energies

MDPI

Review

Blockchain and Machine Learning for Future Smart Grids: A Review

Vidya Krishnan Mololoth *, Saguna Saguna and Christer Åhlund

Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, 971 87 Luleå, Sweden

* Correspondence: vidya.krishnan.mololoth@ltu.se

Abstract: Developments such as the increasing electrical energy demand, growth of renewable energy sources, cyber–physical security threats, increased penetration of electric vehicles (EVs), and unpredictable behavior of prosumers and EV users pose a range of challenges to the electric power system. To address these challenges, a decentralized system using blockchain technology and machine learning techniques for secure communication, distributed energy management and decentralized energy trading between prosumers is required. Blockchain enables secure distributed trust platforms, addresses optimization and reliability challenges, and allows P2P distributed energy exchange as well as flexibility services between customers. On the other hand, machine learning techniques enable intelligent smart grid operations by using prediction models and big data analysis. Motivated from these facts, in this review, we examine the potential of combining blockchain technology and machine learning techniques in the development of smart grid and investigate the benefits achieved by using both techniques for the future smart grid scenario. Further, we discuss research challenges and future research directions of applying blockchain and machine learning techniques for smart grids both individually as well as combining them together. The identified areas that require significant research are demand management in power grids, improving the security of grids with better consensus mechanisms, electric vehicle charging systems, scheduling of the entire grid system, designing secure microgrids, and the interconnection of different blockchain networks.

Keywords: blockchain; machine learning; smart grids; energy trading; electric vehicles; security; demand response management

Citation: Mololoth, V.K.; Saguna, S.; Åhlund, C. Blockchain and Machine Learning for Future Smart Grids: A Review. *Energies* **2023**, *16*, 528. https://doi.org/10.3390/en16010528

Academic Editor: Abu-Siada Ahmed

Received: 14 November 2022
Revised: 21 December 2022
Accepted: 23 December 2022
Published: 3 January 2023

1. Introduction

A wide range of solutions, beyond the classical one of building more lines, cables and transformers, have been proposed to modernize the power grid with new technologies, enabling a more smart automatic networked system. These solutions, typically using new technology, go by the name "smart grids" (SG) or "smart-grid technology". Conventional electric grids have limited abilities to cope up with the present increasing energy demand [1], whereas SGs can automate and manage the needs of the energy industry in a smarter way. The digital technology that allows two-way energy and information flow adds computing, controlling, monitoring and communication capabilities to the conventional power grid, making the grid smart [2]. The concept of distributed generation in SG helps to replace traditional energy sources (fossil-fuel-based) by renewable energy sources (RESs), such as solar and wind energy. This created a new type of grid user called "prosumers" who can generate, consume and trade energy locally. Demand response (DR) programs in SG aim to provide services to reshape demand/load curve by scheduling the energy generation/consumption of grid users. These programs allow users to be part of the electric grid operation by minimizing and shifting their electricity usage during peak periods based on market rates and providing incentives [3]. Electric vehicles (EVs) can also be used in DR programs, as they can act as energy carriers and mobile energy storage, which helps with de-carbonization

and green city development [4]. Grid-to-vehicle (G2V) and vehicle-to-grid (V2G) interaction allow electric vehicles to draw/deliver energy from/to the grid respectively. V2G is still in the conceptual stage; however, its potential for DR management is being explored.

Even though RES is considered one of the solutions to the energy problem, its integration causes challenges to the grid [5]. The unpredictable nature of RES and energy users has added an additional level of uncertainty within the users and the grid. However, at a large scale, to ensure security and efficient energy utilization, it requires large number of communications [6]. These communications should be maintained by a secure channel for ensuring complete grid security. Hence, the design of reliable and secure open communication system represents a key issue in SG deployments. Managing the increasing energy demand, number of electricity users, rise of EVs, energy trading and distributed generation using a centralized system is difficult. Such systems would require complex infrastructure and are effected by single point failure. Moreover, the privacy of users and security aspects will also become a major concern. With the current market structure that involves day-a-head predictions and intra-day predictions for determining energy price and trading, most of the time, energy predictions do not meet, which results in grid imbalance [7]. Hence, the proper scheduling and prediction of energy usage is necessary [8]. For all this, a sophisticated decentralized secure method and an intelligent system which can predict the amount of energy based on the usage pattern and energy demand are required.

Blockchain technology (BC) is a viable solution to overcome the issues of centralized system. BC is an immutable, distributed and P2P network that provides security, privacy and trust among peers using cryptographic techniques. It is the enabling technology behind the most popular cryptocurrency bitcoin [9]. However, the potential of BC was explored in many areas beyond cryptocurrencies, and the invention of smart contracts created a significant impact on several sectors, namely healthcare, markets, supply chain, cyber–physical systems and IoT [10–12]. In ref. [13], the authors explain the application of blockchain in healthcare. Ref. [14] explains the systematic review of blockchain applications in the supply chain. Ref. [15] demonstrates the performance analysis of blockchain enabled wireless internet of things. Ref. [16] proposes a novel blockchain enabled intelligent safe driving assessment framework and investigates the trustworthiness of distributed blockchain for connected and autonomous vehicles (CAVs) data. Ref. [17] proposes a secure and smart framework using blockchain for ensuring trading between heterogeneous radio communications. Ref. [10] performs a comprehensive survey on the application of blockchain technology in internet of things (IoT). In ref. [12], a review of blockchain applications in cyber–physical systems is given. The use of BC in the energy sector is also a key research topic, and several works related to energy trading, electric vehicle security, load balancing, grid security, etc., are in progress [18]. The key concepts of BC, such as encryption algorithms, consensus mechanisms, smart contracts, decentralization and distributed data storage, can be used as a solution to the problems faced in the energy sector today.

