Blockchain-Enabled Smart Grid Applications

Subjects: Engineering, Electrical & Electronic

Contributor: Bhargav Appasani, Sunil Kumar Mishra, Amitkumar V. Jha, Santosh Kumar Mishra, Florentina Magda Enescu, Ioan Sorin Sorlei, Fernando Georgel Bîrleanu, Noureddine Takorabet, Phatiphat Thounthong, Nicu Bizon

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.

Keywords: smart grid ; blockchain ; smart contracts ; cybersecurity ; microgrids ; electric vehicles

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].

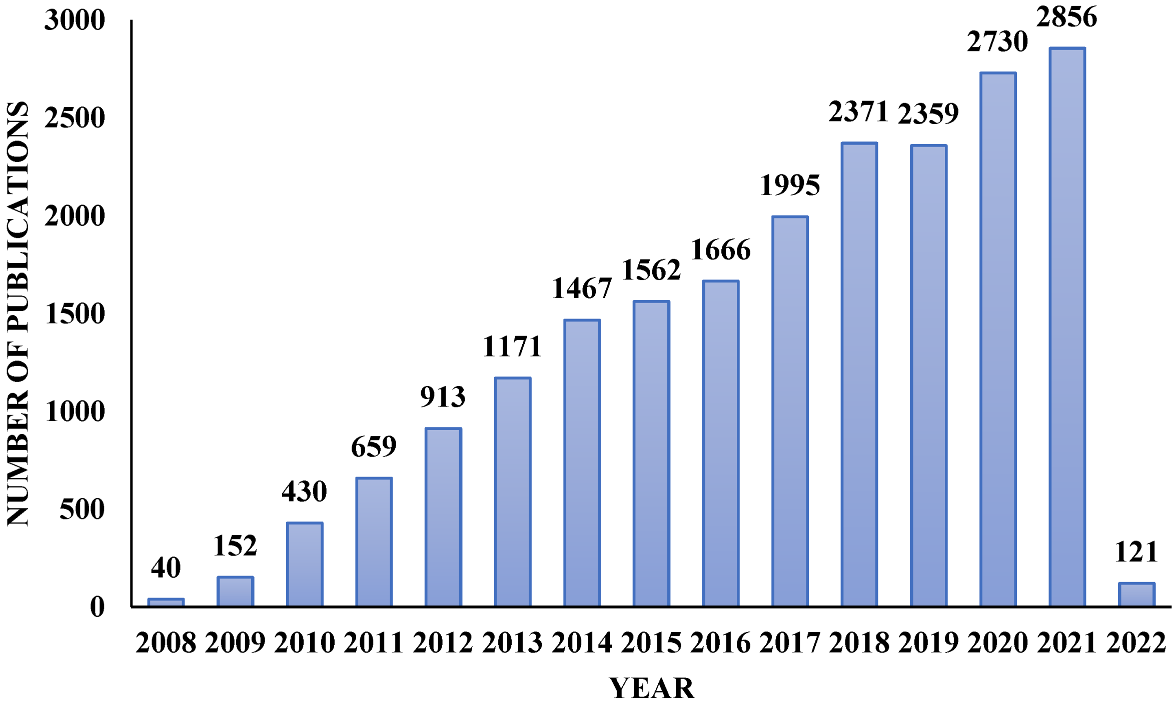

Figure 1. Publication statistics on SG.

