Review

Survey on Blockchain for Smart Grid Management, Control, and Operation

Yohannes T. Aklilu [1],[†] and Jianguo Ding [2],[*],[†]

1   School of Engineering Sciences, University of Skövde, 54128 Skövde, Sweden; yohannes.tadesse.aklilu@his.se
2   Department of Computer Science, Blekinge Institute of Technology, 37179 Karlskrona, Sweden
*   Correspondence: jianguo.ding@bth.se; Tel.: +46-0455-385756
†   These authors contributed equally to this work.

Abstract: Power generation, distribution, transmission, and consumption face ongoing challenges such as smart grid management, control, and operation, resulting from high energy demand, the diversity of energy sources, and environmental or regulatory issues. This paper provides a comprehensive overview of blockchain-based solutions for smart grid management, control, and operations. We systematically summarize existing work on the use and implementation of blockchain technology in various smart grid domains. The paper compares related reviews and highlights the challenges in the management, control, and operation for a blockchain-based smart grid as well as future research directions in the five categories: collaboration among stakeholders; data analysis and data management; control of grid imbalances; decentralization of grid management and operations; and security and privacy. All these aspects have not been covered in previous reviews.

**Keywords:** smart grid; blockchain; smart grid management; smart grid control and operation

1. Introduction

1.1. Smart Grid Architecture

With more and more applications and technological advances, IoT and other power-operated devices are on the rise. To meet the energy demand, numerous small- and large-scale power generation and distribution solutions have been tested worldwide. In addition, the demand for sustainable and renewable energy in all sectors of society is forcing power generation to be versatile. The requirements for a future energy system are also driven by three key principles—Decarbonization, Decentralization, and Digitalization [1]—that ultimately provide the framework for the European Commission's Energy Union Package [2]. The emergence of low-voltage power generation and distribution systems leads to the concept of Internet of Energy (IoE) [3]. The development of IoE has several advantages. It promotes energy generation, distribution, and consumption while meeting the energy demand via smart and automated tools that ensure secure data exchange among stakeholders [4]. The IoE is designed as an open network, which means that all energy sources are equally important [5].

According to the system model proposed by the National Institute of Standards and Technology (NIST) [6], a smart grid domain is a higher-level grouping of organizations, buildings, people, systems, devices, or other actors that share similar goals to exchange, store, process, and handle information needed in the smart grid. The domains of the smart grid include generation, transmission, distribution, consumption, operation, service provider, and market. An overview of the interaction between the different smart grid domains that is extracted from [6] is shown in Figure 1. The generation domain is responsible for energy production using various resources. The service providers control the energy flow and are responsible for energy distribution, operation, and trading. Customers refer to the various Advanced Metering Infrastructures (AMI), automation stations, demand

response, smart appliances, sensors, smart objects, supervisory control and data acquisition (SCADA), electric vehicles, and home energy management [7].
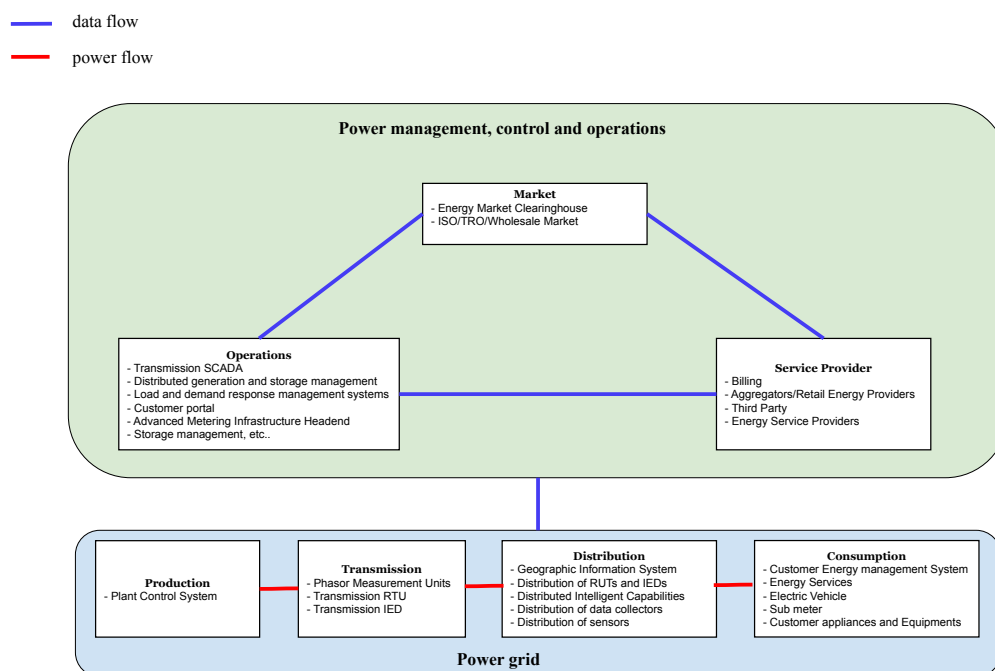
Figure 1. An overview of stakeholders in the different smart grid domains.

The AMI collects, measures, and analyzes energy consumption by enabling bidirectional communication between the utility and the consumer. It consists of three main components: smart meters, the AMI center, and the communication network. Smart meters are devices that record and monitor electricity consumption and transmit real-time data to the AMI center. The AMI center is a server responsible for data management systems. Various communication protocols are used between the household appliances, smart meters, and the AMI center [8].

The SCADA system operates energy systems by measuring, controlling, and monitoring the power grid. The main features of the smart power grid are real-time control, operational efficiency, increased grid stability, and seamless integration with new distributed database technologies as well as renewable energy systems. Smart grids can also be divided into locally managed microgrid infrastructures that deliver emission-free energy and are less dependent on centralized energy sources and high-voltage governmental or corporate-based power units.

Six main requirements have been identified for the smart grid to become intelligent [9]: (1) control of consumer information that enables consumers to have reliable and frequent information about their electricity consumption, (2) accommodation and production technologies that enable a balance between supply and demand, (3) an economic exchange market that enables local market prices and promotes local microgrid production, (4) the prospect of quality energy by diagnosing voltage fluctuations, (5) technical and operational specifications that ensure operational optimization, and (6) security against vulnerabilities that ensure resistance to various types of attackers. The development and implementation of the smart grid have immensely improved the efficiency of management, control, and operation of the power grid and facilitated the integration of renewable energy sources, electric vehicles, bidirectional communication, automated and self-maintaining systems that involve consumers [10].

The current trend toward the development and expansion of microgrids makes centrally controlled intelligent grid management, control, and operation obsolete and difficult

to implement. Fossil-free energy generation and distribution vary depending on weather, energy sources, geographic locations, existing infrastructure, and energy demand, among other factors. These variations and the decentralization of the energy system require modern and flexible management and operation systems as well as innovative energy storage systems [11]. It is also important to understand how to balance power generation and distribution in line with demand across seasons. The length of power lines accounts for a large portion of energy losses. Microgrid and renewable infrastructure generation and distribution can drastically minimize this energy loss while protecting the environment [12]. The introduction of the electricity market can be a motivating factor for the expansion of microgrid production, as it could increase the revenue of the generator while minimizing its consumption costs [13]. The challenge is to establish coordinated and systematically automated production and distribution controls of these microgrids as the number of prosumers increases. The available technologies and achievements of the energy sector are not suitable for microgrids, and therefore, many actors in the energy industry propose blockchain [14] to manage power transactions in microgrids with the aim of promoting local consumption of distributed generation, decentralizing grid management, and P2P power trading [13].

1.2. Potential Extension of Smart Grid

Distributed renewable energy sources are in high demand to address the challenges of climate change while efficiently balancing the production, distribution, transmission, and consumption of energy. With a variety of alternative energy sources, most fuel-based devices can be electrified, minimizing long-distance transmission losses, carbon emissions, and pollution [4,15]. Today, small generators and energy storage systems are increasingly connected to the traditional electric grid. The most common energy sources have been fossil fuels and hydro-power, requiring large investment at the state or corporate level. Technological advances in recent decades are opening windows of opportunities for low-voltage renewable electricity generation by private and small businesses. For example, in Sweden, there are a total of 65,819 solar panels and 4333 wind turbines installed in the year 2020, representing an increase in annual renewable energy generation by approximately 40% from 2016 [16]. These numbers are expected to grow rapidly in the coming years as the Swedish government plans to use 100% renewable energy by 2040. The generation and distribution of decentralized emission-free low-voltage energy is highly recommended and can complement the traditional power sources. The 2030 renewable energy targets that have already been incorporated into official policy by 87 governments around the world aim at building an estimated 721 gigawatts of new capacity in wind, solar, and other non-hydro renewable energy technologies over the next decade [17].

The coordination and integration of a large number of energy sources could pose a particular challenge to highly regulated, traditional, and centralized energy systems. The transition to a decentralized architecture can modernize the energy management and operation as well as the control and monitoring of the integration and automation process, which are still lacking [18]. Various research has highlighted the challenges in protecting microgrid systems during operation, power balancing, and communication between different distributed generation (DG) units such as wind turbines, coal, photovoltaic systems, biomass, hydro-power, fuel cells, etc. [19]. Therefore, it is desirable to integrate microgrid generation and distribution along with conventional power grids in order to create a common and efficient data exchange mechanism.

1.3. Blockchian-Based Smart Grid

Blockchain technology, with its decentralized and secure platform for information exchange as its main feature, can be an interesting example of unifying information exchange among different actors. The application of blockchain in the energy sector is still in its infancy and has a short history of development [5]. However, there is a growing interest with some research reports, application scenarios, and project initiatives in recent

years [1,4,11,12,20–28]. Some blockchain-based frameworks have also been proposed with a particular focus on energy trading for microgrids [13] and a distributed energy market for pricing [29]. Ethereum-based energy trading using information transactions between smart meters in households and distribution system operators (DSOs) has also been proposed [23]. In addition, wireless sensor networks (WSNs) and the Internet of Things (IoT) provide alternative solutions to privacy and security problems through efficient data aggregation and the optimization of energy generation and consumption using smart systems that can monitor and interact with each other [20]. A common platform for smart grid management, operation, and control is needed for the highly diversified energy sector. Proper communication between the different DG units that are connected to the main grid and proper connection contributes to better smart grid performance [19,30]. Communication between DG units is essential for monitoring the voltage and frequency of the microgrid.

