energies

MDPI

Article

Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges

Muhammad Waseem [1,2,†], Muhammad Adnan Khan [1,†], Arman Goudarzi [3,†], Shah Fahad [4,†], Intisar Ali Sajjad [1,†] and Pierluigi Siano [5,6,*,†]

1 Department of Electrical Engineering, University of Engineering and Technology, Taxila 47050, Pakistan
2 School of Electrical Engineering, Zhejiang University, Hangzhou 310027, China
3 Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8P 5C2, Canada
4 Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409, USA
5 Department of Management & Innovation Systems, University of Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano, Italy
6 Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg 2006, South Africa
* Correspondence: psiano@unisa.it
† These authors contributed equally to this work.

Abstract: Smart grid integrates computer, communication, and sensing technologies into existing power grid networks to achieve significant informatization-related advantages. It will provide communication between neighbors, localized management, bidirectional power transfer, and effective demand response. Smart grids (SG) replace conventional grids by integrating various operational measures, including smart automation appliances, smart meters, and renewable energy sources. Regarding energy management and resolving energy issues, SG is one of the most cutting-edge and potentially game-changing innovations. Even still, its complexity suggests that decentralization may provide significant gains. Because of its increasing digitization and interconnectedness, it is also vulnerable to cyber threats. Blockchain, in this sense, is a potential SG paradigm solution that provides several great benefits. Even though blockchains have been widely discussed to decentralize and strengthen smart grid cybersecurity, they have not yet been researched in depth from an application and architectural standpoint. Blockchain-enabled SG applications are the subject of an in-depth research investigation. Electric vehicles (EVs), home automation, energy management systems, etc., are only a few of the many examples that have prompted the proposal of blockchain designs for their respective use cases. Information communication network security is of paramount importance. However, this evolving system raises cybersecurity issues. This paper aims to guide researchers in the right manner so they may build blockchain-based, secure, distributed SG applications in the future. This article also summarizes cybersecurity threats pertaining to smart grids. It starts with a description of a blockchain followed by the blockchain infrastructure, challenges, and solutions for different smart grid applications. A look back at the tried-and-true methods of securing a power grid is offered, and then it discusses the newer and more complex cybersecurity threats to the smart grid. In addition, models of common cyberattacks are presented, and the methods of defense against them are examined.

Keywords: smart grid; blockchain; cybersecurity; home automation; energy management; electric vehicles; cyberattacks; denial-of-service (DoS) attack

Citation: Waseem, M.; Adnan Khan, M.; Goudarzi, A.; Fahad, S.; Sajjad, I.A.; Siano, P. Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies* **2023**, *16*, 820. https://doi.org/10.3390/en16020820

Academic Editors: Carlo Roselli, Elisa Marrasso and Francesca Ceglia

Received: 5 December 2022
Revised: 7 January 2023
Accepted: 9 January 2023
Published: 11 January 2023

1. Introduction

For over a century, electricity has been transmitted from generation to customer end using a one-directional conventional grid system. However, as human civilization progresses rapidly, more fossil fuel-powered power plants are used, resulting in higher

greenhouse gas emission. Consequently, the electricity grid has become a very complicated system. Cascade failures are also more likely to occur in this new setting. Several major blackouts have occurred throughout the globe in the last decade. A smart grid is a future-oriented electrical network supporting renewable power sources, smart distribution, and dynamic load shedding. These characteristics also help prevent cascade failures. A great deal of data about the grid's markets, service providers, and operations must be controlled. In other words, as seen in Figure 1, a smart grid is a highly decentralized and structured communication network to transport and analyze the data gathered. As has just been discussed, wireline and wireless connectivity technologies are used in tandem in a smart grid to facilitate power transfer and management. The purpose of a SCADA system is to keep tabs on the status of a power grid at both the transmission and distribution levels. Instead, data are sent across the network through a number of utility gateways.

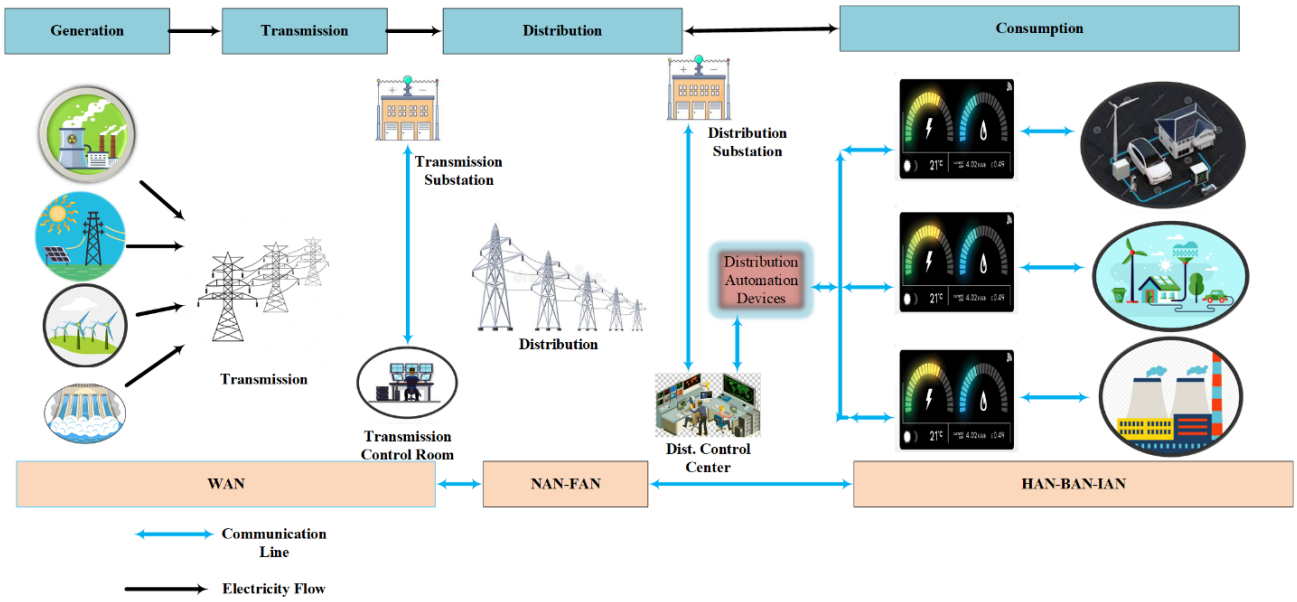

Figure 1. Smart Grid Infrastructure from Generation to Consumer end.

Given the rise in popularity of alternative energy sources, faster signal processors, smarter sensors, etc., the power grid is experiencing rapid evolution. The current need calls for a two-way exchange of data and energy between power producers and consumers [1]. As a result, the conventional power grid is transitioning into a smart grid (SG), a system that can dynamically monitor and manage electricity flow, giving customers stable power [2]. Smart grid integrates computer, communication, and sensing technologies into existing power grid networks to achieve these significant informatization-related advantages. Energy management systems (EMS), electric vehicles (EVs), microgrids (MGs), smart cities (SCs), home automation (HA), and advanced metering infrastructure (AMI) are some of the most prominent examples of SG applications [2].

SG improves power supply dependability and makes various complex and difficult applications a reality [3]. Multiple entities in the grid conduct transactions at any time in this intricate network. Verifying the legality of the business dealings between the parties to a specific SG application is a major issue. Blockchain technology offers a safe and promising answer to this issue. Satoshi Nakamoto's invention of blockchain technology facilitates agreement on the legitimacy of a transaction and keeps everyone involved honest [4,5].

Figure 2 displays the annual number of articles covering blockchain research. In addition, the chart displays the comparable number of articles written on blockchain for SG. Scopus was used to compile the tally of published works. According to the data, blockchain technology is not being used in SG settings at present. Just a small percentage (3.5%) of blockchain articles are really about SG applications. This study aims to analyze the existing

literature on blockchain for SG, classify it according to its intended use, provide blockchain design architecture for different SG uses, pinpoint relevant obstacles, and propose workable solutions. A survey of some review papers related to smart grid application is summarized in Table 1.

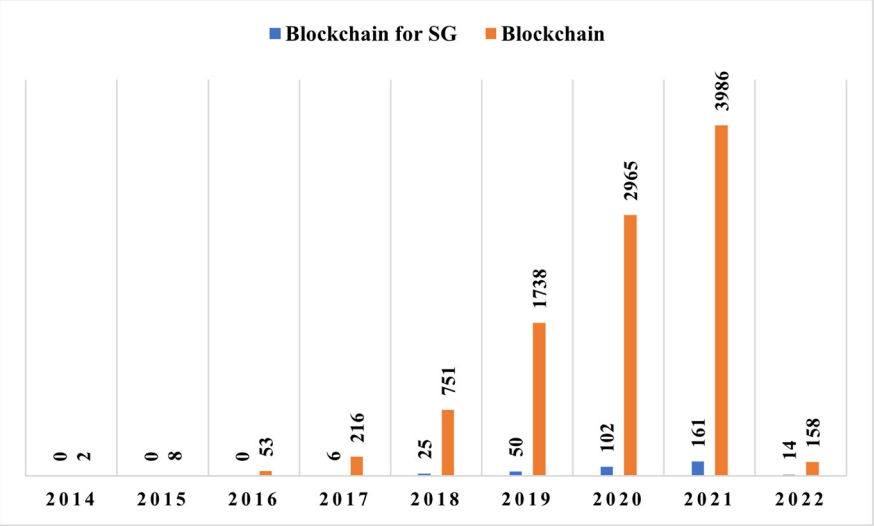

Figure 2. Number of articles on blockchain and blockchain in smart grids.

Table 1. A summarized survey of some review papers related to smart grid application.

Applications	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]	[19]	This Study
HA	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
EVs	✓	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓
Smart Cities	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
AMI	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
MGs	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓
EMs	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓

In contrast to the other research works, this paper focuses on the specific application of blockchain technology to the SG domain in a more holistic approach. In addition, the current paper outlines the framework for SG applications that make use of blockchain technology. Electric vehicles, advanced metering infrastructure, microgrids, and home automation are just a few of the many scenarios where SG might be useful. Different threats to smart grid privacy and security are also discussed, along with counterattack measures.

The paper is broken up into the following parts. The fundamentals of a blockchain are covered in Section 2, covering various terms and concepts associated with blockchain technology. Applications in the SG space that make use of blockchain technology are discussed in Section 3 along with the architectures of several applications, and their challenges and solutions are explained. Section 4 addresses cybersecurity and cyberattacks in smart grids along with counterattack measures, while Section 5 describes the role of blockchain in smart grids and Section 6 wraps up our analysis.

2. Overview of Blockchain

Blockchain technology has gained much interest in recent years. Blockchain was first defined as a cryptocurrency [20] when it was first developed for digital money use. Blockchain was once thought to be Bitcoin, the most widely used cryptocurrency. However, blockchain is what really makes these digital currencies tick. It is a decentralized transaction ledger that several parties may use. Researchers initially had the least interest in this

technology, but Bitcoin's success ultimately swayed them. There was a sharp increase in the number of blockchain applications and usage in different technological areas after 2016. Financial services, medical care, manufacturing, and other sectors are among those which have implemented blockchain more deeply.

Blockchain is a chain of blocks of transactions recorded in series in which various administrators oversee the operation of classic client/server systems. Blockchain is a P2P network [21] in which all users have equal control over the network's direction and operation. Many computers, or nodes, are linked together to form this network, and the blocks in the chain cannot be altered without the network's consent. A record of the centralized database is stored locally on each node in the network [22]. The specifics of a given use case will determine the type of blockchain used. Public blockchains, private blockchains, and consortium blockchains are the three main categories of blockchain [23]. Three types of blockchains exist: public, private, and consortium. In a public or permissionless blockchain, no one may exert authority. Users are not restricted in their ability to read or write to the network. On the other side, private or permissioned ledgers are inaccessible to anybody who is not logged into the network as an authorized user.

The blocks are unreadable because they are protected with an encryption key. Consortium blockchains include both the public and private blockchain models. In contrast to centralized systems, the nodes in a blockchain network verify transactions among themselves in a decentralized manner [24]. Once a transaction has been verified by the nodes and uploaded to the blockchain, there is no way to undo it since the identification of the network nodes stays unanimous. So, the data stored on the blockchain cannot be altered [25].

While blockchain technology has shown promise for building a better infrastructure of the future Internet, there are still a number of issues that need to be resolved. Due to the immaturity of blockchain's development, having access to knowledgeable individuals is essential. Businesses are understandably concerned about the hefty upfront infrastructure costs associated with BCT adoption, despite the many promising applications of this technology. Privacy and security considerations also play a role in the spread of blockchain technology. Legal considerations and difficulty scaling it up are also major concerns [26].