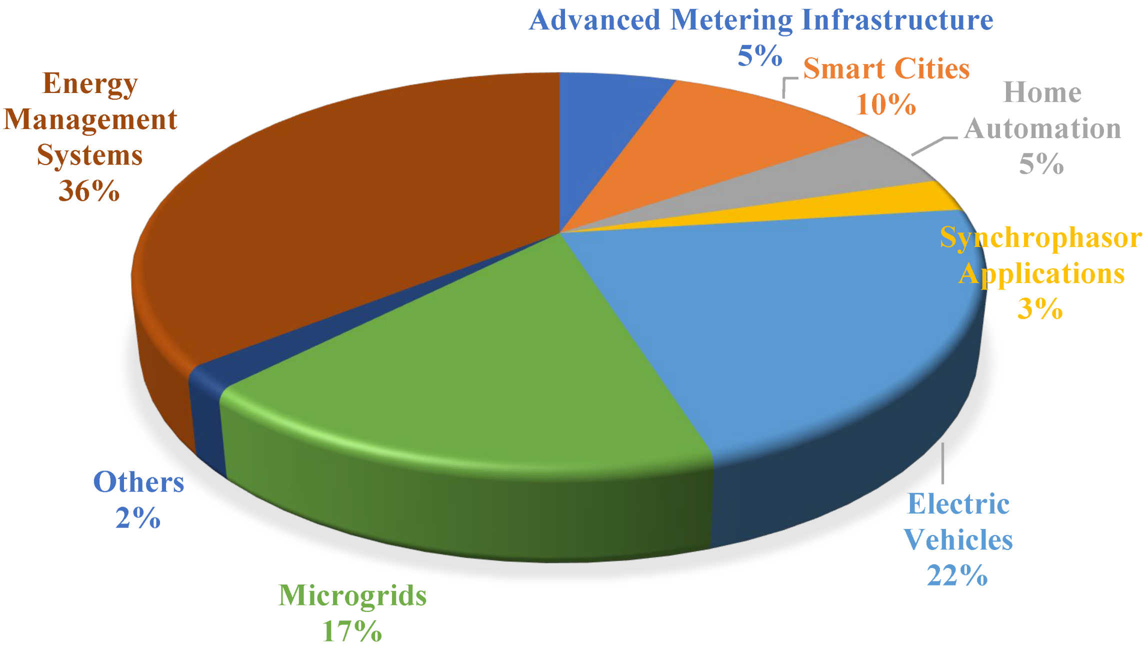

Figure 2. Distribution of research related to SG.

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.

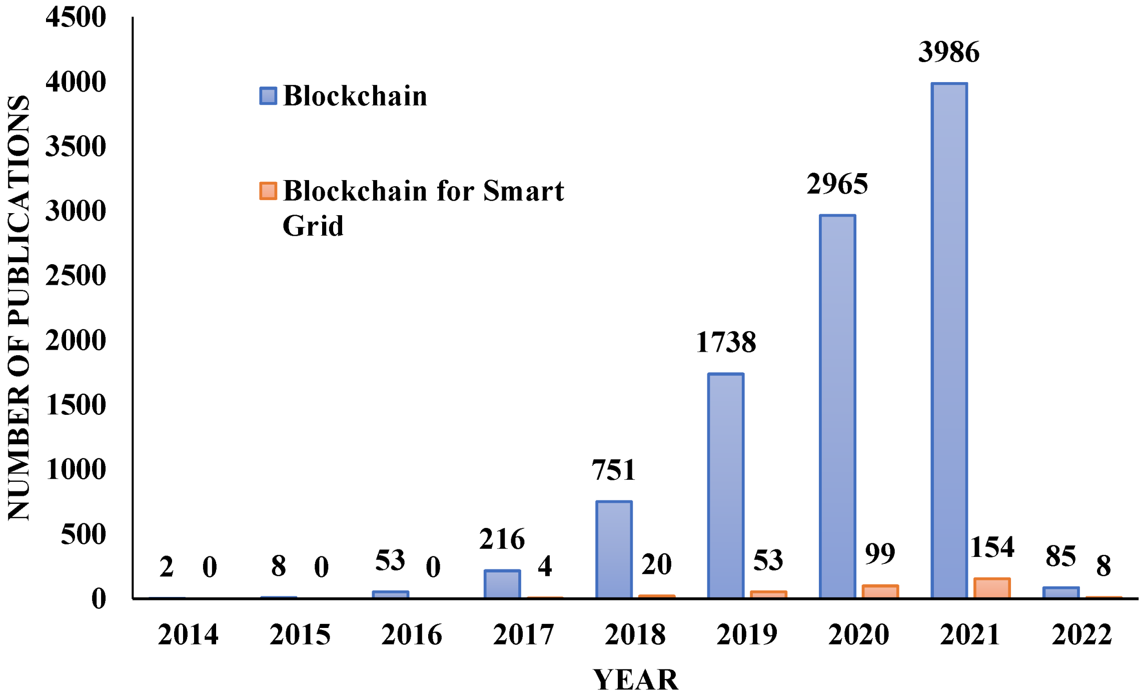

Figure 3. Publication statistics on blockchain and blockchain for SG.

2. Blockchain

2.1. Structure of Blockchain

The blockchain comprises a series of blocks of transactions linked together in a chain. 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 [5]. 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.