This article provides a systematic review of blockchain-based applications for smart grid management, control, and operation. We summarize existing work on the use of blockchain technology in various smart grid domains. The survey focuses particularly on the five key challenges in the smart grid domain. These are (1) collaboration among stakeholders, (2) data analysis and data management, (3) control of grid imbalances, (4) decentralization of grid management and operations, and (5) security and privacy. As far as we know, there has been no systematic research study on blockchain applications for smart grid management, control, and operation. This article aims to fill this gap by providing a comprehensive overview of the topic and highlighting the need for implementing blockchain systems to support infrastructure in controlling, automating, and securing the decentralized application of smart grids.

The main contributions of this paper are as follows:

(1) A systematic overview of the challenges in the current management, control, and operation of smart grids.
(2) A comprehensive overview of the various applications of blockchain for smart grid management, control, and operation, with particular emphasis on the following

- How Blockchain can be used to facilitate collaboration between stakeholders, coordinating power generation, distribution, and automate asset verification.
- The secure and efficient management, analysis, and transfer of data from various advanced metering infrastructures.
- Blockchain applications and implementation for grid imbalance control (frequency and voltage regulation), decentralization of grid management and operations, data access control, security, and privacy for smart grids.

(3) Future research and development directions.

This paper is organized as follows. Section 2 discusses the challenges of smart grid management, control, and operation. Section 3 provides an overview of blockchain and its relevant features. Section 4 discusses the various proposed implementation mechanisms of blockchain for the smart grid. Several proposed blockchain-based applications for smart grid management, control, and operation are reviewed. The section provides also a summary of the different survey articles published in recent years together with an overview of traditional and blockchain-based smart grid applications. Section 5 provides a discussion and further research directions, and a conclusion is presented in Section 6.

2. Challenges for Management, Control, and Operations on Smart Grid

The smart grid currently works with a centralized platform or intermediaries to provide services such as billing, monitoring, bidding, and energy transmission. Although these solutions are mature and work properly, some of the challenges that are related to the current smart grid promote the integration of a large number of smart grids with renewable energy generators and Cyber-Physical Systems. The smart grid is also transforming to a decentralized topology with centralized management and interactive network using IoE (Internet of Energy) [3]. In this new IoE concept, each device is assigned certain attributes

based on an identifier, geographic marker, address, bid price, and offer price based on its requirements. The introduction of these new technologies along with the diversity and expansion of energy sources, complicates the management, control, and operation of the energy sector. We discuss these challenges in detail based on five categories; see Figure 2.
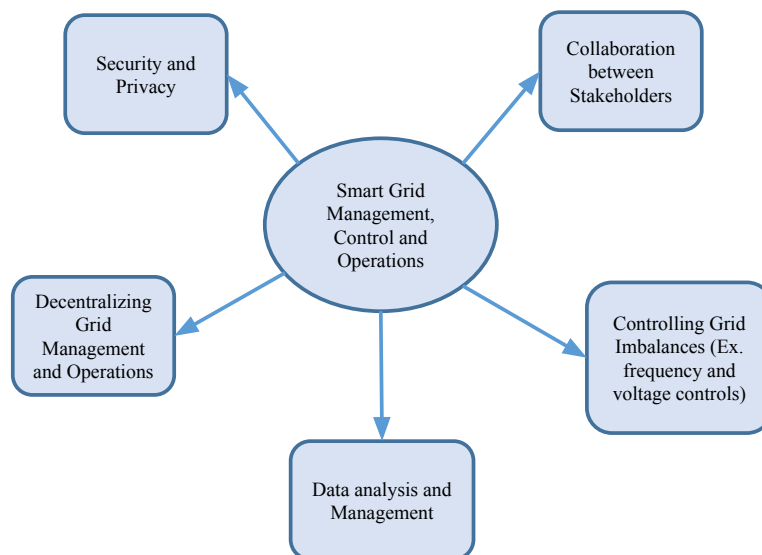
Figure 2. Challenges for management, control, and operation of smart grid.

2.1. Collaboration between Stakeholders

New technologies, high investments, lack of accurate information, etc. complicate the coordination between actors in the energy sector. The current smart grid system faces the problem of energy balancing, especially when different actors are involved in the processes of generation, distribution, trading, and consumption. While much of the literature focuses on the technical aspects of the smart grid challenges, the collaboration between stakeholders is equally important and needs to be properly addressed [25]. Energy suppliers and traders typically request an estimated amount of energy from generators based on their demand analysis. Such an estimate can be inaccurate due to several factors: expansion of the region, population growth, environmental factors, and increase in microgrid generators in the area. This can lead to high distribution losses, unbalanced voltage and frequency loads, and consequent power outages. In addition, some microgrids, such as solar systems, produce more energy during the warm summer months when energy demand is lowest. A modern data exchange system between the stakeholders could pave the way to store the excess produced energy in a local hydrogen gas or battery without affecting the main grid infrastructure. Therefore, it is important to establish close cooperation between relevant players such as generators, distributors, retailers, consumers, and regulators to facilitate grid management.

2.2. Controlling Grid Imbalance

Both physical and technical problems can contribute to imbalances in power generation and consumption. The failure of some network components, such as insulation faults or damaged cables, interference from third parties, vandalism, and natural causes such as wind or storms can contribute to imbalances in power supply. Technical problems such as malicious attacks, frequency deviations, overloads, synchronization losses, and voltage dips can also contribute to power imbalances [9]. Voltage deviations are another potential challenge to grid imbalances. For example, a PV power plant produces more energy during the sunny part of the day when demand is lower. This causes the PV power plant to produce more than the grid load capacity and causes Reverse Power Flow into the transmission grid [31–34]. Therefore, it is essential to control and monitor the power supply in each

period. The article [35] examined the emerging challenges for voltage control in the smart grid. All stakeholders need to adjust their power generation, distribution, and consumption to regulate both active and reactive power [9]. However, this becomes a challenge due to the number and diversity of power generation methods and regulatory requirements.

2.3. Data Analysis and Management

Current smart grid data management faces the problem of data aggregation quality, security, compliance control, common scope, and efficiency of the management mechanism [36]. A large amount of data are generated and transferred between different entities [25]. Accurate and consistent incoming data streams such as weather forecasts and power generation status allow operators to control and monitor the grid system. Such information is very important to avoid sudden and unexpected power supply disruptions. In addition, such big data can also be used for grid operations, alarms, demand forecasts, generation estimates, price adjustments, etc. The data collected tend to be quite large, as multiple smart grid domains are involved in the process. For example, an Advanced Metering Infrastructure that collects data every 10 min instead of every month could increase the data analysis process by more than 4000 times. There is also a regulatory requirement to provide accurate data as frequently as possible, which is challenging. Modern, automated, and secure data processing technology can improve data management, storage, and reporting for the smart grid.

2.4. Decentralizing Grid Management and Operation

Decentralizing grid operations allows stakeholders to control and manage their data locally. The control and operation of a smart grid in a decentralized environment is an important research topic. Demand-side control and optimized operation of the grid are a research area [37]. Distributed automation devices are used to decentralize the operation of the grid. These are devices such as phasor management units (PMUs), remote terminal units (RTUs), SCADA, and smart meters that are used to collect and monitor data. In [10], distributed automation approaches for electric power distribution systems, benefits, and challenges were studied. High-resolution sensors with the ability to report real-time conditions and improve the visibility of the distribution system operator beyond substation assets were also considered. In addition, there are challenges associated with the coordinated and cost-effective integration of distributed smart grid systems, generation assets, and demand response facilities. This complicates the management and operation of distributed energy resources. Further work is needed to facilitate coordination between decentralized and centralized stakeholders.

2.5. Security and Privacy

While decentralizing the operation and management of the smart grid has many benefits, it also brings security and privacy challenges. The SCADA module in modern power systems collects data at remote terminals, transmits, and stores it in plain text to the main control center. This centralized data collection and storage is highly vulnerable to cyberattacks. Cybersecurity is one of the biggest and most difficult challenges facing the current smart grid. Over the years, several cyberattacks have taken place on the smart grid [38]. Attackers use the four steps of Exploration, Scanning, Exploitation, and Maintaining Access [39] to control the system. There are several known attacks on smart grids. One of them is the jabbing attack, in which the attacker installs a malicious smart power meter that sends false data, causing desynchronization and power interruption. The puppet attack sends a signal to the node. Then, the attacker controls the node and sends more signals into the network, causing the smart meter network to become unstable. Another example is the stack smashing attack, which compromises the application layer of the network and leads to the disclosure of sensitive data. An experimental attack, on the other hand, makes the smart grid layer vulnerable to DoS attacks [40]. A comprehensive discussion of attack mechanisms, detection, and countermeasures can be found in [7].

Therefore, security is a major challenge in the management, control, and operation of smart grids. Given the alarming increase in IoT devices with limited security capabilities connected to the smart grid system, much needs to be done to protect sensitive personal and corporate data as well as national security [38].

2.6. Summary of the Challenges for the Current Smart Grid Management, Control, and Operation

In summarizing the challenges of smart grid management, control, and operation, several technical and operational changes can be identified. The dynamic generation and distribution of energy by a large number of distributed generators, the digitization of the grid, and advanced metering systems contribute to fault-tolerant transmission and distribution control. Smart grid owners often have dual roles (generator and consumer), and loads become dynamic and more interactive [22]. Centralized and traditional grid management and operation face challenges, and utilities are seeking viable solutions to these problems. Although distributed energy systems offer benefits such as user tracking, cost savings, and optimized resource allocation [5], technological immaturity and incentive mechanisms compromise the core interests of stakeholders. Table 1 summarizes the challenges for smart grid management, control, and operation.

Table 1. Challenges on the current and future smart grids.