Terminologies and Components of Blockchain

Below are some definitions of terms used to define the critical parts of a blockchain:

Block: Pointers and linked lists are used to represent blocks in a blockchain. Blocks are organized into a sensible hierarchy and aligned with one another using a linked list. A block is a collection of data that is created by a secure hash algorithm and contains details about a transaction, such as timestamps and references to previous blocks. Pointers show where the next block is located. The block header and the block body are the two parts of every block [27]. Below are the fields that make up the block header [28]:

i. Block version: it defines the criteria for validating blocks.
ii. Merkle tree root hash: the total hash value of all transactions in the frame is calculated using this hashing algorithm.
iii. Timestamp: it is represented in seconds in universal time, as of 1 January 1970.
iv. n-Bits: the target size of a block hash.
v. Nonce: it refers to a 4-byte field that begins at 0 and increases by 1 with each hash calculation.
vi. Parent block hash: the 256-bit hash value of the previous block is often known as the parent block hash.

Public and private keys: Blockchain is a system of interconnected, cryptographically secured blocks that is always growing [29]. Blockchain uses an asymmetric key mechanism to verify transactional authentication. A private key is used to encrypt a block's transactions. These transactions are accessible to any node in the network. When using a public key that is accessible to all nodes in the network, these nodes can decrypt the data.

Hash function: Every block contains a cryptographic hash that is connected to the preceding block. To specify a piece of data, hashing generates a fixed-length string. The string's length is irrespective of the data's size.

Consensus procedure: A set of standards and agreement from all network users are used to validate new blocks. To decide whether or not a block is valid, consensus is required. For the consensus procedure, a number of methods are available, including realistic byzantine fault tolerance, proof of work, and proof of stake.

Smart contracts: In a blockchain network, smart contracts are computer programs that run automatically and regulate the transactions between dispersed nodes.

3. Operation Blockchain for Smart Grids Applications

By fostering more trust and promoting greater decentralization, blockchain technology has the potential to alter existing applications drastically. However, the benefits it offers are not being fully used by SG applications despite its increasing expansion [30]. The total publications written about blockchain from the standpoint of different SG applications are 41% about energy management systems, 19% on microgrids, 24% on electric vehicles, 14% on home automation, and 2% on AMI. Scopus was used to compile these numbers, and only journal papers were examined. In a SG, blockchain is extensively used for energy management purposes. The application of blockchain technology has also expanded to include electric vehicles, advanced metering infrastructure, microgrids, home automation, and smart cities [31].

3.1. Blockchain for Home Automation

The resistance and RMS value of a current describe the conduction losses. The output is a smart home that is an IoT-integrated residence that improves the quality of life in many ways, including safety, healthcare, pleasure, and convenience. Technology for the home has improved the quality of life and allowed more people to live independently. Consumers and IT companies are interested in smart homes because of their valuable features, such as behavior tracking and safety assessments. Smart homes have many advantages for homeowners and others but are also susceptible to malicious cyberattacks that put consumers in danger [32]. Although there are existing methods for countering these threats, they are highly centralized and vulnerable to widespread assault. Because of this, the cutting-edge sector of automated smart home applications and facilities lacks the flexibility and scalability required for productive use. Several advanced technologies simplify people's daily routines. These kinds of applications may produce massive amounts of data. There are security concerns associated with storing this dynamic content in archives. Blockchain has been shown to be a reliable and effective tool in the field of remote connection and data transfer in cybersecurity. As a result, it is being used for home automation [33].

Blockchain-based HA infrastructure refers to the use of several electronic gadgets (smart TVs, lighting, etc.), either working autonomously or in concert with one another to monitor the various settings of smart homes. To realize the potential of HA, these intelligent gadgets must be able to communicate with one another. An IoT gateway solves the problems that arise when several smart devices need to communicate with one another [34]. To prevent a security breach, such as to prevent users in one house from accessing the electronics devices in another house, the service provider is responsible for making control suggestions to the users' smart devices on the basis of smart intelligent algorithms. Service providers may employ machine learning algorithms to provide more accurate suggestions and forecasts. Connecting consumers and service providers over a blockchain network improves HA security [35]. Possibly Ethereum or Hyperledger will be used to create the blockchain. A blockchain's overarching design for HA is shown in Figure 3.

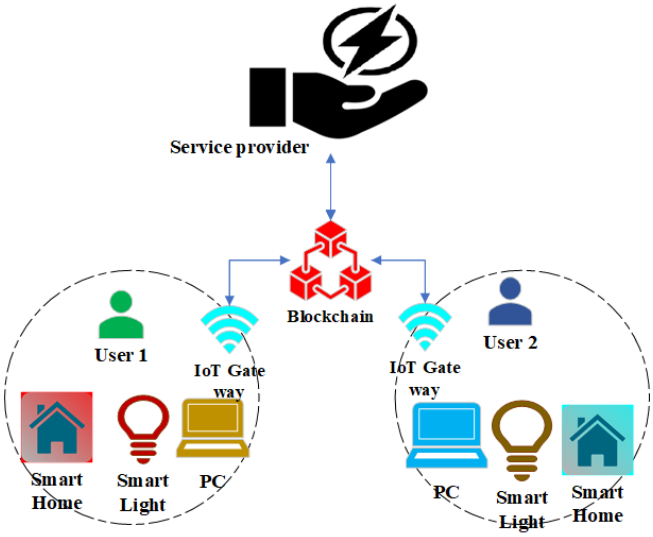

Figure 3. Blockchain's overarching design for HA.

Residents may only interact with the features of their own smart home devices and cannot interact with the smart devices in the neighborhood's smart homes. All household gadgets may connect directly to the blockchain system through the gateway. Blocks containing device data may be linked using the blockchain's hashing algorithm. The service provider can provide data analysis and user-friendly recommendations, but it cannot have access to a smart home's actual gadgets themselves. Through the gateway, all of the gadgets in a house may communicate with the blockchain network.

Challenges and Solutions: Many different blockchain technologies are being put to use in HA-related projects right now [36]. Each system's data are stored in a unique format, making integration difficult. Furthermore, these networks utilize various consensus techniques. Interoperability across different blockchain platforms will only be possible if they are standardized. A further difficulty in using blockchain for HA applications is performing real-time analytics on streaming data. They need to be analyzed and evaluated in real time. For instance, real-time face detection is essential in an intrusion detection system. For real-time applications, processing blockchains might be difficult. Using a minimal framework might be the answer to this problem.

3.2. Blockchain for Advanced Metering Infrastructure

Every consumer's energy usage data are collected, monitored, and sent through a smart meter; this meter is the brain of an AMI system. Many various groups have their own purposes for these meter data. The utility grid may use this information for demand forecasting and scheduling, while the distributor can utilize the information from smart meters to implement pricing structure and invoicing. On the other side, users may use this information for energy management purposes [37]. Despite the many benefits of AMI, transferring data across devices safely is difficult. A key component in reaching this goal is the blockchain-based AMI. Figure 4 presents a general approach for integrating blockchain technology into AMI.

The gateway enables direct connection of the smart meters to the blockchain network [38]. In accordance with the IEC 62056 procedure, the meter readings will include meter identifiers and other data pertinent to the provision of utility services. The data from the AMI are sent to the meters, which are linked to the servers or nodes inside the blockchain network. All other nodes within the blockchain-enabled network are subsequently given access to these blocks. This network must be a private blockchain network accessible only by nodes affiliated with the utility hub. Without sacrificing privacy or security, smart contracts and validations on a private blockchain may reveal inefficiencies in energy use.

Challenges and Solutions: Despite the obvious benefits, blockchain technology has not been extensively used for this SG use case. Scientists have implemented it to improve the safety of AMI software. A lightweight blockchain-based infrastructure was presented in [39] for improving AMI security. This framework had a low energy footprint and was resistant to hacking attempts. Reference [40] demonstrates how blockchain may protect AMI users' private data. The same lack of interoperability and slowness in real time plagues the AMI blockchain, which also affects HA applications.

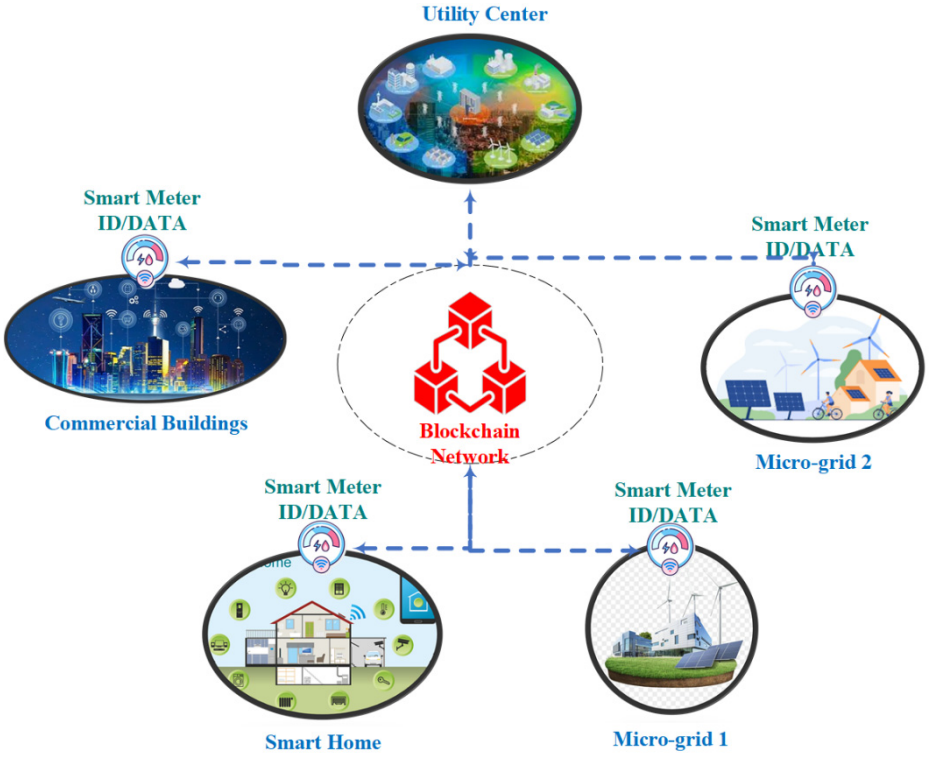

Figure 4. A general approach for integrating blockchain into AMI.

3.3. Blockchain for Electric Vehicles

New connectivity structures—vehicle-to-grid interfaces—have emerged as a result of the fast development of smart grid and the increasing sophistication of electric vehicles (EVs) (V2G) [41]. Logistics businesses, for instance, already provide permanent charging stations (CSs) for their fleet of cars, and this trend is only expected to grow as technologies, such as the Internet of Vehicles (IoV) [42] or the Internet of Things (IoT) [43], become more widely used. Vehicle-to-everything (V2X) technology [44] was developed in response to the need for interoperability between vehicles and other technological systems in the real world. V2X systems consist of integrated vehicle sensor platforms that centralize different functionalities on a single EV server [45]. V2X performance metrics are derived from a data set, including details on the shared multi-networked data and an electric car's technical prowess. 5G networks have emerged and spread rapidly over the globe because of their security, speed of data transmission between linked cars, and global coverage of telecommunication systems [46]. Multi-networked communication systems enabled by 5G technology have the processing capability to run applications at a higher level. A V2X protocol is driven by a 5G network, which in turn encourages the development and integration of blockchain applications [47]. Including blockchain technology in the vehicle-to-everything protocol has the potential to revolutionize intelligent transportation systems, improving both the effectiveness and efficiency of transportation and road safety [48].

Figure 5 depicts the overarching blockchain architecture of EV applications. The infrastructure for electric vehicles based on the blockchain needs frequent nodes to record the behavior of moving vehicles. These nodes are the backbone of the blockchain, validating

blocks and executing smart contracts. These stationary blockchain nodes or access points are where the data from the mobile EVs are sent. Wi-Fi links the many nodes and mobile electric vehicles where every EV has its unique ID number. Information, including battery life, vehicle condition, charging costs, etc., is sent from an EV to its charging station through an access point. The nodes add these data in the form of blocks to the distributed ledger where different blockchain nodes verify the transaction. The transportation authorities may utilize the blockchain network to track the condition of the EVs and provide tailored advice and warnings to each vehicle's owner. However, the transportation department is unable to adjust an EV's settings.

