, 103010. [CrossRef]
131. Vasukidevi, G.; Sethukarasi, T. BBSSE: Blockchain-Based Safe Storage, Secure Sharing and Energy Scheme for Smart Grid Network. In *Wireless Personal Communications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1–12. [CrossRef]