Challenges	Description	Ref.
Collaborations between stakeholders	• Difficulty in allocating resources • Difficulty in establishing reliable data exchange for common goals • Operational challenges due to the dynamics of renewable energy generation • Problems in developing an up-to-date supply and demand program • Limited role or influence of microgrid generators on the management and operation of the smart grid • Problems with real-time performance • High transaction costs • Microgrid generators' voices may be dominated by large energy companies • Difficulty in getting prosumers to participate in decentralized smart grid management • Overcoming regulatory challenges • Transparency • Accountability	[25,30]
Controlling grid imbalances	• Need to monitor smart grid sensors and AMI to control grid overloads and power outages. • Problem of overloading the grid • Load balancing in the grid • Can create Reverse Power Flow • Control of voltage and frequency • Automatic fault detection and maintenance	[9,31–35]
Data analysis and management	• Analyzing the quality of produced energy • Large-scale and complex data aggregation and deployment • Data management on energy production, distribution, and consumption • Management of data transactions between all prosumers	[25,36]
Decentralizing gird management and operations	• Development of a decentralized energy management • Automated P2P energy trading • Automated grid monitoring • Increase in the complexity of energy generation and distribution • Flexibility of energy generation and distribution • Difficulty of scalability • Traceable energy management	[10,37,41]
Security and privacy	• Tamper-proof system for protecting customer data recorded and transmitted in the smart grid • Access control • Authentication • Secure data storage • Security and data protection for smart grids • Data protection and compliance • Establishing secure communications • Protecting the smart grid from cyber attacks • Implementing a decentralized and secure authentication mechanism • Data privacy	[7,25,38,39]

3. Blockchain

While this technology has been around since the 1990s, it has attracted a great deal of interest since Nakomoto published a paper titled "Bitcoin: A Peer to Peer Electronic Cash System" [42]. The paper describes a peer-to-peer electronic transaction between two parties (sender and receiver) without an intermediary financial institution. Since then, the technology has been used for electronic money transactions as well as various other non-financial areas. E-commerce systems such as Bitcoin, Ethereum, Ripple, and Litcoin are some of the popular blockchain applications that are expanding to the financial market and attracting millions of users [43].

The exact definition of blockchain technology differs depending on the desired function and specific implementation. It uses concepts such as cryptography, distributed ledgers, and consensus, among others. However, it is important to emphasize that not all systems with cryptographic implementations can be associated with blockchain and not all distributed ledgers can necessarily be used for the cryptographic functions associated with blockchain [44]. Blockchain is a collection of technologies including fault-tolerant consensus algorithms, smart contracts, public-key cryptography, peer-to-peer networks, and database management technologies that together form a low-cost, secure, and efficient operational management system [24]. Each block is encrypted and linked to the previous one after going through validation and consensus decision processes. There is no limit to the number of blocks in the chain, and this makes it harder to invalidate older blocks. Anyone on the network can view or modify the data without a centralized institution taking responsibility for recording the activity. Blockchain technology is commonly used for (1) a specific cryptographically patched and continuously growing timestamped database, (2) the distributed digital consensus architectures that the database enables, and (3) the application domains that build on that architecture [44].

A typical blockchain transaction can be divided into three phases. (1) First, there is the transaction request, where a node requests the creation of a block by sending data with a specific value to another node within the network. In this phase, a hash code is generated and distributed to all network nodes. (2) All nodes within the network verify the validity of this block based on a previously established consensus mechanism. (3) A node that makes a real effort and finds the correct hash value is awarded as the winner and thus is entitled to add the latest block to the chain.

A blockchain architecture consists of a chain of blocks connected by hash codes that not only serve as IDs but also ensure the integrity of the blocks [45]. Each block consists of a block header, which includes hash values of the previous block header, a timestamp, a nonce, and a hash of the Merkel tree containing a set of transactions in the block. Blockchain security is based on public-key cryptography, followed by hash functions for attack resistance, double spending prevention, and digital signatures for agreement approval and consensus.

Blockchain applications in the financial sector and beyond are being enhanced daily by a number of other technologies that have adopted the technology to save time and money. Industry and enterprise-level systems are implementing blockchain to make their existing system more efficient by minimizing the centralized mediation of data transactions and controls [44]. Retailers such as Walmart and Maersk are using blockchain to track everything from food production to packaging, shipping, distribution, and sales [46]. That is, instead of the manufacturer, the shipper, and other stakeholders collect their own records of the product, blockchain could allow all parties to followup every step in a secure ledger.

3.1. Blockchain Features

Blockchain has good characteristics [4,45,47].

- Decentralization: The blockchain is managed by various decentralized nodes through a consensus protocol and operates on a peer-to-peer basis without the need for authorized and centralized trusted nodes.

- Scalability: As more and more nodes can join the network, the blockchain network can be expanded at will.
- Untrusted but secure: Nodes do not rely on trusted intermediaries for communication, and all records/transactions are protected by asymmetric cryptography. The blockchain does not require blind trust in specific entities.
- Immutability: Unless the majority becomes malicious, the content of the block cannot be changed.
- Transparency and verifiability: The nodes of the network can verify the authenticity of the records and ensure that the blocks are not modified. By opening all records to anyone, transparency allows these blocks to be verified by any node on the network.
- Resilience: Any failure or malicious activity can be easily detected and recovered. This flexibility comes from the decentralization of the architecture avoiding single point of failure. All nodes store their entire chain on their premises.

These features make blockchain a modern distributed network protocol that enables relationships between different participants who do not know each other. The technology is particularly promising in industries where peer networks, such as grid-connected power generators and consumer networks, rely on shared data sets. The power distribution system can also use blockchain to remotely control the power flowing into a given area by monitoring production and consumption statistics.

3.2. Types of Blockchain

Different classifications of blockchain can be found in the literature based on access and validation rights, application environments, docking types, and application range [5]. Based on access and management rights, blockchain can be divided into permissionless and permissioned.

3.2.1. Permissionless Blockchain

In permissionless (or public) blockchain, anyone can join or leave the network at will [48], and any node can participate in transactions as well as consensus processes [1]. In this system, the number of nodes is often large, anonymous, and untrusted. Trust and collaboration between users in the public blockchain are governed by cryptographic puzzles. Systems such as Bitcoin and Ethereum are some examples of public blockchains [42,49]. Some use cases are digital identities, voting, fundraising, etc.

Permissionless blockchain has attracted a lot of interest in the wake of Bitcoin [42] and other digital currencies that sought to decentralize products and services without intermediary third parties. As a result of its ability to store and exchange data irrevocably, industries such as retail and financial institutions have recognized the potential of this technology [48]. For example, if there is a blockchain with information describing the history of a car from production to sale and subsequent services to use, people would prefer to rely on that information rather than the intermediary of the car. However, the system is quite slow. It is difficult to generate items of value. Security depends on the integrity of users. It is too transparent to keep sensitive data. Access is difficult to control. It is vulnerable to hacking and tampering. It consumes a lot of energy, and it is quite complex. Due to these limitations, consent-free blockchain is unsuitable for regulatory communication and smart grid management [24].

3.2.2. Permissioned Blockchain

Permissioned blockchain is designed so that only authorized participants can access the ledgers. Anyone can join the network, but the consensus algorithm is run by a group of nodes that perform the necessary validation. With permissioned blockchain, no incentives are required. Users can determine the level of privacy, decentralization, and management. This system may be suitable for organizations such as the public sector and financial institutions that have a large volume of sensitive data and a number of supporting regulations. For example, a permissioned blockchain can be set up between organizations where certain

counterparties can record transactions in the distributed ledger, but not everyone can read what is written in the ledger [48]. This can provide resilience and redundancy of data storage. The system is typically fast, highly customizable, energy efficient, more flexible, and can be easily adapted to meet current regulations. However, these advantages come at the cost of immunity and censorship. They are also centralized, less transparent, and less anonymous [1]. Furthermore, permissioned blockchains can be divided into private and consortial blockchains based on the levels of node access and validation, respectively.

Private Blockchain is designed so that only authorized participants can access the ledgers. All data in the private blockchain are approved centrally by a specially authorized group, which also sets the access rights in the system. Private blockchain does not need to be transparent, as data access is limited only to authorized nodes. The system is typically fast, highly customizable, energy efficient, more flexible, and can be easily adapted to meet applicable regulations. An example of a private blockchain is MultiChain. Private blockchain is a closed storage network and could limit the free expansion of local renewable energy and therefore is not entirely suitable for smart grid management.

Consortium Blockchain integrates the features of public and private systems to create a more adaptable platform. The consortium blockchain features open consensus for public systems and centralized control for private systems. It is typically used by companies that want to develop their own system and create a broad-based platform for sharing data with stakeholders. For example, consortium blockchain has been used to present marketing products in the banking sector [50] and to distribute data between multiple stakeholders [51]. A multicentric blockchain system is suitable to participate in the regulatory process of a virtual power plant [24]. An example of such a system is the Hyperledger project, which has developed cross-industry blockchain frameworks [52]. Compared to the public blockchain, the consortium blockchain is less decentralized, does not focus on cryptocurrencies, and does not offer direct financial incentives to validators. The key features of these blockchain taxonomies are summarized in Table 2.

3.3. Evolutions of Blockchain

Blockchain development and innovations can be divided into three phases. Blockchain 1.0 concerns Bitcoin and other cryptocurrencies in both centralized and decentralized environments. Blockchain 2.0 explores various applications of the technology in non-digital currency scenarios such as smart contracts and smart cities such as Ethereum. Blockchain 3.0 focuses on the underlying technology and provides a platform for trading applications and innovation for broader public service. For example, DAG (Directed Acyclic Graph) is typically placed in the third category.

3.4. Smart Contracts

A smart contract is a self-enforcing computerized transaction protocol that contains the terms of an agreement between the parties involved [53]. It is designed to automatically perform, control, and document services according to the terms of the agreement. It performs transactions that meet the terms of the agreement between anonymous parties, comply with the organization's laws, or generate tokens [54] without involving an intermediary. An important feature of blockchain smart contracts is to make transactions traceable, transparent, and irreversible. Smart contracts on the blockchain involve agreements between multiple users to store and execute data [5].

3.5. Consensus Algorithms

The consensus algorithm plays an important role in maintaining the security and efficiency of the blockchain [55] especially in solving the Byzantine General Problem [56,57], as well as in ensuring data consistency in case of errors [45]. Two types of fault tolerance can be found in the literature. The first involves fail–stop (or crash) faults that cause nodes to stop participating in the consensus agreement [58]. Such faults are usually caused by hardware or software failures and do not exhibit other malicious behaviors [45] and are

usually relatively easy to resolve. The second group is Byzantine faults, which provide misleading information mainly due to bugs or attacks and usually behave quite randomly. Several consensus algorithms can be found in the literature with particular characteristics, advantages, and disadvantages [45,51,58,59].

Table 2. Different features of blockchain classifications.