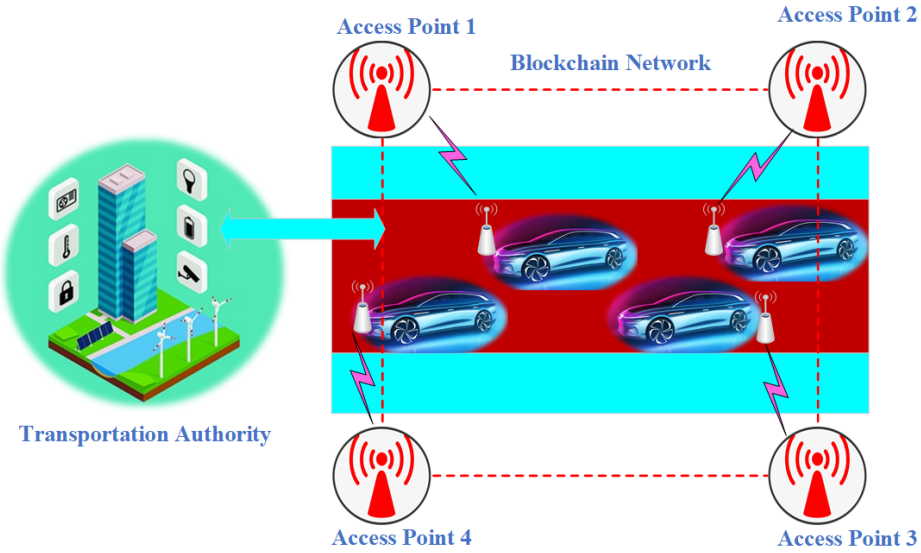

Figure 5. Blockchain architecture of EV applications.

The potential of electric cars as part of a sustainable transport system has gained them widespread attention in recent years. Rapid technological progress enabling smart network connectivity has enabled EVs to interact with their surroundings. Through the use of renewable energies and smart networks, the price of producing power is consistently dropping [49]. Therefore, the creation of a secure communication architecture that preserves data confidentiality and information anonymity is the primary difficulty of peer-to-peer technology, E-trading and D-trading, and integration for electric cars [50]. A blockchain's primary purpose is to hide commercial interactions behind a wall of anonymity without sacrificing data security [51]. The use of blockchain technology in the Emerging Smart Grid is the subject of many academic reviews [52,53]. Security has to be evaluated systematically to improve the SG's dependability, despite the technology's widespread repute for usefulness [54]. In response to this, the implementation of blockchain-based EV charging infrastructure is fully described in [55]. The Ethereum blockchain technology, widely used for implementing decentralized applications, serves as the basis for this research [56]. The benefit it provides is the secure crediting of energy flows between electric car owners and the corporations who control charging stations. The blockchain's inherent constraints, such as high transaction costs owing to network congestion, power dissipation, and transactions that do not alter in the event of mistakes, are the only obstacles that may be eliminated in the future. The importance of technoeconomic assessment of home energy trading systems was further shown by a test case in [57]. An electric vehicle (EV) is one component of this system that might benefit from blockchain technology. Electric vehicles that use blockchain technology not only increase residential engagement with power markets but also significantly mitigate their negative effects on the grid [58].

Challenges and Solutions: Some problems that have yet to be solved are the scalability of blockchain data, the security of downloaded data, and the privacy of blockchain transactions. Processing energy transfers and maintaining user privacy present a significant

difficulty for P2P platforms. The implementation of blockchain technology for EV applications with WSN infrastructure is hindered by the high resource required and transaction cost in terms of energy consumption. If these barriers could be removed, blockchain technology would become the most critical component in EV development. Possible solutions include the creation of compact blockchain algorithms for real-time consensus.

3.4. Blockchain for Renewable Microgrids

Each day brings more evidence of the ongoing shift and development toward a renewable grid based on a wide variety of decentralized energy sources, including solar panels, fuel cells, microturbines, batteries, and so on. Blockchain technology is essential to the smooth execution of these changes. Figure 6 depicts the MG application's generic blockchain architecture. A zone's electrical grid often covers a significant region, requiring many MGs to be considered. These many MGs are linked together through the blockchain system. Without compromising data quality or transparency, the blockchain network intends to improve safety and confidentiality in the MG operation. The produced energy, the power to be transferred with other microgrids, etc., are all included in the data block. Each freshly created block of MG data is verified by a consensus method to ensure its accuracy. After the block has been confirmed, it is added to the blockchain and the network. Blockchain nodes need appropriate algorithms to agree on the nature of the energy being transferred, the value of the power being sold, etc.

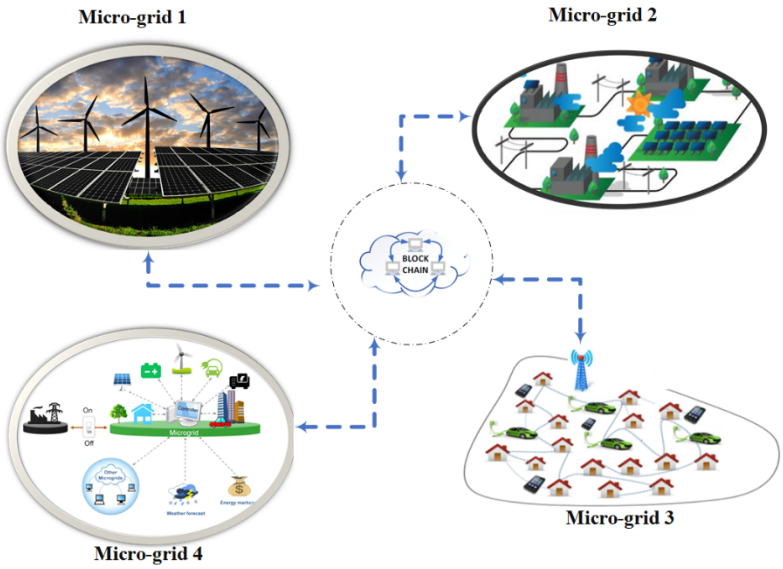

Figure 6. Blockchain architecture for MG.

Blockchain is viewed as a promising solution in renewable microgrids for efficient operation, such as complex point-to-point transactions between producers, traders, and users using intricate algorithms to validate, secure, and record these transactions. This is due to the growing community, financial, diplomatic, and environmental impacts and approaches, such as boosting power consumption, dealing with the middleman, market liberalization, and pollution. From a variety of angles, many authors have examined blockchain in the context of microgrids. The necessity of blockchain, its advantages, and its difficulties were discussed in [59]. Real-world solutions were provided in [11], including the Brooklyn Microgrid, which is based on a blockchain environment and uses the proof-of-work (PoW) mechanism. For individuals who want to suggest and execute workable solutions and approaches for renewable microgrids based on blockchain technology, additional thorough studies can be found in [60]. Furthermore, red. [61] presents an effective P2P blockchain-based energy market between a microgrid and a smart grid, with the distributed consensus algorithm being tested in the presence of a fault data injection attack (FDIA). In the face of a

cyberattack, this paper's primary results demonstrated that the general agreement process continues, with the P2P market's production response coming dangerously near to that of the centralized energy market. In keeping with the solution's spirit, the authors in [62] proposed a concept for a blockchain-based incorporated energy management platform and a bilateral trading mechanism that, according to the simulation findings, significantly optimizes energy flow in a microgrid. In [60], a different model for blockchain-based energy systems was proposed, with a Pythagorean fuzzy technique proposed for selecting the optimal energy generation, distribution, and disposal. Results indicating greater profitability and lower CO_2 emissions were also published in [63], which presents a different P2P energy trading method among the distributed generations based on the same technique employing a fuzzy meta-heuristic method as a pricing solution. In addition, the advantages of combining the power market with blockchain were investigated in [64] where transactions were emphasized utilizing a multi-agent coordination and trading model based on the Ethereum private blockchain. As we go further into the issue in this section, we find that blockchain applications vary depending on the underlying infrastructure technology of microgrids, such as in the case of AC, DC, or hybrid AC–DC MGs [65–67].

Challenges and Solutions: Blockchain-based renewable microgrids [68,69] provide many benefits but face significant obstacles. Limitations in technology, finances, society, the environment, politics and institutions, rules and regulations, social norms, and privacy and security from the beginning to the end are all obstacles to overcome. Key elements, such as privacy, resource management, restrictions, and prices, remain challenging to reconcile practically and effectively. Consortiums run microgrids in various ways; thus, evaluating and settling on the best algorithm or procedures to use; the most appropriate technology; the most appropriate investor; and a highly qualified workforce are essential.

3.5. Blockchain for Energy Management System

A distributed system's development and implementation by incorporating blockchain gives more advantages to both producers and users in the energy market. Wind and solar powers are becoming more popular sources of renewable energy, and as a result, the structure of the energy market and the need for safe energy transactions have evolved to accommodate this growth [70]. This can be accomplished with the use of blockchain technology. Energy marketing transactions have tremendous promise for blockchain's distributed ledger technology. An EMS aims to facilitate trustworthy real-time trading of energy among all participants in the energy market, including but not limited to generating systems (including renewable and nonrenewable energy sources), consumer services, energy providers, etc. [62]. Figure 7 depicts the blockchain architecture used by an EMS.

The SG plans to combine alternative and traditional power plants. On the demand side, we have private residences, apartment complexes, office buildings, shopping centers, etc. Additionally, EV charging facilities are under the purview of SG shoppers. However, the entities in the consumer domain not only use power but also generate it. Prosumers are a term used to describe this kind of customer. Prosumers help ease the power grid's strain when they store and use energy surpluses. While this relieves pressure on the power grid, it also makes it critical to track who buys and sells electricity. Safeguards to protect both parties' personal information are equally crucial to the success of the energy marketplace. Blockchain technology may be included into the EMS to accomplish this goal. As depicted in Figure 7, the blockchain's network seeks to connect all SG areas, including the generating system, the technical infrastructure, the consumption system, the regulator, and the control center. Through its distributed nature, interoperability, and smart contracts, the blockchain-based EMS protects the privacy and integrity of energy transactions. Private blockchains may integrate data controls and selective group access to guarantee safety and privacy in the energy trading market. The blockchain-based EMS improves transparency in P2P energy trading without jeopardizing users' right to privacy because to its decentralized nature.

Challenges and Solutions: Challenges in trading arise as energy expenditures go up for which the trading system requires stringent regulation; it cannot be allowed to operate unchecked. Stringent management of this trading system is essential because as the energy trade rises, the challenges increase more. As a result, in [71], a mechanism for managing energy transactions online was presented, allowing customers to learn more about their own pricing and consumption habits. In ref. [72], Yi Zhang et al. addressed the security issue for users and energy flow. An online double auction-based energy market structure was presented by S.N.G. Gourisetti et al. in [73]. Because of blockchain technology, we can now have smart meters with extra privacy and safety features. Furthermore, a platform to monitor the energy produced from renewable sources by storing and selling energy between residences and communication networks of users was suggested in [74]. The study about applications of blockchain technology in different SG domains is summarized in Table 2 as follows [75].

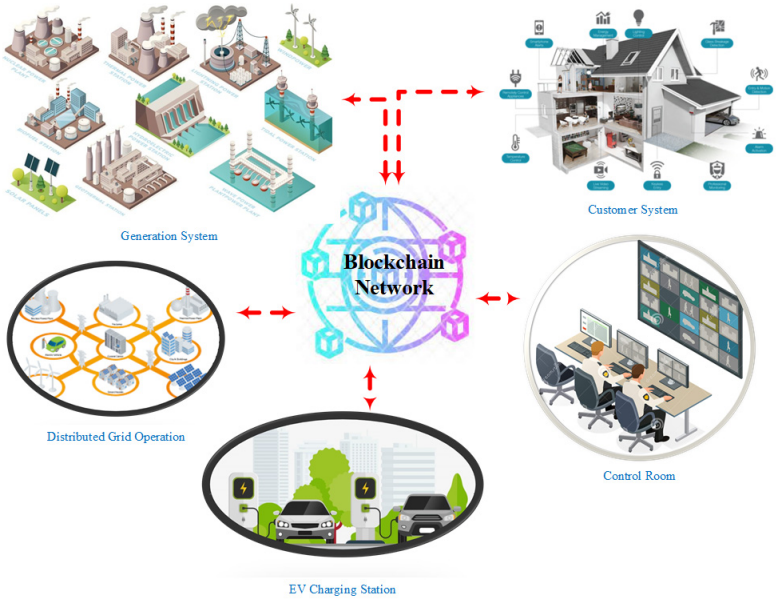

Figure 7. Blockchain architecture used by an EMS.

Table 2. Applications of blockchain technology in different SG domains.