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 [6]. 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 [7]. These three types of blockchains are represented along with their properties in **Figure 4**.

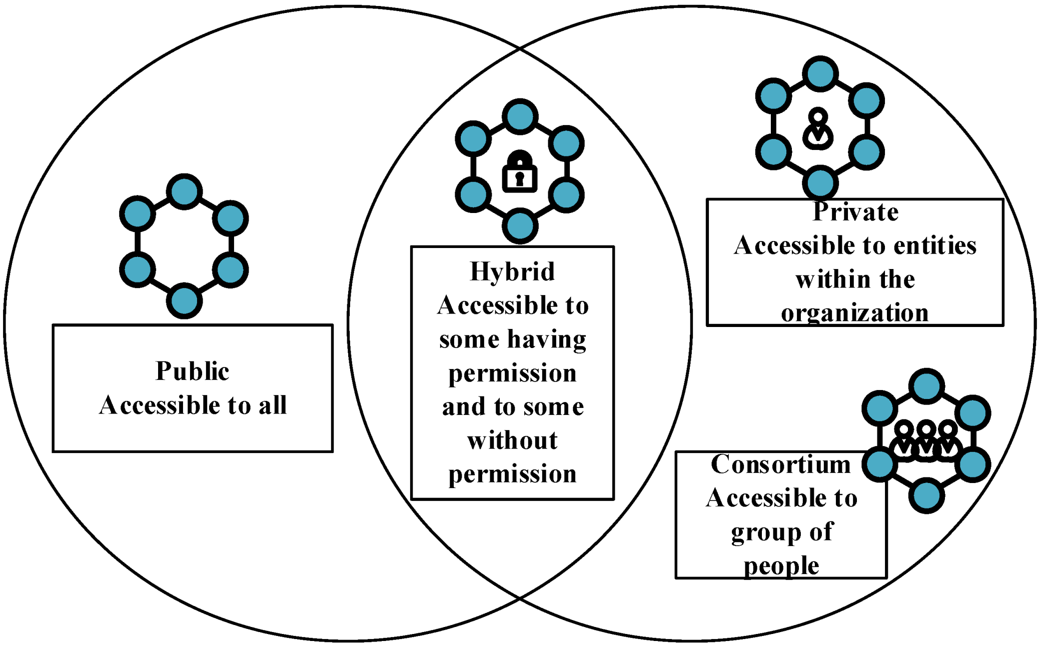
Public
Accessible to all
Hybrid
Accessible to some having permission and to some without permission
Private
Accessible to entities within the organization
Consortium
Accessible to group of people

Figure 4. 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 [8]. 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 5**.

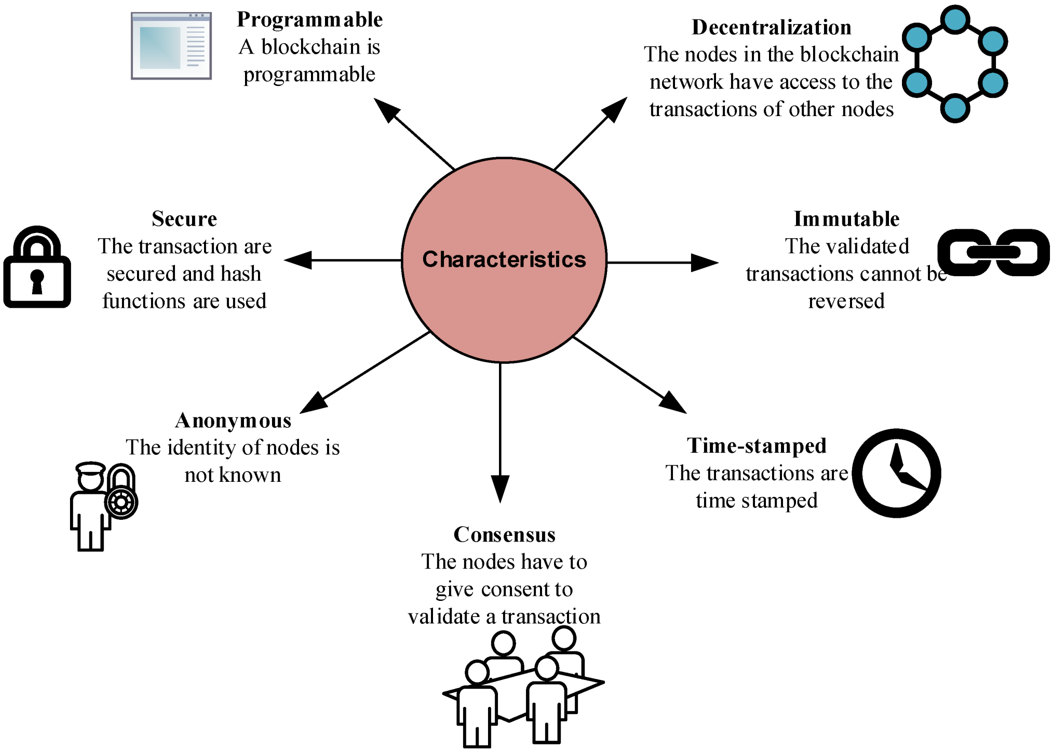
Programmable
A blockchain is programmable
Decentralization
The nodes in the blockchain network have access to the transactions of other nodes
Secure
The transaction are secured and hash functions are used
Characteristics
Immutable
The validated transactions cannot be reversed
Anonymous
The identity of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