Taxonomies	Permissionless	Permissioned	
Properties	**Public**	**Private**	**Consortium**
Governance	Public—any node can join	Managed by one administrator	Managed by a set of participants
Access right	Any node can read, write, leave, and join	Only authorized node	Only a set of authorized nodes
Network scalability	High	Low	Medium
Decentralization level	Highly decentralized	Highly centralized	Semi-centralized
Protocol efficiency	Less efficient	Highly efficient	Highly efficient
Examples	Bitcoin, Ethereum, Ripple, etc.	MultiChain	Hyperledger
Consensus algorithms	No permission is required (PoW: Proof of Work, PoS: Proof of Stake, PoET: Proof of Elapsed Time, etc.)	Permission required (PBFT: Practical Byzantine Fault Tolerance, PoA: Proof of Authority, PoI: Proof of Importance, etc.)	
Data Immutability	Highly immutable	Less immutable	
Transaction Validation	Incentive-based mining by any node	• List of authorized validators • No incentive required	
Main features	• Resistance to censorship • Unregulated and transnational • Anonymous identities • Scalable • Untrusted organizations can participate • Slow transaction speed	• Suitable for highly regulated companies • Efficient transaction throughput • Transaction without fees • Better protection against external attacks • Fast transaction speed	

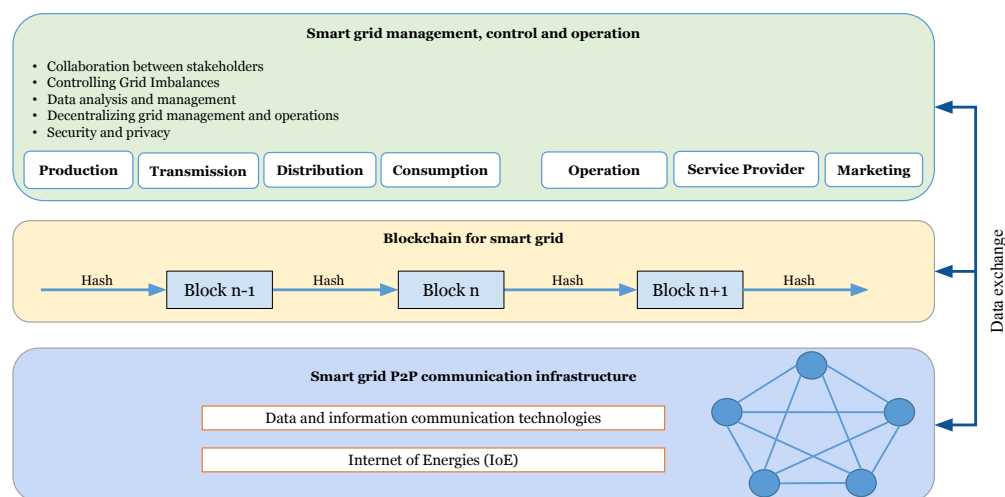## 4. Blockchain for Smart Grid Management, Control, and Operation

Blockchain offers a new solution to these challenges. It minimizes data management, fair incentive mechanisms, regulatory costs and technical issues, transaction fees between distributed nodes, speed of resources, and price adjustment issues. It can also increase transparency among stakeholders, ensure data security and privacy, simplify the energy demand and supply chain, and minimize distribution losses.

The application of blockchain in the energy sector is currently an ongoing area of research and development [60]; however, most of these applications have not yet progressed beyond the pilot stage. One notable example is the Brooklyn Microgrid [61], which allows local solar energy consumers to exchange data via blockchain. Another example is the UK's Electron project [62], which uses a blockchain-based platform to enable grid operators, systems, local energy markets, and distributed energy sources to participate in multiple grid optimization markets with different energy assets. Countries around the world are recognizing the potential applications of blockchain in the energy sector. For a list of efforts by companies to implement blockchain in the energy sector, see [22]. Figure 3 shows a potential blockchain infrastructure for managing, controlling, and operating smart grids.

4.1. Summarizing Recently Published Surveys on Blockchain Applications for Smart Grid

A number of studies have also been published that address various blockchain applications, challenges, opportunities, and future trends. In [22], the authors provided an up-to-date and comprehensive summary of blockchain use for smart grids by analyzing a number of peer-reviewed articles, research results, and entrepreneurial projects. The authors in [26] presented an overview of blockchain-based solutions to smart grid challenges

and their advantages and disadvantages. The article identified relevant blockchain-based applications especially at the cyber-physical level of the smart grid. In [1], the authors conducted a survey to systematically identify potential blockchain implementations for smart grid as well as the associated challenges and opportunities. A comprehensive overview of blockchain applications for future decentralized smart grids is provided in [4]. The article discusses that current smart grids face several challenges such as scalability, transparency, and extensibility, high computational cost, availability of attacks, and inability to control future power supply consisting of multiple components.

Figure 3. Blockchain infrastructure for smart grid management, control, and operation.

Table 3 summarizes recently published studies in this area. The table also describes the approach of the study compared to our article. Some of the articles address the use of blockchain in smart grid marketing, grid decentralization, data aggregation and storage, and security and privacy mechanisms. Relevant challenges for grid management and operation arising from stakeholder collaboration, grid imbalances, data analytics, and management have not been addressed in existing review articles. Moreover, the challenges covered are often viewed from the retail perspective. This work includes the challenges not considered in other studies as well as recent developments in smart grid management, control, and operation.

4.2. Comparing Traditional and Blockchain-Based Management, Control, and Operation for Smart Grid

Energy has traditionally been generated, distributed, and controlled by companies with large financial resources. The introduction of Advanced Metering Infrastructures (AMI) that enable bidirectional communication between generators, distributors, retailers, and consumers makes it possible to transform the traditional workforce into a smart grid. Smart systems such as Wireless Sensor Networks (WSNs), the Internet of Things (IoT), Virtual Power Plants (VPPs), and other intelligent control systems also enable the optimization of power generation and consumption. These advanced technologies makes the power grid system smarter, more efficient, and automated [20,24]. The smart grid operations are traditionally controlled and managed centrally, making the grid infrastructure vulnerable to different kinds of attack. This results in various operational delays due to extensive data management, access control, and security. Table 4 compares the various advantages of a decentralized blockchain-based smart grid with centralized traditional smart grid management. It shows that using blockchain for data management and control of the smart grid is beneficial to create a diversified platform where relevant stakeholders have equal influence on the overall operation of the infrastructure.

Table 3. Summary of typical surveys and reviews on blockchain challenges for smart grid management, control, and operation.

Ref.	I	II	III	IV	V	Discription
[1]	L	L	M	M	L	Conducts a systematic review of the potential applications of blockchain for energy company operations, wholesale energy trading and supply, energy imbalance settlement, digitization of IoT platforms, and P2P trading and distributed energy supply.
[4]	L	L	M	M	L	Provides a comprehensive overview of blockchain applications for AMI, the distributed energy trading market, monitoring, control, and metering, electric vehicle and charging station metering, and microgrid operations.
[5]	L	L	L	L	L	Reviews research progresses of blockchain technology for the energy sector particularly on distributed energy systems, optimization of energy trading, electric vehicles, smart device connection and intelligent control, and supporting environmental challenges.
[20]	L	L	M	M	H	Provides an overview of blockchain applications for P2P energy trading infrastructure, electric vehicle energy trading, asset maintenance security, energy generation and distribution, and privacy and security techniques.
[26]	L	L	L	M	M	Reviews various aspects, advantages, and disadvantages of using blockchain for energy trading, microgrid operations, EV, and cyber-physical security.
[63]	L	L	L	H	L	Provides an overview of blockchain applications for energy trading, infrastructure management, and smart grid operations.
[64]	L	L	L	H	M	Provides current improvements in blockchain applications for smart grids, identifies opportunities, challenges, and potential solutions in various areas of the smart grid.
[65]	M	L	M	M	M	Analyzes the applicability of blockchain for Smart Grid 2.0 with the goal of facilitating grid decentralization.
[66]	L	L	L	L	M	Provides an overview of blockchain applications for various areas of smart cities, including smart grid for energy trading, improving data security, renewable energy financing, and Thing-to-Thing energy trading.
[67]	L	L	L	L	L	Reviewed recent developments in energy trading, taxonomies, challenges, and potential solutions.
[68]	L	L	M	M	M	Provides a bibliometric analysis and review of blockchain implementations for energy marketing, data exchange and security, energy management and scalable systems, information transfer, P2P energy sharing, and trading in microgrids, among others.
[69]	L	L	L	L	L	Presents blockchain applications for China's energy sector. The article focuses in particular on energy financing, trading, consumption, and Energy Internet.
[70]	L	L	L	L	H	Provides a comprehensive overview of blockchain technology solutions for smart grid transformation from the perspective of technological advances in its industrial applications, challenges, and opportunities.
[71]	L	L	L	L	M	Presents the latest blockchain ideas, architectures, and technologies for cybersecurity in the smart grid.
[72]	L	L	L	M	M	Comprehensively presents existing blockchain applications for P2P trading of Electric Vehicle, carbon emission trading, etc.
This Paper	H	H	H	H	H	Provides a systematic overview of blockchain in the smart grid for stakeholder collaboration, data analytics and management, grid imbalance control, decentralization of grid management and operations, and security and privacy.

I: Collaboration among stakeholders, II: Data analysis and management, III: Control of grid imbalances, IV: Decentralization of grid management and operations, and V: Security and privacy; H: High coverage, M: Medium coverage, L: Low coverage.

Table 4. Comparison of management, control, and operation between traditional smart grid and blockchain-based smart grid [73].