Application Area	Description	Domain	Mechanism Used
Home Automation (HA)	While computationally quick and affordable, access control in smart homes is vulnerable to malicious assaults.	Access control	Private blockchain
	Secure method of transferring medical data to the medical facility, but has higher overhead	Home care	Ethereum blockchain
	Reduces communication overhead but adds extra overhead when sending patient data.	Home care	Private blockchain
	Decreases the block size for charging bill payment. Cyberattacks could happen because of this as well.	EV-charging bill payment	Lightweight basic blockchain
	The storage of older people's data is efficient and of higher quality, but it is subject to DoS attacks.	Home care	Consortium blockchain
	A scalable but pricey method of IoT device authentication	Authentication mechanism	Ethereum blockchain
	A very flexible automated payment system with off-chain transaction support	Automated payment	Bitcoin blockchain
	A quick and efficient payment procedure. This might be open to nefarious attacks.	Lightweight payment system	NA

Table 2. *Cont.*

Application Area	Description	Domain	Mechanism Used
Electric Vehicles (EVs)	Utilizing a game-theoretic method to effectively distribute mining duties to the mining clusters	V2X communications	Blockchain-based cellular V2X networks
	Deploying a novel framework (secure V2X) while protecting the confidentiality and security of the V2X protocol	Secure V2X communications	Blockchain and NDN (named data networking)
	Maintaining data confidentiality and information anonymity while improving the distribution network and renewable energy network.	Energy trading and charging payment system for EVs	Private blockchain
	Charging management framework with crediting in the safety zone of the energy flows between the owners and the companies.	Charging management	Ethereum blockchain platform
	Residential energy trading systems with reduced impact on the energy distribution network.	Blockchain platform	Ethereum blockchain platform
Microgrids (MGs)	Economic and energy blockchain-based flow with fund authentication and automatic control of transactions.	Local energy market	Public blockchain
	Decrease electricity costs for each time slot and local energy demand and generation balance, and optimize energy use, particularly during peak hours.	Local energy market/microgrid/smart grid	Private blockchain with PoW mechanism
	Decentralized market mechanism	Microgrid/smart grid	Private blockchain
	Lower electricity price control over power generation, and full self-consumption of renewable energy	Local energy market/microgrid	Public blockchain
	Both a decentralized and a semi-centralized structure are suggested. Framework 2 utilizes fewer transactions, is more flexible, and is less secure compared to Framework 1, which uses more transactions.	Local energy market/microgrid	Solc, Mocha, React.js, Next.js, Ganachecli, Metamask, Ganache-cli, and Web3
	Ensure security and reach consensus when cyberattacks happen.	Microgrid/smart grid	Either public or private blockchain
	Improve microgrid energy flow and lower import prices	Microgrid	Private blockchain
	Framework and proposed methodology for energy management	Renewable energy	Either public or private blockchain
Energy Management Systems (EMS)	Real-time consumer transaction verification, risk management for energy transactions, and security	Secure energy transaction	Blockchain
	Determining the energy trade's open price and allowing network members to monitor transactions	Energy price	Blockchain
	Lowering the cost of electricity needed to power the blockchain's operations while also improving the technology's energy efficiency	Blockchain performance. Blockchain-based virtual electricity generation	Blockchain
	Securing energy flow and users, as well as differentiating prices based on a classification of providers and consumers.	Smart contract trading	Blockchain
	Energy architecture objectives, and increased security	Energy market	Blockchain
	Energy trading between residents	Energy trading	Blockchain
	Energy trading with low transaction costs	Renewable energy	Blockchain

Table 2. *Cont.*

Application Area	Description	Domain	Mechanism Used
	Cloud service platform design for energy trading without intermediaries	Smart contract	Blockchain
	Trading through a secure decentralized system and smart contracts	Blockchain evolution and challenges	Blockchain
Smart Cities (SCs)	Enhancing citizens' standards of living	Smart village architecture	Blockchain in healthcare
	Online consultation data storage security, privacy, and integrity	Application of BC in the health system	Blockchain in healthcare
	How to use BC technology in the medical field to keep track of the patient's health. Effective data management and real-time patient monitoring	Application of BC technology in the healthcare	Blockchain in healthcare
	Modernizing the healthcare system with improved data security, privacy, and integrity	Public health in the smart society	Blockchain in healthcare
	A combination strategy based on off-chain storage and on-chain verification to increase privacy and security	Development of a BC based platform for healthcare	Blockchain in healthcare
	Exploiting photovoltaic parks, reducing pollution, selling extra energy, and lowering production costs	Green energy marketing	Blockchain in Smart City
	Effective trade, high-quality production, and capitalizing on energy surplus	Energy management	Blockchain in Smart City
	Energy trading, control, and use for irrigation systems that is effective	Utilizing renewable energy for irrigation	Blockchain in Smart City
	Design of a model for processing edge nodes in real time to increase system resilience	Scalable network of smart cities with hybrid architecture	Blockchain in Smart City
	An extensive analysis spanning numerous viewpoints on blockchain in smart cities and communities	Security issues for the smart city	Blockchain in Smart City
	Applications and study options for the BC-based smart city concept	Social issues	Blockchain in Smart City
	With the deployment of BC, the chain-based food traceability system was used as a case study to improve the effectiveness of supply chain management in the sector.	Supply chain data management	Blockchain in Smart City

3.6. Blockchain for Energy Management System

The smart city framework is rapidly changing because of the proliferation of technologies such as blockchain, the IoT, and cloud computing. The future of the Internet of Things (IoT) will determine the design of "smart cities", including the number and type of sensors and "smart objects" used to gather information about public facilities and services, as well as the availability of that information to the general public, the effectiveness of environmental safeguards, and the level of economic growth. Figure 8 depicts an overarching blockchain architecture for SCs [76]. It would be impractical to run all of the smart city's services on the same blockchain network. Because of this, cities of varying sizes and types of smart services will need different configurations of blockchain networks. It is possible that each blockchain may be tailored to the specific needs of a particular application. Data generated by smart equipment (such as smart cars, smart houses, and smart hospitals) are recorded in a blockchain. To guarantee the services run well, we will need appropriate techniques and blockchain frameworks [77].

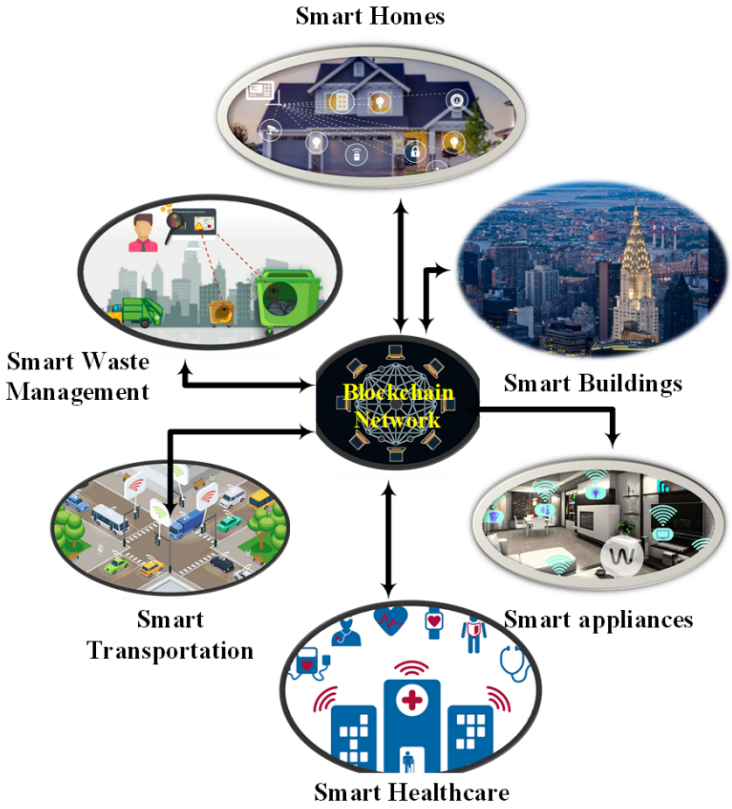

Figure 8. Overview of a blockchain architecture for SCs.

Some of the issues with smart city transportation were discussed in [78,79]. These studies showed how to use blockchain, which allows for the use of distributed stored data and performs transactions between producers and beneficiaries without the need for intermediaries, such as banks or governments, to improve public transportation and logistics [80,81], water supply [82,83], green energy [84,85], the environment [86,87], health [88,89], and education [90,91]. Smart contracts are becoming increasingly important in the evolution of transactions between parties, and blockchain architecture will bolster this trend. These contracts are initiated by either party's actions (understandings) or by the readings of sensors, actuators, or Internet-of-Thing tags [92]. As a result, logistics, energy, the ecosystem, water management, health, and other sectors will all benefit from block chain technology as they help transform communities into smart cities.

Challenges and Solution: Entities in smart cities come in a wide variety. Smart city entities employ various blockchain networks, each optimized for particular use cases. When it comes to smart transportation, for instance, the devices are constantly moving to new spots, but they are static in terms of smart illumination. The blockchain's architecture has to be well thought out before use due to the dispersed nature of the entities. There is a need for proper research to enhance blockchain technology so that it must be robust and quick. Furthermore, it might be difficult to obtain data from one blockchain network to another in the SC because of a lack of compatibility.

4. Blockchain-Enabled Cybersecurity System for Smart Grids

4.1. Common Security Risks in Smart Grids

Smart grids provide a number of possible concerns that might affect both businesses and normal consumers. Customers' personal information, among other sensitive pieces of data, may be at danger if the organization suffers any attack. Customers are vulnerable even when they are not online because enemies may attempt to snoop on them and steal private information. The percentage of cyberattacks is higher in the USA compared to any other country, which is 73%, while all other countries have cyberattacks less than 5%, and

sector wise, the energy sector has the topmost level of cyberattacks, which is 51%. It is common knowledge that cyberattacks may severely damage the smart grid. Cyberattacks may compromise a smart grid's availability, integrity, and privacy. Most cyberattacks may be broken down into a wide variety of subtypes, making it hard to list them all. The CIA Classification for smart grid attacks is listed in Table 3. This section will introduce several common forms of cyberattacks on the smart grid.

Table 3. CIA classification for smart grid attacks.

CIA	Attack
Confidentiality [15]	Social Engineering, Eavesdropping, Traffic Analysis, Unauthorized Access, Password Pilfering, MITM, Snifitting, Replay, Masquerading, and Data Injection
Integrity [16]	Tampering, Replay, Wormhole, False Data Injection, Spoofing, Data Modification, Time Synchronization, Load Drop, MITM, and Masquerading
Availability [17]	Wormhole, Jamming, Denial of service, LDos, Buffer Overflow, Teardrop, Smurf, MITM, Spoofing, Puppet, Time Synchronization, and Masquerading

4.1.1. Denial-of Service (DoS) Attacks

Distributed denial-of-service (DoS) attack is a kind of cyberattack in which hackers send out false instructions to a server or network, causing the service to be interrupted, either momentarily or permanently, for the target audience [93]. To overburden systems and prevent incomplete queries, attackers repeatedly send many requests to the targeted computer or resource [94]. The standard DoS attack employs a single computer and a single communication link to overwhelm the target network or resource. Distributed denial-of-service (DDoS) attacks are similar in nature but use a group of computers and networks to overwhelm their intended victim. Since it is hard to halt the attack by limiting a single source, the consequences of this attack might be far more severe [95].

Current denial-of-service and distributed denial-of-service (DDoS) attacks on smart rids target a variety of communication levels, including the application layer, the network and transport layers, the media access control (MAC) layer, and the physical layer [96]. Due to their poor computing capabilities, application-layer-based DoS/DDoS attacks can compromise millions of ICT devices in a smart grid [97]. Extreme data volumes are the mainstay of denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on the network and transport layers, slowing transmission bandwidth in the communication channels and ultimately impairing access for legitimate users. The quality of end-to-end communications is at risk from this form of assault [98]. To gain access to the network by reducing the performance of those who use the same communication channel, a DoS/DDoS attack at the MAC layer might deliberately tamper with the MAC settings. It is common knowledge that three types of frames (data frames, control frames, and management frames) are used to convey information at the MAC layer. While data frames are usually encrypted, management and control frames are not protected in the same way. As a result, denial-of-service and distributed denial-of-service attacks may disrupt the control and management infrastructure. It is a common practice for an attacker to use signal jamming to conduct a denial-of-service or distributed denial-of-service attack at the physical layer; all they need is a bridge to the communication channels. According to previous reports, jammer assaults on a smart grid may cause anything from delayed delivery of time-critical signals to a total denial of service [99].

4.1.2. False Data Injection Attack (FDIA)

FDIA may have detrimental effects on a power system because it can disrupt the state estimation process, leading the system operator astray [100]. State estimate is often a vital part of any control center. It takes raw sensor readings from the SCADA system, filters

them, and then manipulates each bus's status. Many power system applications rely on state estimates' outcomes [101,102]. False and malicious data information may be used to deliberately mislead energy management systems' control and monitoring functionalities (EMSs). Furthermore, a malevolent assault might lead to disastrous outcomes. The primary research foci are the theoretical foundations, practical implications, and countermeasures of FDIAs. The goal of the theoretical work is to develop injection vectors that can evade detection by the command-and-control server in a variety of scenarios. On the application side, i.e., energy management systems (EMS) and market management systems, the effect of FDIAs on power system functioning is evaluated (MMS). The primary responsibility of the defender is to provide system operators with effective defense tactics [103]. A legal FDIA may affect the electricity market and energy distribution and disrupt power system operations. Recently, Xie et al. [104,105] investigated both the ex-ante and ex-post effects of FDIAs in the electrical market. One of the goals of an assault is to increase one's gain. As a rule, they aim to buy virtual power cheaply at one node and then resell it to other nodes via an FDIA for profit.