Figure 5. 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

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 [9][10]. 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 [11]. The fundamental architecture of the synchrophasor measurement system involves a phasor measurement unit (PMU), phasor data concentrator (PDC), and the communication network [12]. 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 [13]. 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.

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. [14]. 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 [15], 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.

3.2. 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 [16]. 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.

3.3. 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 6**.

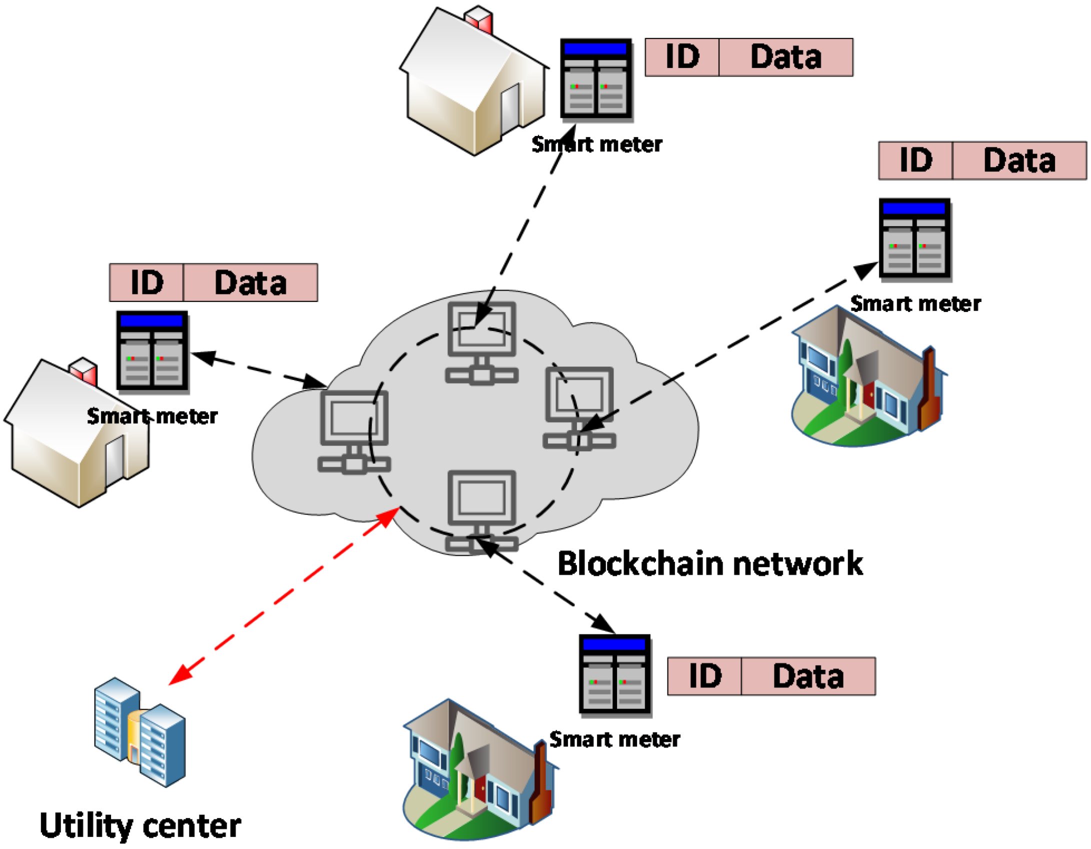

Figure 6. The architecture of blockchain for AMI.