Smartgrid Domains	Traditional Smart Grid	Blockchain Based Smart Grid
Production	• Largely non-renewable energy sources are involved • Often at a large scale from the central source	• All energy sources can use the platform • Microgrid prosumers can make a significant contribution to the renewable energy market
Transmission and Distribution	• Consumers cannot get updates of energy consumption on a regular basis • Limited control due to lack of demand–supply information flow • Long distribution distance contributes to high distribution loss • Power transaction procedures can be a bit complex and insecure	• Consumers can get energy consumption regularly, accurately, and fast • Power distribution is highly controlled • Local production and distribution is encouraged and greatly minimizes distribution loss • Simplified and highly secured transaction procedures
Consumption	• Consumers have no influence on the smart grid management, control, and operation	• Consumers can take part in the smart grid management, operation, and control as microgrid producers
Operation	• Customers often have limited choices of energy supplier • Operated manually and is vulnerable to unintentional or malicious attack • System updates and maintenance is done manually • Customers have often paper-based or digital contract • Centrally managed frequency and voltage control—difficult to manage with several distributed generators units involved • Prone to failures and can lead to a blackout	• Customers have several energy suppliers, many of which can be renewable sources • Automated and self-monitoring system minimizing bureaucracy • Automatically detect errors and self-troubleshoots • Customers have smart contract • Automatic frequency and voltage control can be done both locally and centrally • The system is not affected by some failed or unresponsive nodes
Service provider	• Unauthorized individuals/authorities can get access to sensitive data • Vulnerable to cyber threats • Sensitive information from the different stakeholders can leak without tracing the source	• The smart contract ensures that only eligible entities have access to relevant data • Highly secured and difficult to hack the system • Data encryption and Merkel hash in the distributed network ensures maximum security
Marketing	• Monitored by centralized governance • Price setting, billing, and other operations are governed centrally	• Decentralized, but can also be semi-centralized • Smart contract-based decentralized and automated price setting, billing and other operations can be used

4.3. Blockchain-Based Solutions for Smart Grid Challenges

Smart grid management and control is an important issue due to the diversity and number of DG units. Demand-driven control and optimization of network management is the focus of research. Feasibility and use case studies have been conducted on the use of blockchain for smart grid management, control, and operation [22]. A systematic review of blockchain applications for the energy sector at the national and institutional levels is

presented in [5]. In addition, [74] and a related paper by [75] explored how blockchain can be used in smart power management in the SealGrid platform, which allows users to monitor power consumption in real time without compromising security. The authors in [4] emphasize that the future of the smart grid must provide some level of security by (1) ensuring that unauthorized people cannot access information; (2) preventing unauthorized people from modifying the data; (3) cryptographic solutions provide adequate data protection; (4) denying authorized permission and granting access to those with the proper privileges; (5) authentication that ensures entities performing a specific task cannot deny their action; (6) developing a fault-tolerant network that is resistant to various attacks; (7) more efficient monitoring; (8) using advanced privacy technologies to protect information disclosure; and (9) promoting trust, transparency, and democracy among all stakeholders. In this subsection, we summarize blockchain-based applications for smart grid management, control, and operation based on the challenges discussed in Section 2.

4.3.1. Collaboration between Stakeholders

The consortium blockchain is used to support the virtual power plant (VPP) control system, improve operational activities, optimal scheduling, and efficient trading, and solve the problem of lack of real-time performance, high transaction costs, and information security [24]. Exploiting the similarities between VPP and blockchain in terms of data injection and information communication between different nodes within the system, the authors developed a VPP control system model based on blockchain. The model integrates discrete power supply, load, and other smart devices to share data with two blockchain systems, one technical and one commercial. The technical blockchain controls the process by connecting to the SCADA system via Ethernet to support power transmission, balancing, voltage, and frequency control, and to provide stable transmission and scheduling for the VPP. The commercial blockchain supports the process of energy quantity, price, transaction contracts, etc. The authors of [30] proposed a blockchain-based data ledger to store and track the energy generation and consumption of public buildings. The proposed platform facilitates transparency among stakeholders by making raw data available to the public to provide sustainable, affordable, reliable, and modern energy services to citizens. The availability of this raw data facilitates data analysis not only for research and development but also for production and distribution controls and resource management.

4.3.2. Controlling Grid Imbalance

Blockchain provides a mechanism to synchronize data from a variety of sources. These can help grid operators monitor different energy resources simultaneously, control voltage and frequency, and coordinate communication between different energy stakeholders. Blockchain can also help regulate voltage and frequency on the smart grid. Voltage and frequency fluctuations can lead to power outages. This can be solved by the continuous monitoring of power generation and consumption. However, the increasing number and variation of energy sources make the control system unstable. With blockchain technology, we can accurately and continuously determine the amount of energy produced and consumed, so that the grid is resilient to unexpected frequency or voltage overloads. Blockchain-based production control for distributed generation systems to avoid grid congestion is proposed by [76]. In addition, [77] has proposed a framework for using blockchain to monitor PV-based electric vehicle charging stations to regulate load frequency. The author's proposal integrates blockchain with a smart energy controller to optimally manage grid capacity considering load frequency and PV availability. The proposed framework improves user privacy, the immutability and transparency of energy data, energy tracking and availability, and sharing among users.

4.3.3. Data Analysis and Management

Blockchain as a distributed database system creates decentralized temper-proof but traceable networked copies of the data under a certain consensus verification. Blockchain

can support the smart grid data analysis and management, data protection, and aggregation [78]. Along with the diversity of distributed generation (DG), the smart grid is also changing its data aggregation and analysis mechanisms. Aggregators such as Demand Response (DR) and Virtual Power Plant (VPP) provide grid services to a wide range of energy resources. However, these aggregation mechanisms pose challenges to operators due to their large-scale and complex deployment and therefore require management and control. Establishing trust and transparency between DG entities and aggregators is also important to maintain short- and long-term interaction. To address these challenges, some blockchain-based solutions have already been proposed. In [36], a blockchain-based power grid data management architecture is proposed to realize binding data recording and business collaboration among multiple nodes. The proposed framework promotes collaboration among data aggregation and analysis processes, provides real-time awareness of data sharing to various stakeholders, simplifies the process of data access, coordinates data application, and facilitates technical support for smart grid data management and operation. The authors in [79] propose a blockchain-based decentralized aggregation mechanism that handles all transactions between decentralized energy owners, demand response, and virtual power plants. Blockchain can also be used for decentralized data collection, analysis, and management to minimize data communication and storage costs [80]. In [81], a consortial blockchain-based multidimensional data aggregation and control mechanism is proposed to ensure the security of stream data during communication. The proposed architecture creates a dynamic stream data control and operation architecture by simplifying the low data aggregation efficiency, computational complexity, feedback accuracy, and key management and data repair. Integrating blockchain with advanced metering systems could help utility operators predict future consumption needs by monitoring the continuous and accurate immutable data provided by blockchain technology.

4.3.4. Decentralizing Grid Management and Operation

A distributed data aggregation and storage mechanism using blockchain to secure grid sensor data was proposed by [82]. The authors in [80] identified three blockchain-related characteristics (decentralization, trust, and incentives) to analyze the smart grid-related literature and identify requirements for NIST conceptual models [6]. According to the authors, blockchain enables the decentralized collection and verification of metering applications at multiple levels and solves the problem of centralized data collection that could potentially affect smart grid performance. The authors also describe that the use of blockchain for smart grids facilitates decentralized energy-trading mechanisms, improves the operational efficiency of VPPs, enables demand response management systems in microgrids and consumer cities, renewable energy tracking, and edge computing for decentralized P2P interactions, among others. In [83], decentralized data aggregation for microgrids using Pallier and PBFT homomorphic encryption is proposed to protect user privacy and data integrity in public storage and sharing. The authors have also proposed an automatic and distributed solution for energy distribution in a microgrid using Ethereum Smart Contract. In [84], the authors propose a decentralized energy regulation and exchange application based on Ethereum smart contracts. Their framework minimizes reliance on a central authority, improves the efficiency of renewable energy resources, and addresses privacy and security issues. Smart contracts are used in [85] to propose a blockchain-based platform for peer-to-peer energy trading, decentralized energy management, energy flexibility aggregation, and community-based VPP operation. In [86], a blockchain-based keyless decentralized authentication architecture between service providers and end users in the smart grid is proposed to improve certification reliability and non-repudiation. In this approach, smart meters send a request and then receive the response through a consortium-based blockchain network that does not require a trusted agent. Ethereum smart contract with blockchain is used in [87] for interaction between energy generation and consumption between different smart meters in different buildings. The framework automatically monitors the availability of energy reserves

and smart meters and initiates transaction requests. The authors also proposed a digital identity management algorithm that authenticates smart meters and blockchain ledgers to mitigate port scans and port-based attacks on the Ethereum blockchain. In [88], the authors investigated the feasibility of using blockchain for transactive distributed grid management and operation of interconnected microgrids to optimize the financial and physical operation of power grid systems.

It has been shown that these blockchain-based systems can support the physical layer of the smart grid. Aggregation, analysis, and management of grid data can improve the missions of transmission system operators (DSOs) by providing accurate data on electricity generation, distribution, and consumption. Blockchain, along with various underlying technologies, can facilitate decision making at different levels of grid operations. However, maintaining data security, integrity, and privacy in the grid environment for both data aggregation and analysis is a complex issue that requires thorough investigation.

4.3.5. Security and Privacy

Traditional smart grids have been subjected to a number of malicious cyberattacks over the years, using various methods such as Denial of Service (DoS) to gain unauthorized control over the grid, resulting in partial or complete power outages. Studies have shown that blockchain, whose main characteristic is the immutability of data, can provide a solution to this problem. There are several known attacks on smart power grids. One of them is the jabbing attack, in which the attacker installs a malicious smart electricity meter that sends false data, causing desynchronization and power interruption. The puppet attack sends a signal to the node. Then, the attacker controls the node and sends more signals into the network, causing the smart meter network to become unstable. Another example is the stack smashing attack, which compromises the application layer of the network and leads to the disclosure of sensitive data. An experimental attack, on the other hand, makes the smart grid layer vulnerable to DoS attacks [40]. A comprehensive review of blockchain in smart grid for cybersecurity from application and technology perspectives was conducted by [71].

Several promising blockchain-based techniques have been proposed to address privacy and user security challenges in the smart grid. Privacy Preserving Energy Transactions (PETra) is described in [89] as a secure distributed ledger-based energy trading solution that provides anonymity for communication, bidding, and trading. The framework enables secure and verifiable trading of energy futures, preserves prosumers' privacy, and allows distribution system operators to regulate trading and enforce security rules. The proposed framework was later extended by [90] to illustrate communication and transaction anonymity. The authors in [91] presented a scheme for efficient data aggregation and privacy protection based on blockchain. In addition, [92] proposed blockchain-based lightweight security solutions for advanced metering infrastructures to prevent man-in-the-middle attacks and data tampering through timely adversarial node detection, localization, and provenance through blockchain. A permission-based blockchain edge model for smart grid networks to ensure data privacy and energy security is proposed by [93]. The proposed model aims to ensure the traceability of energy consumption while protecting end-user privacy, enable optimal energy management, and enable controllers to assess the identity of the edge device in smart grid networks.

A novel cybersecurity architecture for smart grids based on blockchain to improve data security is proposed by [94]. The algorithm leverages advanced metric infrastructures such as smart meters and virtual power plants and uses an edge-fog cloud computing architecture. In [95], the authors show how the immutability of the blockchain can be used to detect non-technical frauds such as energy theft, metering errors, billing process errors, etc. This helps utilities control and monitor the power distribution network. In [82], a blockchain-based smart grid protection framework against cyberattacks is presented to improve the self-defense capabilities, robustness, and security of the power grid. In addition, ref. [96] proposed a blockchain-based solution backed by a smart contract to create a

temperature-proof system to protect consumer data collected and transmitted in the smart grid system. The proposed system provides transparency, auditability, and immutability.