4.1.3. Phishing

Since phishing is so simple to do, it might be the initial step in exposing companies and their consumers to danger. Hackers may get access to sensitive information about an electricity company if its clients do not properly dispose of their bills and payment receipts [106]. However, employees may also face threats from inside the company, such as phishing emails that appear legitimate but really include malware that steals personal information. Giving information to unreliable sources and understanding the ramifications of these threats may have a privacy and financial impact on smart grid consumers. Hence, it is a major issue for designing a defense against phishing assaults [107].

4.1.4. Eavesdropping

Some forms of spoofing attacks include eavesdropping and analyzing traffic patterns. The intruder may steal private data by eavesdropping on network traffic. Keeping the devices linked to the broader network, which a smart grid relies on, is challenging. Therefore, it poses a danger to the whole system. Most data security centers are concerned about smart grid since it presents the most significant threat of data theft [108].

4.2. Security Breaches

A smart grid is a technological composite that uses network and communication technologies to provide a number of advantages while delivering electricity. Smart grids, however, may be susceptible to the same dangers associated with online systems. Numerous security breaches have occurred, and these are examined in various papers that detail the effects of certain significant cyberattacks and provide recommendations for preventing such assaults in the future [35].

4.2.1. Trojan-Horse Malware Black Energy

A cyberattack incident occurred amid a civil war scenario on 25th December 2015. A cyberattack on an electrical power plant in the Ukrainian city of Ivano-Frankivsk placed the lives of 80,000 people in danger by leaving them in the dark. The cyberattack was performed by utilizing a spear-phishing email and a Trojan-horse software known as the "BlackEnergy" [108]. This was a very destructive virus that could wipe files, corrupt hard drives, and even take over afflicted machines. The cyberattack progressed further when the culprit launched a targeted denial-of-service assault (DoS attack) on the industry's utility equipment, disabling the support phone number of the operator at the power plant [109]. Therefore, customers could not report the outage because of the DoS attack. This issue worsened significantly and severely since the cyberattack stole information and destabilized a country's essential infrastructure. Without heat or power, many people perished in the bitter cold. This is the single most disastrous event in recent history [110].

4.2.2. Stuxnet

Stuxnet is a dangerous computer worm that attacks SCADA systems (SCADA). In 2010, Stuxnet was discovered for the first time (Denning, 2012). It was speculated that the United States' and Israeli spy services were responsible for developing the Stuxnet [111]. The harmful Stuxnet computer worm leverages the Microsoft Windows' operating system and networks and is capable of manipulating programmable logic controllers (PLCs), which are responsible for managing the electromechanical operations of machines. The massive computer worm Stuxnet managed to enter the control system of Iran's Nuclear Power Plant, where it manipulated the (PLCs) that regulated the centrifuges used to separate nuclear material, causing them to spin faster than normal and rip the machinery apart [112]. In response to the Stuxnet computer virus, the specialized machinery increased their rotational speed and promptly began damaging the nuclear fuel. While Stuxnet itself poses little threat to infected machines, it does perform a check to determine whether the infected machine is linked to certain Siemens PLC types. The United States and Israel designed Stuxnet to stop Iran's nuclear weapon development.

4.2.3. WannaCry Ransomware

WannaCry ransomware was a catastrophic piece of software that brought down the computers of thousands of average individuals all around the world and crippled major corporations, such as Renault and FedEx. On 12 May 2017, the WannaCry ransomware was released. Over 200 thousand machines were infected with the WannaCry Ransomware malware, which locked data and demanded a fee to decrypt them [113]. If victims did not pay the USD 300 in bitcoins, the hackers sought to decrypt the whole system and threatened to wipe all of the system data permanently. According to reports, the WannaCry Ransomware assault had the greatest effect on NHS hospital systems, resulting in the cancellation of over 19,000 appointments and putting many lives at risk. Twenty million pounds in penalties and an additional seventy-two million pounds in cleaning up and updating the IT systems made up the overall cost of rebuilding the NHS's IT infrastructure [114]. The ransomware assault was disseminated in a number of different ways, including via phishing emails and antiquated computers that lacked the latest Microsoft security updates. According to the joint investigation conducted by the United States, the United Kingdom, and Australia, the assault was carried out by highly skilled hackers from North Korea. As computers in hospitals are utilized for life-or-death surgeries, the focus on this deadly cyberattack has created a terrible danger to human lives [115].

4.3. Countermeasures against Cyberattacks

Concerning cybersecurity in smart grids, the information and communication networks are particularly exposed to threats and hazards. Practicing certain security risks preferably requires a security solution to guard against vulnerabilities. The greatest challenge to a network and system is the dangers and threats that it faces. Figure 9 shows the classification of smart grid attacks and threats from different sources. Protecting the integrity of a smart grid system and its data requires a proper protection scheme that can counterattack to a wide range of cyberattacks. It is believed that using many defensive measures at different detecting nodes may achieve a protected and secure system. A distributed denial-of-service (DDoS) assault is one of the most significant dangers to a smart grid because it may cause the breakdown of the communication networks and control systems that are the foundation of the smart grid. The two types of strategies against DoS attacks followed by a discussion of additional counterattacks for smart grid is given as follows.

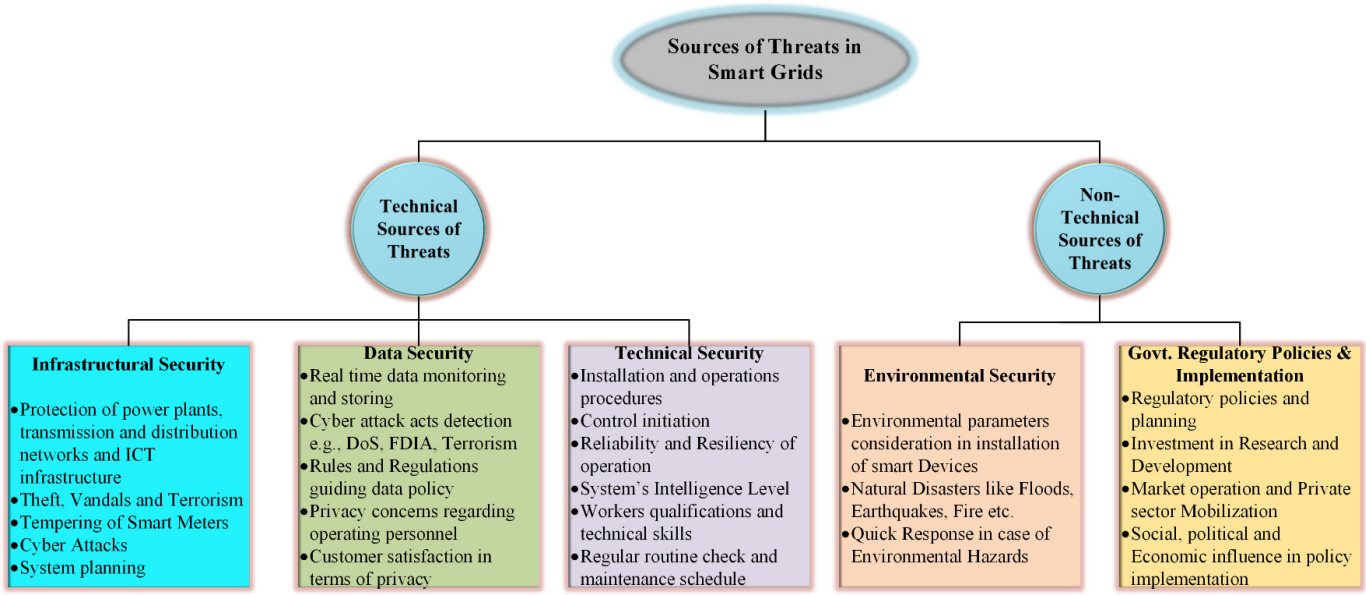

Figure 9. Classification of smart grid attacks and threats from different sources.

4.3.1. Detection and Defense for DoS Attack

DoS cyberattacks may be initiated from anywhere in the globe with access to communication networks including the Internet, and a smart grid must be able to identify and defend against these attacks. Obviously, the first step in taking precautions against assaults is to identify them [116]. Detection based on the signal itself occurs at the physical MAC layer. By receiving the signal and gauging its intensity, a DoS attack detector may determine whether an attack is in progress and sound an alert if one is. Detection based on individual packets is a method that may be used to evaluate the transmission's success across any number of layers. Given that DoS assaults often cause packet loss or delay, and, consequently, a decline in network performance, this is a common and efficient strategy. DoS attacks may be detected, and the security of a network can be tested or measured by sending out probe packets in advance. The hybrid approach aims to improve the accuracy of threat detection by designing a single integrated strategy out of two or more methods [117].

Defense, in the form of attack mitigation measures, may be deployed to protect a network against DoS assaults after they have been identified. There are two primary categories of countermeasures: those that operate at the network layer and those that operate at the physical layer. Defenses against denial-of-service attacks that include some kind of network layer mitigation are rate limiting, filtering, and reconfiguration. The goal of rate-limiting technique is to restrict the transmission speed of malicious packets. Filtering employs a filtering system based on comparing packet source addresses to a blacklist, blocking any suspicious traffic so the attacking packets will not reach their intended targets in this manner. Reconfiguring the network's architecture to provide the victim extra resources or shut down the attacking nodes is one approach [118]. In a wireless smart grid, a wireless jamming attack should be the principal denial-of-service attack. Jamming-resistant techniques have been developed in recent years to reduce the effects of this kind of assault. In coordinated control, different methods, including direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), and chirp spread spectrum (CSS), are used to protect against wireless cyberattacks. However, in DSSS, the secret is designed to be unknowable to attackers in a straight sequence, while in FHSS, the secret is supposed to be unknowable to attackers in a hopping pattern. With uncoordinated protocols, a new secret is generated randomly for each conversation, making it difficult for the attackers to gather enough knowledge to disrupt the signal. This approach holds

significant promise for securing wireless communications in a decentralized setting since it does not rely on the transmitter and the receiver sharing an assumed secret [119].

4.3.2. Encryption

The stated encryption encodes data so an unauthorized party cannot decode them. Any piece of information that is encrypted and then any data that the hackers intercept are useless in the form of raw code. Encryption may be seen as a kind of hidden coding. A cipher is the method by which your information is encrypted, and a key is the set of rules that enables you to read the message again [120]. The most highly rated VPN services use 256-bit AES (Advanced Encryption Standard), the industry's strongest encryption standard, where 256 is the length of the encryption cipher being employed. With 256-bit encryption, the number of possible permutations exceeds the number of stars in the Milky Way. Banks and governments all across the globe rely on this degree of encryption to protect their sensitive information [121].

4.3.3. Authentication

Robust authentication systems are of utmost importance in situations when it is necessary to maintain authentication and manage access [122]. An "implicit deny policy" may be useful in implementing authentication and the policy's usage in allowing only explicit users access to the network. This policy provides the business with security solutions and allows for the differentiation of rights across users (e.g., management can view all extra data linked to projects, while workers have restricted access to data). By limiting access to trusted employees, you can lessen the likelihood of a security breach and know exactly who logged in. In addition, SSL protocols may be used to perform authentication. Cyberattacks, such as denial of service, might compromise the protocols [123]. Because of the increased bandwidth needed for communication inside a smart grid network, cryptographic methods may be employed for authentication [124].

4.3.4. Malware Protection

Malware protection is essential for a smart grid because of the need to secure and protecting the embedded system and the general-purpose systems that are linked to the smart grid from cyberattacks. To verify the integrity of the embedded software, a manufacturer's key is needed. To provide the solutions, the manufacturer's software may need to be authentic, and the company may need to implement risk management in order to limit the damage that may come from installing counterfeit programs [115]. An alternative to utilizing the manufacturer's key is to ensure that the program is authentic and has not been illegally duplicated. Antivirus software is often used as a first line of defense when it comes to warding off malware. Threats may become susceptible to malware through phishing assaults, but the antivirus software must be up to date with the latest patch, and the attacker must not discover a means to evade the protection. Using a network intrusion prevention system (NIPS), which can both restrict user access to a network and defend it from cyberattacks, is the most efficient and secure method for securing a smart grid. In addition, the NIPS can keep an eye on intrusion data and respond to halt an attack before it ever begins. Network intrusion detection systems (NIDS) provide another option for smart grid security by monitoring and analyzing the network traffic in order to identify and prevent network-based attacks [125].