The smart meters can be directly connected to the blockchain network through the gateway [17]. 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.

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) [18]. In the future, the importance of EVs using technologies such as the Internet of Vehicles (IoV) [19] or the Internet of Things (IoT) [20] 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 [21], 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 [22]. 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 [23]. 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 [24]. 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 [25].

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.

3.6. 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.

3.7. 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.

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 [26]. 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. [27]. 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.

The SG is a typical cyber-physical system [28]. 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.

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 7**.

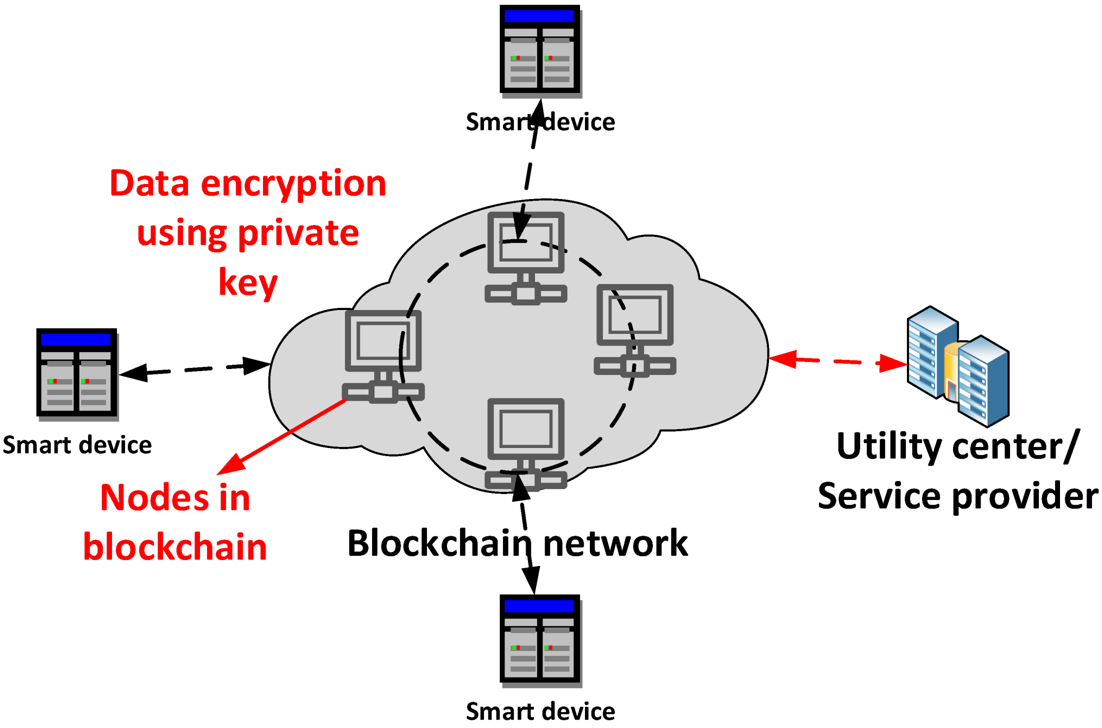

Figure 7. The architecture of SG cybersecurity using blockchain.

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.

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.

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.
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.
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.
5. 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.
6. 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.
7. 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.
8. 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.
9. Appasani, B.; Mohanta, D.K. A review on synchrophasor communication system: Communication technologies, standards and applications. Prot. Control Mod. Power Syst. 2018, 3, 37.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.

23. 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.
24. 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.
25. 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.
26. Rafique, Z.; Khalid, H.M.; Muyeen, S.M. Communication Systems in Distributed Generation: A Bibliographical Review and Frameworks. IEEE Access 2020, 8, 207226–207239.
27. 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.
28. Mahmoud, M.S.; Khalid, H.M.; Hamdan, M.M. Cyberphysical Infrastructures in Power Systems: Architectures and Vulnerabilities; Elsevier: Amsterdam, The Netherlands, 2021.

Retrieved from https://encyclopedia.pub/entry/history/show/67576