Blockchain has also been used for access control systems in the smart grid. In [97], the application of blockchain for identity-based combined encryption, signature encryption, and signature encryption scheme for the smart grid is proposed, which solves the pressing problem of private key generator, ensures secure key management, and involves more users in the daily management of the smart grid.

4.4. A Summary of Blockchain Applications for Smart Grid Management, Control, and Operation

Table 5 summarizes the various blockchain applications that have been proposed in recent years for the management, control, and operation of smart grids. Blockchain technology could provide a solution to these challenges by providing a decentralized platform through which all participants can share information equally. The technology could enable all participants to collaboratively create a platform without having to trust each other in any way [44]. The adoption of blockchain in the energy sector has several benefits: Energy blockchain technology promotes the decentralized production and distribution of low-voltage energy systems [24]. It also supports simplified multi-level systems [5], in which energy producers, distribution system operators, transmission system operators, and consumers can communicate directly with each other to ensure the operation process. In addition, blockchain, in combination with smart contracts, enables efficient management of the smart grid [98]. Using predefined consensus rules, smart contracts send signals to all nodes to ensure legitimate transactions. In this way, all energy storage flows can be controlled automatically, which contributes to the accuracy of the balance between supply and demand [99]. Blockchain can also record, store, and distribute all energy transaction data, ensuring decentralized security of all energy flows and business activities [5].

Table 5. Blockchain-based solutions to address the challenges in smart grid management, control, and operations.

Blockchain Application Areas	Blockchain-Based Solutions to Address the Challenges	Ref.
Collaboration between stakeholders	• Facilitates trust and transparency between stakeholders and the public • Automatic monitoring and maintenance of the smart grid • Enables resource allocation, tracking of environmental indicators • Improves efficiency of renewable energy sources • Improves the digitalization of the grid and enables new applications for the power system • Facilitate the role/influence of microgrid prosumers in the management and operation of the smart grid	[24,30]
Controlling Grid Imbalance	• Regulation of voltage and fair distribution of production between distributed generation units • Enables a temperature-safe system to protect customer data collected and transmitted to the smart grid	[76,77]

Table 5. *Cont.*

Blockchain Application Areas	Blockchain-Based Solutions to Address the Challenges	Ref.
Data analysis and management	• Protection of authenticity and correctness of aggregated data • Creation of immutable data structures that cannot be modified • Highly scalable and support for microtransactions • Enhancement of the architecture for the power management system to monitor power consumption in real time • A secure data aggregation based on encryption • Enabling a multi-dimensional data aggregation control mechanism for the smart grid • Decentralized aggregation mechanism to handle all transactions between different smart meters	[36,79–81]
Decentralizing grid management and operations	• Improve authentication and non-repudiation • Support the power management process without a trusted party • Participation in distributed computing to reduce the VPP's computational load • Promotion of decentralization • Improve transparency, digitize the grid, and enable new applications for the power system • Support advanced metering infrastructure control systems to improve operational activities, optimal planning, and efficient trading • Enables traceable energy management on the smart grid	[78,80,82–88]
Security and privacy	• Create immutable data structures that cannot be modified • Improving cybersecurity and privacy for smart grids • Improving security and privacy, information security, access control • Localization and provenance • Solves the problem of lack of real-time performance, high transaction costs, and information security • Timely identification of adversarial nodes	[40,71,82,89–97]

5. Discussion and Future Research Directions

From the review, it is clear that a blockchain-based smart grid requires systematic work from design to implementation. It needs support from both technical and non-technical aspects. Localized standalone solutions cannot make the blockchain system fully functional. A lot of fundamental work is needed to ensure efficient management, control, and operation for blockchain-based smart grids. Further discussion and research directions are addressed below.

5.1. Collaboration between Stakeholders

The introduction of blockchain technology into the smart grid, a widely accepted and well-functioning system, is always a challenge to harmonize the collaboration between all stakeholders.

(1) Better understanding of the needs and the future. All smart grid stakeholders (energy producers, transmitters, distributors, consumers, regulators, coordinators, etc.) need to understand and evaluate current challenges and future trends in energy management and their environmental, social, economic, and regulatory implications in order to accept and implement them. Some of the resulting issues need to be addressed.

(2) Effective coordination and consensus mechanism. Energy stakeholders will be participants, contributors, and beneficiaries of the blockchain system whose interests and responsibilities do not fully align but must collaborate and participate in a blockchain-

based smart grid system. This requires all stakeholders to be able to achieve an effective coordination and consensus mechanism with the technical support of the blockchain and also to thoroughly engage with this decentralized, entirely new system, technical means, and business model.

(3) Advanced technical tools and newer administrative systems. Increased collaboration among regulatory, administrative, technical, and commercial stakeholders is needed to develop coherent blockchain systems that can improve upon existing systems. This collaboration must be based on more modern technical tools and newer administrative systems. Relevant technology development outcomes need to be tested, validated, and improved in real-world smart grid systems.

(4) Seamless integration. Blockchain-based system technology must address and improve upon the shortcomings of current systems and provide scalability, speed, accuracy, and security, as well as seamless integration with current advanced metering infrastructure.

5.2. Controlling Grid Imbalance

With the development of smart grids, the need for applications and integration of various renewable energy sources, including the management of various imbalances in the blockchain system, is increasing.

(1) Synchronization. Blockchain-based smart grids require mechanisms to synchronize data from multiple sources to balance the associated imbalances resulting from (1) voltage and frequency shifts in the grid system itself, (2) continuous dynamic changes in energy generation, transmission, distribution, and demand, (3) changing energy consumption patterns and quantities, and (4) flexible and variable energy exchange and trading.

(2) Integration and interaction. Deep integration and interactive control technology between blockchain and different parts of the grid is an urgent problem to solve. The sharing characteristics, timely data updates, and stability of the architecture possessed by blockchain technology provide a good technical basis for solving these imbalance problems.

(3) Automation control. Further research is needed to investigate the scope of blockchain design and implementation, the associated interfaces to each control system, and blockchain-based automation control and coordination technologies.

(4) Information exchange. The main mission of blockchain-based decentralized grid management and operations is to ensure secure information exchange among relevant stakeholders, improve the supply and demand chain, facilitate the participation of professional renewable energy consumers in energy markets, control congestion with automated frequency and voltage monitoring systems, and protect critical grid resources with real-world implementations are all areas for future research.

5.3. Data Analysis and Management

Blockchain-based smart networks greatly extend the digitization of existing power grids. So, data analysis and management is a big issue in the context.

(1) Big Data. Each electronic and digital component of the grid continuously generates various types of data to control and maintain the grid system and to support its commercial operations. The complex and large-scale decentralized system implies that the complex and volatile distributed data needs to be accumulated, fused, analyzed, and rationalized for use.

(2) Data fusion. Advanced data processing and management technologies need to be combined with blockchain systems to address the challenges of the 3Vs (volume, velocity, and variety) of data in the smart grid, high scalability and scalability, diversity and heterogeneity of data types, and timeliness of data processing.

(3) Off-chain data processing. Blockchain itself does not have the rationalization design and processing ability to handle big data, but the combination of smart contract and

off-chain data processing can allow the refined core data to enter the main chain of blockchain, and most of the lengthy and trivial local data analysis and processing are processed outside the localized chain and controlled by the smart contract for relevant data analysis, which will greatly improve the capacity and efficiency of smart grid based on blockchain. This will greatly improve the capability and efficiency of data analysis and processing of blockchain-based smart grids.

(4)   Data techniques. Advanced data techniques such as machine learning, deep learning, etc., need to be introduced to help analyze all kinds of big data related to smart grids.

5.4. Decentralizing Grid Management and Operations

Blockchain-based decentralized management and operation of the smart grid is very different from the traditional centralized management and operation model.

(1)   Extensive decentralization. Traditional centralized management has centralized managers and controllers coordinating the global management of all types of grid issues and operations. The blockchain-based smart grid brings the concept of decentralization to the grid system in terms of technology, data, business, and its management and operations, but it also implies a complete change in business logic and technical systems as well as a change in the management model.

(2)   Evolution from decentralization. Decentralization not only avoids the risk of a single point of failure in a complex smart grid but also brings an evolution of the system, including (1) autonomy of individual nodes, (2) automation of the system's business execution (code execution based on smart contracts), and (3) resilience of the system with high fault tolerance and system robustness.

(3)   Deep centralization. Decentralized management and operation can facilitate and accelerate network operation decisions at various levels and make frequent and tedious day-to-day business and operations extremely efficient.

(4)   Updating of management model. The redesign and implementation of fully decentralized grid management and operation requires not only further research on the technical implementation of the system at all levels but also the adaptation of the management rules and concepts of the existing system.

(5)   Mitigating the risks associated with decentralization. Attention must also be paid to how to avoid the risk of system chaos and disorder that may arise after decentralization.

5.5. Security and Privacy

Blockchain-based smart grids pose no fewer cybersecurity risks than existing smart grids.

(1)   Enlarged attack surface. As with any IT system, the same cyberattacks that are on the rise and remain a threat to the smart grid. The performance of a blockchain-based smart grid relies heavily on the autonomous management and automated operation of the technical system due to its decentralized and efficient architecture and operation. However, due to the ever-growing attack surface of the smart grid system, the blockchain-based system needs to maintain the security of the grid business, the security of the grid system, the security of the grid data, and the privacy of all participants. In addition, the blockchain itself may also be exposed to new cyberattacks or data-oriented intelligent attacks. These issues needs to be properly monitored and researched.

(2)   Off-chain attacks. Since the blockchain system is supported by and serves other parts of the smart grid, any potential attacks outside the chain may eventually affect the performance of the blockchain system, e.g., injecting manipulated data into the blockchain, reading data from the blockchain through malicious manipulation, etc.

(3)   Local vulnerability vs. global security. The security vulnerability of each component and the protection of the operation process of each functional area must be considered in the development of the future blockchain system.

(4)   Hierarchical protection. The hierarchical structure of the blockchain (including the functional hierarchy, data hierarchy, business hierarchy, etc.) and the cooperation between multi-branch chains also help to avoid security risks and increase the security and resilience of the system and data.