4.3.5. Network Security

VPNs allow users to increase their protection while connecting to a public network through the Internet. Using public network infrastructure puts sensitive information at risk, thus a virtual private network (VPN) employs a number of security measures, including encryption, to safeguard data in transit. Furthermore, virtual private networks (VPNs) are employed for communication since they provide a safe channel for data transfer. There are two distinct VPNs, both of which provide advantages to businesses and their frequent

customers [126]. Remote access virtual private networks (VPNs) allow users to connect to internal company networks through a public network. After authenticating, users on mobile devices and desktop computers will be able to access the VPN server. When the credentials are right, the authentication is able to confirm access and provide access to the virtual network's resources. An organization's proprietary apps and data are among the resources that are accessible solely inside the company. Connecting to a VPN gateway allows users of the remote access VPN to perform their duties from any location. Virtual private networking (VPN) between two sites is quite similar to VPN access from a remote location. However, it often links the whole network in a single spot, even if the networks themselves are situated elsewhere; this is helpful for a bigger company that has to safely share its resources with several outposts in different areas to serve its partner or client business [127].

4.3.6. Risk and Maturity Assessments

Recent years have seen the development of a variety of ingenious methods for efficiently conducting cybersecurity risk assessments and executing mitigations in extensive, sophisticated networks and infrastructure where complete security audits cannot be performed owing to time and capacity constraints. Cyber defense triage is a technique proposed by [128] that helps identify high-impact attack areas that need security solutions immediately. Again, security holes and weak spots may be found and corrected if a maturity assessment is performed, as suggested in [129]. This includes risk assessment, which is only one of several controls that can be reviewed.

4.3.7. IPS and IDS

Technologies for identifying and blocking intrusions in a network include intrusion prevention systems (IPS) and intrusion detection systems (IDS). An IPS is a kind of network protection that can recognize and stop certain attacks [130]. Intrusion prevention systems constantly monitor your network, recording any suspicious activity. An IPS alerts the system administrators and they shut down the access points and set up the firewalls to avoid further assaults. It is possible to utilize an IPS to detect when workers or visitors to a network are breaking the regulations set out by the company. In contrast, an IDS is just tasked with monitoring the network and alerting system administrators to any suspicious activity [131].

5. Blockchain Implication for Cybersecurity of Smart Grid Paradigm

Considering a more diverse and dispersed structure for SG is necessary in light of the urgent need to include renewable energy sources. This goal has been accomplished with the use of a DER and a decentralized power-generating system [132]. However, this has added further layers of complexity to the SG. PMUs, smart meters, home automation sensors, remote terminal units, etc., are only a few examples of the equipment that make up a SG's complex infrastructure, which also includes devices from the generation, transmission, distribution, user, operation, marketing, and utility domains [133]. Maintaining the reliability of this fantastic SG infrastructure needs constant vigilance. Different applications are needed for a different set of communication tools and protocols. A wide area network (WAN) serves as the backbone of the communication system (WAN). Local area networks (LAN), home area networks (HAN), wireless sensor networks (WSN), neighborhood area networks (NAN), etc. are a few examples of various forms of communication networks. The TCP/IP protocol suite is widely used for data transmission over these communication networks. In short, TCP/IP is not a safe protocol to use. As a result, the SG apps' communication network is very susceptible to assault. Although a SG has adopted some basic security measures, such as a firewall, intrusion detection, encryption, and authentication, it is still susceptible to a number of cyberattacks. In [134], the author provides a thorough overview of the different detection techniques available for spotting cases of erroneous data injection.

Generally speaking, a SG fits the profile of a cyber-physical system [135,136]. Cybersecurity is an essential factor that guarantees the three key properties of every cyber-physical system: availability, confidentiality, and integrity. As a property, "availability" means that all information may be accessed quickly and easily. Depending on the severity of the cyberattack, availability may be hindered by data blockage, data delay, data corruption, or data loss. Cyberattacks have a significant effect on the accessibility of SG apps. To prevent other parties from gaining access to sensitive or private data, the system is said to have the quality of confidentiality. The privacy and copyrights of a SG application might be jeopardized by a hack on confidentially. Theft of password-related information is one way that such accidents might allow unauthorized access to the program, which can have catastrophic effects on its functioning. To prevent tampering, corruption, or deletion of data, integrity is defined as the capacity of an application to prevent unwanted access to its storage system. Information used to setup an application may be compromised by an assault on its integrity, resulting in a catastrophic loss. The sensors, for instance, may end up misconfigured due to the change data, which would then cause the SG program to fail. Blockchain is an open, decentralized ledger that cannot be altered once it has been created and does not need a trusted third party to function. Because of this, blockchain is an essential component of SG apps because it provides a safe means of transferring data. The security of a SG application may be fortified by using a blockchain to specifically counteract threats. Due to the numerous types of participants and the diverse ways in which agreement is reached, a public blockchain is the safest of the different types of blockchains. Members of the public blockchain may maintain their anonymity, but only trustworthy nodes are allowed to participate in the consortium and private blockchains. Proof of work is used as the consensus method in the public blockchain, whereas multi-party voting and rigorously pre-approved nodes are used in the consortium blockchain and private blockchain, respectively. However, the processing cost of a public blockchain is quite high. Therefore, consortium and private blockchains are preferred over public blockchains when security concerns are minimal and computational complexity is low.

Smart devices create data that are sent to the blockchain network server through the TCP/IP protocol. The data may be hashed and encrypted at the device level, forming the block that can later be added to the blockchain network if the devices have sufficient processing capacity. This is the safest design since if the data are altered once they leave the devices, they will invalidate the block because of the update in the hash function. This, however, places significant computational strain on the end nodes, which are often already performing many simultaneous activities. Another option is to use TCP/IP to transfer data to blockchain servers/nodes and then construct blockchain blocks. Though less safe, it lacks the computing capability of more advanced smart gadgets. The latter is where the use of private and public keys for further authentication might be useful. Since all consortium blockchain members are known and trustworthy, and the consensus method is centered on multi-party consensus with no anonymity loopholes, this design intends to maximize security. The administration and the management choose the nodes that will participate in mining on the consortium and private blockchains.

6. Challenges and Potential Future Research Directions

To fully realize blockchain's potential as a game-changing component, a number of significant issues related to scalability, computing cost, security, and privacy need to be resolved.

Scalability limitations: The throughput, efficiency, and computing cost of existing blockchain systems are all too often inadequate. Many blockchains now have long processing times for transactions to be put into the chain of previously verified blocks because of limitations in block size. As a result, block time grows exponentially, degrading the system's efficiency. If every transaction is recorded in the distributed ledger, it will grow to be enormous very quickly [137,138]. IoT data are massive because of the complexity of IoT use cases, such as smart cities and eHealth. As a result, the amount of data generated

by IoT devices will explode, making it difficult for a blockchain to handle such massive data sets. As a result of these drawbacks, many app developers do not consider blockchain technology to be a viable replacement for the status quo in managing complex IoT networks [139–141]. High computational cost: As the computational cost of a blockchain, the fee for executing a transaction was published by Wood et al. [142]. There are several moving parts in the execution of a transaction, such as creating robust security, mining, verifying, and storing it across a distributed network of users [143]. Together, these procedures need a considerable amount of processing time. Some mining methods, such proof of work (PoW), proof of stake (PoS), and practical Byzantine fault tolerance (pBFT), need much more power than others. To validate transactions, for example, proof of work (PoW), the most decentralized mining mechanism, involves solving a complex mathematical problem. IoT systems struggle to match the resource requirements of PoW for qualifying the most decentralized nature because of their limited resources. The complexity of a blockchain system will need substantial technological and human resources, even for IoT devices with reasonably high processing capabilities. Concerns about high maintenance costs from consumers would be sparked, preventing the widespread use of blockchain-based services.

Security and privacy issue: Blockchain technology is resilient to DDoS, Sybil, selfish mining, and ransomware, but the current implementation has its own security issues. Blockchain's consensus mechanisms and the confirmation of new transactions are vulnerable to manipulation by actors that control more than 50% of the computers operating the blockchain. In Bitcoin parlance, this is known as a 51% assault. Blockchains are vulnerable to data loss and network interruption if their transactions are not closely monitored. Sybil attacks include malevolent nodes creating many identities in order to deceive others by reporting incorrect information or overwhelming the network with fraudulent transactions [144,145]. Distributed denial-of-service attacks is more challenging on a blockchain network. However, DDoS assaults and similar message-stealing attacks are particularly prevalent on blockchain networks [146]. DDoS attacks target monetary services, including mining, electronic wallets, and cryptocurrency exchanges. Selfish mining is a technique used in bitcoin mining wherein a group of miners pool their resources in order to maximize their revenue. In selfish mining, a miner (or group of miners) deliberately withholds or releases blocks from the network to maximize their financial gain [147–151]. Storing all types of health data on a blockchain creates a delay in performing transactions and risks data leakage and revelation of patients' sensitive information, despite the fact that blockchain and IoT can facilitate secure data exchange.

More research into the construction of a blockchain-based smart grid framework, including an IDS and DAPPS tailored to smart grid applications, may be pursued using various architectural approaches. Considering DDoS attacks, FDIA attacks, breaches, and man-in-the-middle attacks, a testing framework for a blockchain-enabled smart grid may be researched and created. Multiple distributed blockchain networks may be combined to form the blockchain network of the whole transmission system, a potential benefit of the distributed implementation of the blockchain with smart contract functions. The ability to monitor and regulate the transmission system in a decentralized, cyber-secured environment can deal with the rising number of distributed generators (DGs) and protect the system's functioning from a single point of failure. A power grid, for instance, may be partitioned into areas, each of which would be monitored by a unique collection of ICT devices enabled by the Internet of Things (IoT) and equipped with smart contracts containing the governing logic and algorithms. It is possible to designate one area as the command center and then create a system for invoking contracts across separated areas that considers the time syncing of sensors and actuators. The distributed control algorithm must provide individual subcontracts for regional generation and consumption control. Additionally, sophisticated algorithms for cyber-protected RTU and IED control in the smart grid may be built as part of blockchain-based smart contracts. To regulate voltage, tap changers in the electrical grid may be operated using smart controls stored on the blockchain.

7. Conclusions

As data storage and processing capabilities improve, so does SG. Blockchain is one such innovation that has the ability to revolutionize a SG's internal financial dealings. The blockchain may be used to authorize transactions without a central authority since it is a decentralized and secure system. It has been underused for SG applications despite its enormous utility in other fields. In this study, we looked at blockchain technology from the point of view of its potential usefulness in SG settings. Important SG applications were outlined, along with suggested general structures and highlighted obstacles. The analysis could help researchers focus their efforts on creating unique technologies that can handle the demands of real-world SG applications. From many vantage points, blockchain-based technologies are still in their infancy and represent unsolved research questions for the future. Many SG apps run in real time, and the blockchain should not slow them down. Computing demands place a heavy burden on the resources available in blockchain-based systems. Blockchain technology has to be optimized to run on less resource-intensive frameworks without sacrificing security. To make this technology widely used and interoperable, regulators will need to establish standardized processes. Future study into some of these questions has the potential to alter the landscape of blockchain-based systems radically.

Competency- and productivity-wise, smart grids outperform their historical counterparts because they are more secure, employ more renewable energy sources, enhance energy management efficiency, lower consumers' electricity bills, and cut down on greenhouse gas emissions and reduce their environmental impact. Yet, another internet-wide cybersecurity risk will be introduced by this novel system. As the conventional power grid increasingly relies on private networks that do not need a major cybersecurity concern, the importance of cybersecurity in the power sector grows. As a result, cybersecurity in smart grid is an emerging area of study that is gaining traction in both the academic circles and the business world. While several papers have discussed the security advantages and vulnerabilities of smart grids in their study, almost all of them have concluded that a denial-of-service attack is the greatest danger to smart grid that makes it vulnerable to network attacks, which would effectively shut down the whole grid.

This article provides an overview and discussion of cybersecurity in the smart grid context. Several significant cyberattack models have been given, along with defensive strategies to counteract them. This study also considers potential smart grid-related difficulties. The complexity of smart grids arises from the wide range of devices that must communicate over an extensive network coverage. The most challenging part of securing these devices is to protect them against cyberattacks over large geographical networks. Finally, computer network protocols must be updated to reflect the current communication state to provide complex encryption techniques and offer security countermeasures. As a result, it will protect us from more sophisticated cyber threats.