6. Conclusions

Blockchain-based smart grid systems can be executed independently and automatically according to certain predefined consensus mechanisms without human intervention, brokers, or central authorization, and enable efficient data aggregation techniques to solve privacy and security problems in the grid. This paper systematically explores blockchain-based applications for the management, control, and operation of smart grid systems. The paper focuses on non-financial applications of blockchain in the energy sector and divides the challenges into five main categories: stakeholder collaboration, grid imbalance, data management and operations, decentralization of grid operations, and security and privacy. Based on the review, analysis, and comparison with existing reviews, the paper identifies additional challenges and highlights future research directions in the five categories.

Existing technologies leverage different blockchain architectures for different application scenarios and demonstrate that the technology can be used to support smart grid infrastructure management and operations. However, actual implementations of the technology for grid management, control, and operations presented in the literature are still sporadic and localized. There is a lack of systematic technologies for smart grid management, control, and operation. This requires deconstruction of the existing grid management, control, and operation, and systematic planning, design, and development of the corresponding blockchain application system by combining the technical advantages of blockchain. Since it is difficult to update the architecture of the blockchain system and the online storage of data is very long-lived, it is necessary to have a very clear understanding of the structure, business, and technical management of the existing power grid. A detailed prior knowledge of the future business and commercial expansion of the smart grid and a relatively clear prediction of the system technology and business trends are essential factors to design and develop a highly reliable, scalable, long-lived, and open blockchain system.

References

1.   Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
2.   European Commission (EU). Energy Union Package, A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy, Brussels. 2015. Available online: https://www.eea.europa.eu/policy-documents/com-2015-80-final (accessed on 26 November 2021).
3.   Shahzad, Y.; Javed, H.; Farman, H.; Ahmad, J.; Jan, B.; Zubair, M. Internet of energy: Opportunities, applications, architectures and challenges in smart industries. *Comput. Electr. Eng.* **2020**, *86*, 106739 [CrossRef]
4.   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]
5.   Wang, Q.; Su; M. Integrating blockchain technology into the energy sector—From theory of blockchain to research and application of energy blockchain. *Comput. Sci. Rev.* **2020**, *37*, 100275. [CrossRef]
6.   Pillitteri, V.; Brewer, T. *Guidelines for Smart Grid Cybersecurity, NIST Interagency/Internal Report (NISTIR)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014. Available online: doi:10.6028/NIST.IR.7628r1 (accessed on 17 September 2021). [CrossRef]

7. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [CrossRef]
8. Faisal, M.A.; Aung, Z.; Williams, J.R.; Sanchez, A. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study. *IEEE Syst. J.* **2014**, *9*, 31–44. [CrossRef]
9. Ourahou, M.; Ayrir, W.; Hassouni, B.E.; Haddi, A. Review on smart grid control and reliability in presence of renewable energies: Challenges and prospects. *Math. Comput. Simul.* **2020**, *167*, 19–31. [CrossRef]
10. Salkuti, S.R. Challenges, issues and opportunities for the development of smart grid. *Int. J. Electr. Comput. Eng. (IJECE)* **2020**, *10*, 1179–1186. [CrossRef]
11. Mattila, J.; Seppälä, T.; Naucler, C.; Stahl, R.; Tikkanen, M.; Bådenlid, A.; Seppälä, J. *Industrial Blockchain Platforms: An Exercise in Use Case Development in the Energy Industry (No. 43)*; ETLA Working Papers; ETLA Economic Research: Helsinki, Finland, 2016.
12. Konashevych, O.I. Advantages and current issues of blockchain use in microgrids. *Electron. Model.* **2016**, *38*, 93–104. [CrossRef]
13. Xue, L.; Teng, Y.; Zhang, Z.; Li, J.; Wang, K.; Huang, Q. Blockchain technology for electricity market in microgrid. In Proceedings of the 2017 2nd International Conference on Power and Renewable Energy (ICPRE), Chengdu, China, 20–23 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 704–708.
14. Yuan, Y.; Wang, F.Y. Blockchain: The state of the art and future trends. *Acta Autom. Sin.* **2016**, *42*, 481–494.
15. Davis, S.J.; Lewis, N.S.; Shaner, M.; Aggarwal, S.; Arent, D.; Azevedo, I.L.; Benson, S.M.; Bradley, T.; Brouwer, J.; Caldeira, K.; et al. Net-zero emissions energy systems. *Science* **2018**, *360*, 6396. [CrossRef]
16. Energimyndigheten. 2020. Available online: https://www.energimyndigheten.se/statistik/den-officiella-statistiken/statistikprodukter/natanslutna-solcellsanlaggningar/ (accessed on 23 November 2021).
17. Ajadi, T.; Cuming, V.; Boyle, R.; Strahan, D.; Kimmel, M.; Logan, M.; McCrone, A. Global Trends in Renewable Energy Investment 2020. https://www.fs-unep-centre.org/wp-content/uploads/2020/06/GTR_2020.pdf (accessed on 23 December 2021).
18. Hannan, M.A.; Tan, S.Y.; Al-Shetwi, A.Q.; Jern, K.P.; Begum, R.A. Optimized controller for renewable energy sources integration into microgrid: Functions, constraints and suggestions. *J. Clean. Prod.* **2020**, *256*, 120419. [CrossRef]
19. Badal, F.R.; Das, P.; Sarker, S.K.; Das, S.K. A survey on control issues in renewable energy integration and microgrid. *Prot. Control. Mod. Power Syst.* **2019**, *4*, 8. [CrossRef]
20. Alladi, T.; Chamola, V.; Rodrigues, J.J.; Kozlov, S.A. Blockchain in smart grids: A review on different use cases. *Sensors* **2019**, *19*, 4862. [CrossRef]
21. Di Silvestre, M.L.; Gallo, P.; Guerrero, J.M.; Musca, R.; Sanseverino, E.R.; Sciumè, G.; Vasquez, J.C.; Zizzo, G. Blockchain for power systems: Current trends and future applications. *Renew. Sustain. Energy Rev.* **2020**, *119*, 109585. [CrossRef]
22. Foti, M.; Vavalis, M. What blockchain can do for power grids? *Blockchain: Res. Appl.* **2021**, *2*, 100008. [CrossRef]
23. Hussain, S.S.; Farooq, S.M.; Ustun, T.S. Implementation of blockchain technology for energy trading with smart meters. In Proceedings of the 2019 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, India, 22–23 March 2019; IEEE: Piscataway, NJ, USA, 2019; Volume 1, pp. 1–5.
24. Li; Y.; Teng, Y.; Cao, R.; Li; N. Research on Coordination Control Systems of Virtual Power Plant Based on Blockchain. In Proceedings of the 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), Xi'an, China, 21–24 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1377–1383.
25. Kappagantu, R.; Daniel, S.A. Challenges and issues of smart grid implementation: A case of Indian scenario. *J. Electr. Syst. Inf. Technol.* **2018**, *5*, 453–467. [CrossRef]
26. Musleh, A.S.; Yao, G.; Muyeen, S.M. Blockchain applications in smart grid–review and frameworks. *IEEE Access* **2019**, *7*, 86746–86757. [CrossRef]
27. Hamouda, M.R.; Nassar, M.E.; Salama, M.M.A. A Novel Energy Trading Framework Using Adapted Blockchain Technology. *IEEE Trans. Smart Grid* **2020**, *12*, 2165–2175. [CrossRef]
28. Mazzola, L.; Denzler, A.; Christen, R. Towards a Peer-to-Peer Energy Market: An Overview. *arXiv* **2020**, arXiv:2003.07940.
29. Cheng, S.; Zeng, B. and Huang, Y.Z. Research on application models of blockchain technology in the distributed electricity market. In *IOP Conference Series: Earth and Environmental Science*; IOP Publishing: London, UK, 2017; Volume 93, p. 012065.
30. Galici, M.; Mureddu, M.; Ghiani, E.; Celli, G.; Pilo, F.; Porcu, P.; Canetto, B. Energy Blockchain for Public Energy Communities. *Appl. Sci.* **2021**, *11*, 3457. [CrossRef]
31. Unahalekhaka, P.; Sripakarach, P. Reduction of reverse power flow using the appropriate size and installation position of a BESS for a PV power plant. *IEEE Access* **2020**, *8*, 102897–102906. [CrossRef]
32. Mahato, G.C.; Choudhury, T.R.; Nayak, B.; Debnath, D.; Santra, S.B.; Misra, B. A Review on High PV Penetration on Smart Grid: Challenges and its Mitigation using FPPT. In Proceedings of the 2021 1st International Conference on Power Electronics and Energy (ICPEE), Bhubaneswar, India, 2–3 January 2021; pp. 1–6. [CrossRef]
33. Holguin, J.P.; Rodriguez, D.C.; Ramos, G. Reverse Power Flow (RPF) Detection and Impact on Protection Coordination of Distribution Systems. *IEEE Trans. Ind. Appl.* **2020**, *56*, 2393–2401. [CrossRef]
34. Frost, R.; Zieland, L.; Sharafi, D.; Susanto, J. Impact of Reverse Power Flow in Distribution Feeders on Under-Frequency Load Shedding Schemes. In Proceedings of the 2020 International Conference on Smart Grids and Energy Systems (SGES), Perth, Australia, 23–26 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 100–104.
35. Sun, H.; Guo, Q.; Qi, J.; Ajjarapu, V.; Bravo, R.; Chow, J.; Li, Z.; Moghe, R.; Nasr-Azadani, E.; Yang, G.; et al. Review of challenges and research opportunities for voltage control in smart grids. *IEEE Trans. Power Syst.* **2019**, *34*, 2790–2801. [CrossRef]

36. Shen, L.; Hao, B.; Li, Y.; Yu, H.; Zhang, S.Z.; Men, H.; Fan, J. Blockchain-based Power Grid Data Asset Management Architecture. In Proceedings of the 2020 International Conference on Computer Science and Management Technology (ICCSMT), Shanghai, China, 20–22 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 207–211.
37. Samad, T.; Annaswamy, A.M. Controls for smart grids: Architectures and applications. *Proc. IEEE* **2017**, *105*, 2244–2261. [CrossRef]
38. 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]
39. Engebretson, P. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*; Elsevier: Amsterdam, The Netherlands, 2013.
40. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [CrossRef]
41. Triantafyllou, A.; Jimenez, J.A.P.; Torres, A.D.R.; Lagkas, T.; Rantos, K.; Sarigiannidis, P. The challenges of privacy and access control as key perspectives for the future electric smart grid. *IEEE Open J. Commun. Soc.* **2020**, *1*, 1934–1960. [CrossRef]
42. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Bitcoin* **2008**. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 27 December 2021).
43. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
44. Mattila, J. *The Blockchain Phenomenon—The Disruptive Potential of Distributed Consensus Architectures (No. 38)*; ETLA Working Papers; ETLA Economic Research: Helsinki, Finland, 2016.
45. Fu; X.; Wang, H.; Shi, P. A survey of Blockchain consensus algorithms: Mechanism, design and applications. *Sci. China Inf. Sci.* **2021**, *64*, 121101. [CrossRef]
46. Rapier, E. From Yelp reviews to mango shipments: IBM's CEO on how Blockchain will change the world. *Bus. Insid.* **2017**, *21*, 2017.
47. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
48. Cash, M.; Bassiouni, M. Two-tier permission-ed and permission-less blockchain for secure data sharing. In Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud), New York, NY, USA, 21–23 September 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 138–144.
49. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
50. 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.
51. Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, *154*, 113385. [CrossRef]
52. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
53. Szabo, N. Formalizing and securing relationships on public networks. *First Monday* **1997**, *2*. [CrossRef]
54. Clack, C.D.; Bakshi, V.A.; Braine, L. Smart contract templates: Foundations, design landscape and research directions. *arXiv* **2016**, arXiv:1608.00771.
55. Du, M.; Ma, X.; Zhang, Z.; Wang, X.; Chen, Q. A review on consensus algorithm of blockchain. In Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 2567–2572.
56. Castro, M.; Liskov, B. Practical byzantine fault tolerance. *OSDI* **1999**, *99*, 173–186.
57. Lamport, L.; Shostak, R.; Pease, M. The Byzantine generals problem. In *Concurrency: The Works of Leslie Lamport*; ACM: New York, NY, USA, 2019; pp. 203–226.
58. Baliga, A. Understanding blockchain consensus models. *Persistent* **2017**, *4*, 1–14.
59. Ferdous, M.S.; Chowdhury, M.J.M.; Hoque, M.A. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *J. Netw. Comput. Appl.* **2021**, *182*, 103035. [CrossRef]
60. Hasse, F.; Von Perfall, A.; Hillebrand, T.; Smole, E.; Lay, L.; Charlet, M. *Blockchain—An Opportunity for Energy Producers and Consumers*; PwC Global Power & Utilities: Sydney, Australia, 2016; pp. 1–45.
61. Brooklyn. BMG. Brooklyn Energy. 2019. Available online: https://www.brooklyn.energy/ (accessed on 23 November 2021).
62. Electron. Electron. Lounch and Operate Distributed Energy Markets. 2020. Available online: https://electron.net/ (accessed on 23 November 2021).
63. Samy, S.; Azab, M.; Rizk, M. Towards a Secured Blockchain-based Smart Grid. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021; pp. 1066–1069. [CrossRef]
64. 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]
65. 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]
66. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2794–2830. [CrossRef]

67. Aggarwal, S.; Kumar, N.; Tanwar, S.; Alazab, M. A Survey on Energy Trading in the Smart Grid: Taxonomy, Research Challenges and Solutions. *IEEE Access* **2021**, *9*, 116231–116253. [CrossRef]

68. Ante, L.; Steinmetz, F.; Fiedler, I. Blockchain and energy: A bibliometric analysis and review. *Renew. Sustain. Energy Rev.* **2021**, *137*, 110597. [CrossRef]

69. Zhu, S.; Song, M.; Lim, M.K.; Wang, J.; Zhao, J. The development of energy blockchain and its implications for China's energy sector. *Resour. Policy* **2020**, *66*, 101595. [CrossRef]

70. 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]

71. Zhuang, P.; Zamir, T.; Liang, H. Blockchain for cybersecurity in smart grid: A comprehensive survey. *IEEE Trans. Ind. Inform.* **2020**, *17*, 3–19. [CrossRef]

72. Bao, J.; He, D.; Luo, M.; Choo, K.K.R. A survey of blockchain applications in the energy sector. *IEEE Syst. J.* **2020**, *13*, 3370–3381.

73. Rhydwan, A.H.M.; Choyon, M.M.S.; Iftekhar, M.N.; Sad, A.M.H.; Nandi, D. Smart Grid Implementation with Consortium Blockchain: A Proposed Model for Bangladesh. In Proceedings of the 2020 Emerging Technology in Computing, Communication and Electronics (ETCCE), Dhaka, Bangladesh, 21–22 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.

74. Suciu, G.; Sachian, M.A.; Vochin, M.; Dobrea, M.; Beceanu, C.; Iosu, R.; Petrache, A. Blockchain applicability using Smart Power Management: SealedGrid Architecture. In Proceedings of the 2019 IEEE PES Innovative Smart Grid Technologies Europe (Ismart gridT-Europe), Bucharest, Romania, 29 September–2 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.

75. Suciu, G.; Sachian, M.A.; Dobrea, M.; Istrate, C.I.; Petrache, A.L.; Vulpe, A.; Vochin, M. Securing the smart grid: A blockchain-based secure smart energy system. In Proceedings of the 2019 54th International Universities Power Engineering Conference (UPEC), Bucharest, Romania, 3–6 September 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–5.

76. Danzi, P.; Angjelichinoski, M.; Stefanovic, C.; Popovski, P. Distributed proportional-fairness control in microgrids via blockchain smart contracts. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 45–51.

77. Madhu, G.M.; Vyjayanthi, C.; Modi, C.N. A Novel Framework for Monitoring Solar PV based Electric Vehicle Community Charging Station and Grid Frequency Regulation using Blockchain. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–7.

78. Dong, Z.; Luo, F.; Liang, G. Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems. *J. Mod. Power Syst. Clean Energy* **2018**, *6*, 958–967. [CrossRef]

79. Mnatsakanyan, A.; Albeshr, H.; Al Marzooqi, A.; Bilbao, E. Blockchain-Integrated Virtual Power Plant Demonstration. In Proceedings of the 2020 2nd International Conference on Smart Power & Internet Energy Systems (SPIES), Bangkok, Thailand, 15–18 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 172–175.

80. Aderibole, A.; Aljarwan, A.; Rehman, M.H.U.; Zeineldin, H.H.; Mezher, T.; Salah, K.; Salah, Damiani, E.; Svetinovic, D. Blockchain technology for smart grids: Decentralized NIST conceptual model. *IEEE Access* **2020**, *8*, 43177–43190. [CrossRef]

81. Fan, M.; Zhang, X. Consortium blockchain based data aggregation and regulation mechanism for smart grid. *IEEE Access* **2019**, *7*, 35929–35940. [CrossRef]

82. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z.Y. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Trans. Smart Grid* **2018**, *10*, 3162–3173. [CrossRef]

83. Luo, X.; Xue, K.; Xu, J.; Sun, Q.; Zhang, Y. Blockchain Based Secure Data Aggregation and Distributed Power Dispatching for Microgrids. *IEEE Trans. Smart Grid* **2021**, *12*, 5268–5279. [CrossRef]

84. Nurgaliev, A.S.; Vershinin, I.S.; Minyazev, R.S. Concept and implementation of blockchain demonstration unit within the smart grid. In Proceedings of the 2019 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), Sochi, Russia, 25–29 March 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.

85. Cioara, T.; Pop, C.; Zanc, R.; Anghel, I.; Antal, M.; Salomie, I. Smart Grid Management using Blockchain: Future Scenarios and Challenges. In Proceedings of the 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Bucharest, Romania, 11–12 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5.

86. Zhang, H.; Wang, J.; Ding, Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy* **2019**, *180*, 955–967. [CrossRef]

87. DeCusatis, C.; Lotay, K. Secure, decentralized energy resource management using the ethereum blockchain. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security And Privacy in Computing and Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1907–1913.

88. Li, Z.; Bahramirad, S.; Paaso, A.; Yan, M.; Shahidehpour, M. Blockchain for decentralized transactive energy management system in networked microgrids. *Electr. J.* **2019**, *32*, 58–72. [CrossRef]

89. Laszka, A.; Dubey, A.; Walker, M.; Schmidt, D. Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers. In Proceedings of the Seventh International Conference on the Internet of Things, Linz, Austria, 22–25 October 2017; pp. 1–8.

90. Bergquist, J.; Laszka, A.; Sturm, M.; Dubey, A. On the design of communication and transaction anonymity in blockchain-based transactive microgrids. In Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, Las Vegas, NV, USA, 11–15 December 2017; pp. 1–6.

91. Guan, Z.; Si; G.; Zhang, X.; Wu, L.; Guizani, N.; Du, X.; Ma,Y. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. *IEEE Commun. Mag.* **2018**, *56*, 82–88. [CrossRef]

92. Kamal, M.; Tariq, M. Light-weight security and blockchain based provenance for advanced metering infrastructure. *IEEE Access* **2019**, *7*, 87345–87356. [CrossRef]

93. Gai, K.; Wu, Y.; Zhu, L.; Xu, L.; Zhang, Y. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. *IEEE Internet Things J.* **2019**, *6*, 7992–8004. [CrossRef]

94. Olivares-Rojas, J.C.; Reyes-Archundia, E.; Gutiérrez-Gnecchi, J.A.; Cerda-Jacobo, J.; González-Murueta, J.W. A novel multitier blockchain architecture to protect data in smart metering systems. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1271–1284. [CrossRef]

95. Casado-Vara, R.; Prieto, J.; Corchado, J.M. How blockchain could improve fraud detection in power distribution grid. In Proceedings of the 13th International Conference on Soft Computing Models in Industrial and Environmental Applications, San Sebastian, Spain, 20–22 June 2018; Springer: Cham, Switzerland, 2018; pp. 67–76.

96. Gao, J.; Asamoah, K.O.; Sifah, E.B.; Smahi, A.; Xia, Q.; Xia, H.; Zhang, X.; Dong, G. GridMonitoring: Secured sovereign blockchain based monitoring on smart grid. *IEEE Access* **2018**, *6*, 9917–9925. [CrossRef]

97. Zhou, Y.; Guan, Y.; Zhang, Z.; Li, F. A blockchain-based access control scheme for smart grids. In Proceedings of the 2019 International Conference on Networking and Network Applications (NaNA), Daegu, Korea, 10–13 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 368–373.

98. Mylrea, M. Distributed autonomous energy organizations: Next-generation blockchain applications for energy infrastructure. In *Artificial Intelligence for the Internet of Everything*; Academic Press: Cambridge, MA, USA, 2019; pp. 217–239.

99. Brilliantova, V.; Thurner, T.W. Blockchain and the future of energy. *Technol. Soc.* **2019**, *57*, 38–45. [CrossRef]