Author Contributions: Conceptualization, M.W. and M.A.K.; methodology, M.W., M.A.K., A.G., S.F., I.A.S. and P.S.; software, M.W. and M.A.K.; validation, M.W., M.A.K. and A.G.; formal analysis, M.W., M.A.K., A.G., S.F., I.A.S. and P.S.; investigation, M.W., M.A.K., A.G., S.F., I.A.S. and P.S.; resources, M.W., M.A.K., A.G., S.F., I.A.S. and P.S.; data curation, M.W.; writing—original draft preparation, M.W. and M.A.K.; writing—review and editing, M.W., M.A.K., A.G., S.F., I.A.S. and P.S.; visualization, M.W., M.A.K., A.G., S.F., I.A.S. and P.S.; supervision, I.A.S.; project administration, I.A.S.; funding acquisition, P.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data supporting the reported results are available in the manuscript.

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. Des Sci. Tech.* **2021**, *65*, 245–252.
2. Mahmoud, M.A.; Md Nasir, N.R.; Gurunathan, M.; Raj, P.; Mostafa, S. 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. Kaltakis, K.; Polyzi, P.; Drosatos, G.; Rantos, K. Privacy-Preserving Solutions in Blockchain-Enabled Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 9792. [CrossRef]
5. 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]
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. 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]
9. 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]
10. 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]
11. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
12. 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]
13. 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]
14. Zia, M.F.; Benbouzid, M.; Elbouchikhi, E.; Muyeen, S.; Techato, K.; Guerrero, J.M.J.I.A. Microgrid transactive energy: Review, architectures, distributed ledger technologies, and market analysis. *IEEE Access* **2020**, *8*, 19410–19432. [CrossRef]
15. Guru, D.; Perumal, S.; Varadarajan, V. Approaches towards blockchain innovation: A survey and future directions. *Electronics* **2021**, *10*, 1219. [CrossRef]
16. 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]
17. Liaqat, R.; Sajjad, I.A.; Waseem, M.; Alhelou, H.H. Appliance Level Energy Characterization of Residential Electricity Demand: Prospects, Challenges and Recommendations. *IEEE Access* **2021**, *9*, 148676–148697. [CrossRef]
18. 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]
19. Khan, T.; Yu, M.; Waseem, M. Review on recent optimization strategies for hybrid renewable energy system with hydrogen technologies: State of the art, trends and future directions. *Int. J. Hydrogen Energy* **2022**, *47*, 25155–25201. [CrossRef]
20. 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]
21. 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]
22. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A survey on blockchain for information systems management and security. *Inf. Process. Manag.* **2021**, *58*, 102397. [CrossRef]
23. 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]
24. 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.
25. WU, Z.; LIANG, Y.; KANG, J.; YU, R.; HE, Z. Secure data storage and sharing system based on consortium blockchain in smart grid. *J. Comput. Appl.* **2017**, *37*, 2742.
26. Hasan, M.K.; Alkhalifah, A.; Islam, S.; Babiker, N.; Habib, A.; Aman, A.H.M.; Hossain, M. Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 9065768. [CrossRef]
27. Kumar, A.; Bhushan, B.; Nand, P. Preventing and Detecting Intrusion of Cyberattacks in Smart Grid by Integrating Blockchain. In *Micro-Electronics and Telecommunication Engineering*; Springer: Singapore, 2022; pp. 119–130.

28. Thakare, S.; Pund, M. Introduction to Blockchain and Terminologies. In *Blockchain for Smart Systems*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2022; pp. 3–20.
29. Çelik, D.; Meral, M.E.; Waseem, M. The progress, impact analysis, challenges and new perceptions for electric power and energy sectors in the light of the COVID-19 pandemic. *Sustain. Energy Grids Netw.* **2022**, *31*, 100728. [CrossRef]
30. Guo, Y.; Wan, Z.; Cheng, X. When Blockchain Meets Smart Grids: A Comprehensive Survey. *High-Confid. Comput.* **2022**, *2*, 100059. [CrossRef]
31. Çelik, D.; Meral, M.E.; Waseem, M. Scenarios, Virtualization and Applications for Blockchain Technology in Smart Grids. In Proceedings of the 2022 IEEE Kansas Power and Energy Conference (KPEC), Manhattan, KS, USA, 25–26 April 2022; pp. 1–5.
32. Waseem, M.; Lin, Z.; Liu, S.; Sajjad, I.A.; Aziz, T. Optimal GWCSO-based home appliances scheduling for demand response considering end-users comfort. *Electr. Power Syst. Res.* **2020**, *187*, 106477. [CrossRef]
33. Mathew, R.; Mehbodniya, A.; Ambalgi, A.P.; Murali, M.; Sahay, K.B.; Babu, D.V.J.S.E.T. Assessments. In a virtual power plant, a blockchain-based decentralized power management solution for home distributed generation. *Sustain. Energy Technol. Assess.* **2022**, *49*, 101731.
34. Augello, A.; Gallo, P.; Sanseverino, E.R.; Sciumè, G.; Tornatore, M. A Coexistence Analysis of Blockchain, SCADA Systems, and OpenADR for Energy Services Provision. *IEEE Access* **2022**, *10*, 99088–99101. [CrossRef]
35. Goudarzi, A.; Ghayoor, F.; Waseem, M.; Fahad, S.; Traore, I. A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. *Energies* **2022**, *15*, 6984. [CrossRef]
36. Majeed, R.; Abdullah, N.A.; Ashraf, I.; Zikria, Y.B.; Mushtaq, M.F.; Umer, M. An intelligent, secure, and smart home automation system. *Sci. Program.* **2020**, *2020*, 4579291. [CrossRef]
37. Tian, H.; Jian, Y.; Ge, X. Blockchain-based AMI framework for data security and privacy protection. *Sustain. Energy Grids Netw.* **2022**, *32*, 100807. [CrossRef]
38. Khan, M.A.; Sajjad, I.A.; Tahir, M.; Haseeb, A. IOT Application for Energy Management in Smart Homes. *Eng. Proc.* **2022**, *20*, 43.
39. Kamal, M.; Tariq, M. Light-weight security and blockchain based provenance for advanced metering infrastructure. *IEEE Access* **2019**, *7*, 87345–87356. [CrossRef]
40. 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]
41. 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]
42. Islam, M.M.; Shahjalal, M.; 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.
43. 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]
44. Pal, R.; Chavhan, S.; Gupta, D.; Khanna, A.; Padmanaban, S.; Khan, B.; Rodrigues, J.J. A comprehensive review on IoT-based infrastructure for smart grid applications. *IET Renew. Power Gener.* **2021**, *15*, 3761–3776. [CrossRef]
45. 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]
46. 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]
47. 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]
48. 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]
49. 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]
50. Gomes, L.; Spínola, J.; Vale, Z.; Corchado, J.M. Agent-based architecture for demand side management using real-time resources' priorities and a deterministic optimization algorithm. *J. Clean. Prod.* **2019**, *241*, 118154. [CrossRef]
51. Khan, P.W.; Byun, Y.-C. Blockchain-based peer-to-peer energy trading and charging payment system for electric vehicles. *Sustainability* **2021**, *13*, 7962. [CrossRef]
52. Musleh, A.S.; Yao, G.; Muyeen, S. Blockchain applications in smart grid–review and frameworks. *IEEE Access* **2019**, *7*, 86746–86757. [CrossRef]
53. 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]
54. 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]
55. 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]
56. Dib, O.; Brousmiche, K.-L.; Durand, A.; Thea, E.; Hamida, E.B. Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun.* **2018**, *11*, 51–64.

57. Saxena, S.; Farag, H.E.; 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]
58. 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]
59. Vieira, G.; Zhang, J. Peer-to-peer energy trading in a microgrid leveraged by smart contracts. *Renew. Sustain. Energy Rev.* **2021**, *143*, 110900. [CrossRef]
60. Yildizbasi, A. Blockchain and renewable energy: Integration challenges in circular economy era. *Renew. Energy* **2021**, *176*, 183–197. [CrossRef]
61. 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]
62. 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]
63. 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.* **2021**, *136*, 110452. [CrossRef]
64. 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]
65. 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]
66. 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.* **2022**, *135*, 107499. [CrossRef]
67. 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.* **2022**, *135*, 107515. [CrossRef]
68. 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.* **2020**, *117*, 109488. [CrossRef]
69. Khan, M.A.; Ali, A. Hybrid Fuzzy-PI and ANFIS Controller Design for Rotor Current Control of DFIG Based Wind Turbine. *Pak. J. Eng. Technol.* **2022**, *5*, 35–41. [CrossRef]
70. Çelik, D.; Meral, M.E.; Waseem, M. Investigation and analysis of effective approaches, opportunities, bottlenecks and future potential capabilities for digitalization of energy systems and sustainable development goals. *Electr. Power Syst. Res.* **2022**, *211*, 108251. [CrossRef]
71. Hu, W.; Li, H. A blockchain-based secure transaction model for distributed energy in Industrial Internet of Things. *Alex. Eng. J.* **2021**, *60*, 491–500. [CrossRef]
72. Zhang, Y.; Shi, Q. An intelligent transaction model for energy blockchain based on diversity of subjects. *Alex. Eng. J.* **2021**, *60*, 749–756. [CrossRef]
73. 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]
74. Khan, T.; Waseem, M.; Tahir, M.; Liu, S.; Yu, M. Autonomous hydrogen-based solar-powered energy system for rural electrification in Balochistan, Pakistan: An energy-economic feasibility analysis. *Energy Convers. Manag.* **2022**, *271*, 116284. [CrossRef]
75. 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. [CrossRef]
76. Esposito, C.; Ficco, M.; Gupta, B.B. Blockchain-based authentication and authorization for smart city applications. *Inf. Process. Manag.* **2021**, *58*, 102468. [CrossRef]
77. Rejeb, A.; Rejeb, K.; Simske, S.J.; Keogh, J.G. Blockchain technology in the smart city: A bibliometric review. *Qual. Quant.* **2022**, *56*, 2875–2906. [CrossRef] [PubMed]
78. 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 July2021; pp. 1–6.
79. 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.
80. Kumar, A.; Singh, A.K.; Ahmad, I.; Kumar Singh, P.; Verma, P.K.; Alissa, K.A.; Bajaj, M.; Ur Rehman, A.; Tag-Eldin, E. A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. *Sensors* **2022**, *22*, 5921. [CrossRef]
81. 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]
82. 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]
83. Rocha, G.d.S.R.; de Oliveira, L.; Talamini, E. Blockchain applications in agribusiness: A systematic review. *Future Internet* **2021**, *13*, 95. [CrossRef]

84. Waseem, M.; Lin, Z.; Ding, Y.; Wen, F.; Liu, S.; Palu, I. Technologies and practical implementations of air-conditioner based demand response. *J. Mod. Power Syst. Clean Energy* **2020**, *9*, 1395–1413. [CrossRef]
85. Rizwan, M.; Waseem, M.; Liaqat, R.; Sajjad, I.A.; Dampage, U.; Salmen, S.H.; Obaid, S.A.; Mohamed, M.A.; Annuk, A. SPSO Based Optimal Integration of DGs in Local Distribution Systems under Extreme Load Growth for Smart Cities. *Electronics* **2021**, *10*, 2542. [CrossRef]
86. Megahed, N.A.; Abdel-Kader, R.F. Smart Cities after COVID-19: Building a conceptual framework through a multidisciplinary perspective. *Sci. Afr.* **2022**, *17*, e01374. [CrossRef]
87. 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.
88. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.-K.R.; Zomaya, A. Blockchain for smart communities: Applications, challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *144*, 13–48. [CrossRef]
89. Al Sadawi, A.; Madani, B.; Saboor, S.; Ndiaye, M.; Abu-Lebdeh, G.J. A comprehensive hierarchical blockchain system for carbon emission trading utilizing blockchain of things and smart contract. *Technol. Forecast. Soc. Chang.* **2021**, *173*, 121124. [CrossRef]
90. Zia, M. B-DRIVE: A blockchain based distributed IoT network for smart urban transportation. *Blockchain Res. Appl.* **2021**, *2*, 100033. [CrossRef]
91. Pournaras, E. Proof of witness presence: Blockchain consensus for augmented democracy in smart cities. *J. Parallel Distrib. Comput.* **2020**, *145*, 160–175. [CrossRef]
92. Iqbal, M.M.; Waseem, M.; Manan, A.; Liaqat, R.; Muqeet, A.; Wasaya, A. IoT-Enabled Smart Home Energy Management Strategy for DR Actions in Smart Grid Paradigm. In Proceedings of the 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST), Islamabad, Pakistan, 12–16 January 2021; pp. 352–357.
93. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A survey of denial-of-service attacks and solutions in the smart grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]
94. Huseinovic, A.; Mrdovic, S.; Bicakci, K.; Uludag, S. A taxonomy of the emerging Denial-of-Service attacks in the smart grid and countermeasures. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; pp. 1–4.
95. Du, D.; Li, X.; Li, W.; Chen, R.; Fei, M.; Wu, L. ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1698–1711. [CrossRef]
96. Valliammai, A.; Bavatharinee, U.; Shivadharshini, K.; Hemavathi, N.; Meenalochani, M.; Sriranjani, R. A Comprehensive Study on Distributed Denial of Service Attacks in Internet of Things Based Smart Grid. In Proceedings of the International Conference on Intelligent Data Communication Technologies and Internet of Things, Coimbatore, India, 12–13 September 2019; pp. 685–691.
97. Raja, D.J.S.; Sriranjani, R.; Parvathy, A.; Hemavathi, N. A Review on Distributed Denial of Service Attack in Smart Grid. In Proceedings of the 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 22–24 June 2022; pp. 812–819.
98. Holik, F.; Flå, L.H.; Jaatun, M.G.; Yayilgan, S.Y.; Foros, J. Threat modeling of a smart grid secondary substation. *Electronics* **2022**, *11*, 850. [CrossRef]
99. Acarali, D.; Rao, K.R.; Rajarajan, M.; Chema, D.; Ginzburg, M. Modelling smart grid IT-OT dependencies for DDoS impact propagation. *Comput. Secur.* **2022**, *112*, 102528. [CrossRef]
100. Mukherjee, D.; Chakraborty, S.; Ghosh, S. Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids. *Electr. Eng.* **2022**, *104*, 259–282. [CrossRef]
101. Yan, J.-J.; Yang, G.-H.; Wang, Y. Dynamic Reduced-Order Observer-Based Detection of False Data Injection Attacks With Application to Smart Grid Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6712–6722. [CrossRef]
102. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts. *Renew. Sustain. Energy Rev.* **2022**, *163*, 112423. [CrossRef]
103. Mahi-Al-rashid, A.; Hossain, F.; Anwar, A.; Azam, S. False data injection attack detection in smart grid using energy consumption forecasting. *Energies* **2022**, *15*, 4877. [CrossRef]
104. Wang, S.; Bi, S.; Zhang, Y.-J.A. Locational detection of the false data injection attack in a smart grid: A multilabel classification approach. *IEEE Internet Things J.* **2020**, *7*, 8218–8227. [CrossRef]
105. Deng, R.; Liang, H. False data injection attacks with limited susceptance information and new countermeasures in smart grid. *IEEE Trans. Ind. Inform.* **2018**, *15*, 1619–1628. [CrossRef]
106. Nafees, M.N.; Saxena, N.; Cardenas, A.; Grijalva, S.; Burnap, P. Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. *ACM Comput. Surv.* **2022**. [CrossRef]
107. Kimani, K.; Oduol, V.; Langat, K. Cyber security challenges for IoT-based smart grid networks. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 36–49. [CrossRef]
108. Gunduz, M.Z.; Das, R. Analysis of cyber-attacks on smart grid applications. In Proceedings of the 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, 28–30 September 2018; pp. 1–5.
109. Le, T.D.; Anwar, A.; Loke, S.W.; Beuran, R.; Tan, Y. Gridattacksim: A cyber attack simulation framework for smart grids. *Electronics* **2020**, *9*, 1218. [CrossRef]

110. Zheng, L.; Gao, T.; Zhang, X. Security protection and testing system for cyber-physical based smart power grid. In Proceedings of the PURPLE MOUNTAIN FORUM 2019-International Forum on Smart Grid Protection and Control; Springer: Singapore, 2020; pp. 847–857.
111. Abdullah, H.I.M.; Mustaffa, M.Z.; Rahim, F.A.; Ibrahim, Z.-A.; Yusoff, Y.; Yussof, S.; Bakar, A.A.; Ismail, R.; Ramli, R. Smart grid digital forensics investigation framework. In Proceedings of the 2020 8th International Conference on Information Technology and Multimedia (ICIMU), Selangor, Malaysia, 24–26 August 2020; pp. 200–205.
112. Xu, K.; Wang, X.; Xu, H.; Dong, N.; Han, M.; Zhou, X. A vulnerability scanning scheme based on attack graph for smart grid industrial control system. *IOP Conf. Ser. Earth Environ. Sci.* **2021**, *645*, 012060. [CrossRef]
113. Faquir, D.; Chouliaras, N.; Sofia, V.; Olga, K.; Maglaras, L. Cybersecurity in smart grids, challenges and solutions. *AIMS Electron. Electr. Eng.* **2021**, *5*, 24–37.
114. Akbanov, M.; Vassilakis, V.G.; Logothetis, M.D.J. Ransomware detection and mitigation using software-defined networking: The case of WannaCry. *Comput. Electr. Eng.* **2019**, *76*, 111–121. [CrossRef]
115. Kuznetsov, A.; Kavun, S.; Smirnov, O.; Babenko, V.; Nakisko, O.; Kuznetsova, K. Malware correlation monitoring in computer networks of promising smart grids. In Proceedings of the 2019 IEEE 6th International Conference on Energy Smart Systems (ESS), Kyiv, Ukraine, 17–19 April 2019; pp. 347–352.
116. Shaaban, A.R.; Abdelwanees, E.; Hussein, M. Distributed Denial of Service Attacks Analysis, Detection, and Mitigation for the Space Control Ground Network: DDoS attacks analysis, detection and mitigation. *Proc. Pak. Acad. Sci. A Phys. Comput. Sci.* **2020**, *57*, 97–108.
117. Sairam, V.; Kumar, M. Counter attacks as self-defense. *Int. J. Sci. Res. Eng. Trends* **2019**, *5*, 976–981.
118. Toapanta, S.M.T.; Gallegos, L.E.M.; Morán, M.J.C.; Rojas, J.G.O. Analysis of models of security to mitigate the risks, vulnerabilities and threats in a company of services of telecommunications. In Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 9–12 March 2020; pp. 445–450.
119. Neves, R.H.; Silva, A.A.; Gava, V.; Azevedo, M.T.; Sandoval, J.F.; Oliveira, F.S.; Guelfi, A.E.; Kofuji, S.T. DoS Attack on SDN: A study on control plane strategies in-band and out-of-band. *Res. Sq.* 2022, *preprint*.
120. Zeng, Z.; Li, Y.; Cao, Y.; Zhao, Y.; Zhong, J.; Sidorov, D.; Zeng, X. Blockchain Technology for Information Security of the Energy Internet: Fundamentals, Features, Strategy and Application. *Energies* **2020**, *13*, 881. [CrossRef]
121. Khan, M.A.; Saleh, A.M.; Waseem, M.; Sajjad, I.A. Artificial Intelligence Enabled Demand Response: Prospects and Challenges in Smart Grid Environment. *IEEE Access* **2023**, *11*, 1477–1505. [CrossRef]
122. Guan, Z.; Zhang, Y.; Zhu, L.; Wu, L.; Yu, S. EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid. *Sci. China Inf. Sci.* **2019**, *62*, 32103. [CrossRef]
123. Agarkar, A.; Agrawal, H. A review and vision on authentication and privacy preservation schemes in smart grid network. *Secur. Priv.* **2019**, *2*, e62. [CrossRef]
124. Sureshkumar, V.; Anandhi, S.; Amin, R.; Selvarajan, N.; Madhumathi, R. Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication. *IEEE Syst. J.* **2020**, *15*, 3565–3572. [CrossRef]
125. Almasarani, A.; Majid, M. 5G-Wireless sensor networks for smart grid-accelerating technology's progress and innovation in the kingdom of Saudi arabia. *Procedia Comput. Sci.* **2021**, *182*, 46–55.
126. Nguyen, T.N.; Liu, B.-H.; Nguyen, N.P.; Chou, J.-T. Cyber security of smart grid: Attacks and defenses. In Proceedings of the ICC 2020-2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
127. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [CrossRef]
128. Sundararajan, A.; Hernandez, A.S.; Sarwat, A.I. Adapting big data standards, maturity models to smart grid distributed generation: Critical review. *IET Smart Grid* **2020**, *3*, 508–519. [CrossRef]
129. Mir, A.W.; Ramachandran, R.K. Security gaps assessment of smart grid based SCADA systems. *Inf. Comput. Secur.* **2019**, *27*, 434–452. [CrossRef]
130. Annor-Asante, M.; Pranggono, B. Development of smart grid testbed with low-cost hardware and software for cybersecurity research and education. *Wirel. Pers. Commun.* **2018**, *101*, 1357–1377. [CrossRef]
131. Kisielewicz, T.; Stanek, S.; Zytniewski, M. A Multi-Agent Adaptive Architecture for Smart-Grid-Intrusion Detection and Prevention. *Energies* **2022**, *15*, 4726. [CrossRef]
132. Rafique, Z.; Khalid, H.M.; Muyeen, S. Communication systems in distributed generation: A bibliographical review and frameworks. *IEEE Access* **2020**, *8*, 207226–207239. [CrossRef]
133. 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]
134. 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]
135. Inayat, U.; Zia, M.F.; Mahmood, S.; Khalid, H.M.; Benbouzid, M. Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects. *Electronics* **2022**, *11*, 1502. [CrossRef]
136. Waseem, M.; Lin, Z.; Liu, S.; Zhang, Z.; Aziz, T.; Khan, D. Fuzzy compromised solution-based novel home appliances scheduling and demand response with optimal dispatch of distributed energy resources. *Appl. Energy* **2021**, *290*, 116761. [CrossRef]

137. Biswas, S.; Sharif, K.; Li, F.; Maharjan, S.; Mohanty, S.P.; Wang, Y. PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain. *IEEE Internet Things J.* **2020**, *7*, 2343–2355. [CrossRef]
138. Waseem, M.; Lin, Z.; Liu, S.; Jinai, Z.; Rizwan, M.; Sajjad, I.A. Optimal BRA based electric demand prediction strategy considering instance-based learning of the forecast factors. *Int. Trans. Electr. Energy Syst.* **2021**, *31*, e12967. [CrossRef]
139. Aziz, T.; Lin, Z.; Waseem, M.; Liu, S. Review on optimization methodologies in transmission network reconfiguration of power systems for grid resilience. *Int. Trans. Electr. Energy Syst.* **2021**, *31*, e12704. [CrossRef]
140. Waseem, M.; Sajjad, I.A.; Haroon, S.S.; Amin, S.; Farooq, H.; Martirano, L.; Napoli, R. Electrical Demand and its Flexibility in Different Energy Sectors. *Electr. Power Compon. Syst.* **2020**, *48*, 1339–1361. [CrossRef]
141. Kim, S.; Kwon, Y.; Cho, S. A Survey of Scalability Solutions on Blockchain. In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 17–19 October 2018; pp. 1204–1207.
142. Wood, E. A Secure Decentralised Generalised Transaction Ledger, Ethereum Proj. *Yellow Pap.* **2014**, *151*, 1–32.
143. Jabbar, A.; Dani, S. Investigating the link between transaction and computational costs in a blockchain environment. *Int. J. Prod. Res.* **2020**, *58*, 3423–3436. [CrossRef]
144. Michelin, R.A.; Dorri, A.; Steger, M.; Lunardi, R.C.; Kanhere, S.S.; Jurdak, R.; Zorzo, A.F. SpeedyChain: A framework for decoupling data from blockchain for smart cities. In Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: Computing, networking and services, New York, NY, USA, 5–7 November 2018; pp. 145–154.
145. Huang, J.; Kong, L.; Chen, G.; Wu, M.-Y.; Liu, X.; Zeng, P. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3680–3689. [CrossRef]
146. Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K.-K.R. Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access* **2019**, *7*, 176935–176951. [CrossRef]
147. Kang, J.; Xiong, Z.; Niyato, D.; Ye, D.; Kim, D.I.; Zhao, J. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2906–2920. [CrossRef]
148. Goudarzi, A.; Fahad, S.; Ni, J.; Ghayoor, F.; Siano, P.; Haes Alhelou, H. A sequential hybridization of ETLBO and IPSO for solving reserve-constrained combined heat, power and economic dispatch problem. *IET Gener. Transm. Distrib.* **2022**, *16*, 1930–1949. [CrossRef]
149. Goudarzi, A.; Zhang, C.; Fahad, S.; Mahdi, A.J. A hybrid sequential approach for solving environmentally constrained optimal scheduling in co-generation systems. *Energy Rep.* **2021**, *7*, 3460–3479. [CrossRef]
150. Fahad, S.; Goudarzi, A.; Li, Y.; Xiang, J. A coordination control strategy for power quality enhancement of an active distribution network. *Energy Rep.* **2022**, *8*, 5455–5471. [CrossRef]
151. Fahad, S.; Goudarzi, A.; Xiang, J. In From Grid Feeding to Grid Supporting Converters: A Constant Power Active Distribution Network Perspective. In Proceedings of the 2020 IEEE 29th International Symposium on Industrial Electronics (ISIE), Delft, The Netherlands, 17–19 June 2020; pp. 862–867.