Machine learning (ML) techniques can be exploited to develop energy prediction algorithms and the proper scheduling of energy usage. A large amount of the energy consumption data of several users is generated from smart meters that also contain users' private/confidential information as well as sensitive information of utility providers. This high volume of data increases the complexity of data analysis. Hence, a ML model is needed that can handle such a large amount of data for ensuring proper SG operation while preventing data security attacks. Extensive research is being carried out in this field [19–21]. ML techniques applied in smart energy grids help in load prediction, faulty data detection, big data analysis, power quality measurement, DRM and weather forecasting [22]. Further, the accurate, early prediction of energy helps to balance the generation/consumption by the proper scheduling of energy usage [7,8].

To achieve a decentralized, secure, efficient network optimization and management, combined BC and ML solutions will give significant benefits [23]. Centralized ML techniques are inefficient and require many complicated parameters [24]. Similarly, BC can only achieve, at most, two of the three properties—decentralization, scalability and security—at

the same time. Motivated from these facts, the joint consideration of BC technology and ML techniques has many potential advantages in several fields, especially in the energy sector. BC principles, such as data security, distributed consensus, and immutability along with ML prediction algorithms will help to develop a secure, decentralized and balanced grid [25,26]. The major concern for applications considering BC and ML is (1) the ideal choice of the BC type, miners and consensus mechanism, and (2) the choice of a suitable prediction algorithm which provides a scalable, reliable, accurate and secure energy trading or charging system. Considering these aspects, we identify the need for a literature review in the area that can give insights into addressing the challenges arising from their combined use in smart grids.

The scope of this article (see Figure 1) is to understand the use of BC and ML techniques in SG applications. A number of surveys that address the integration of BC with SG are presented in [6,18,27–30], while others have looked into the integration of ML with SG [8,31]. From these, we identify the potential of integrating the combination of BC and ML for SGs. However, to the best of our knowledge, there is no extensive review that integrates BC and ML in the context of SG.

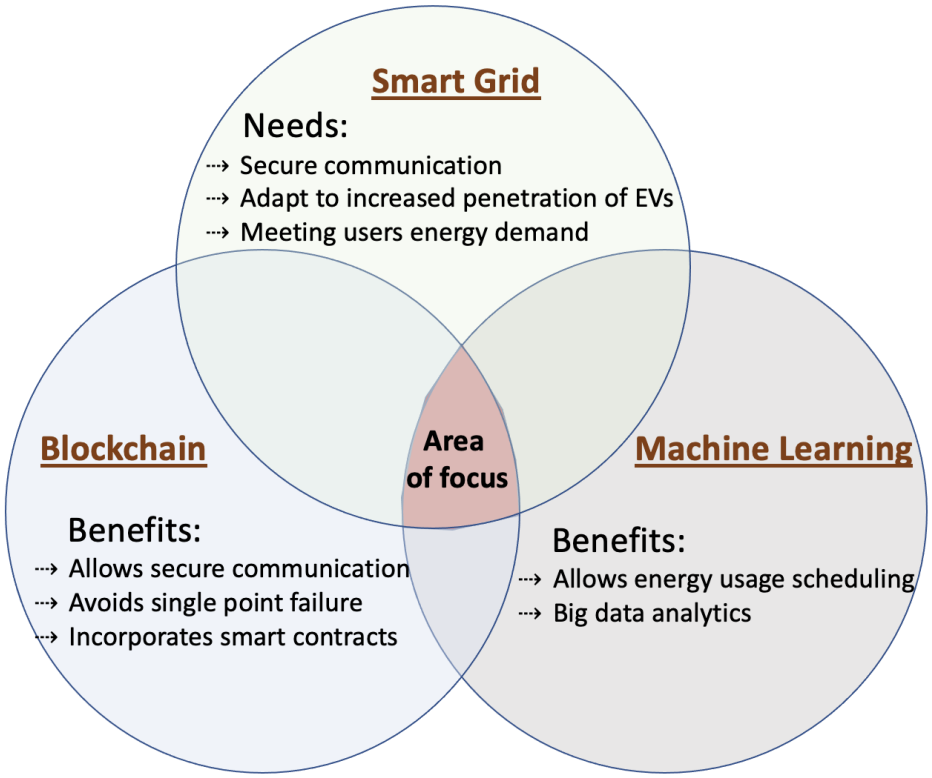

Figure 1. Scope of the paper.

In our review paper, we used the following methodology. We selected papers that were identified based on relevance, publication venue, and citations. We used the keywords "smart grid", "blockchain", "machine learning", "smart grid and blockchain applications", "smart grid and machine learning applications", and "smart grid, blockchain and machine learning". With the initial search, we identified the main smart grid application areas as energy trading, demand response management and electric vehicles. In this context, we reviewed more than 100 related research publications and aim to discuss the overview of SGs, BC, and ML, analyze and classify different approaches that model SG using BC and ML, and understand the existing research problems in this field. Our review specifically focuses on (1) SG security issues, (2) P2P energy trading, (3) EVs, (4) demand management using BC and ML, and (5) the interoperability of BC networks. There are studies that closely resemble our study ([25,32,33]), which evaluates the state of the art. However, our aim is

to identify the application of BC and ML in SGs and the benefits/challenges of applying both techniques together for smart grids. Our review helps the researchers to identify the BC, ML applications for SGs, existing research gaps and the need for further research to address those gaps.

The main contributions of this article include the following:

- An introduction and tutorial for the concepts of smart grid, blockchain technology, machine learning and associated challenges.
- Identifying the benefits and challenges of blockchain and machine learning techniques within smart grid application.
- Investigating the combined integration of blockchain and machine learning in the context of smart grid.
- Identifying the gaps in the research covering the integration of smart grids, blockchain and machine learning with a review of the existing works.

The outline of the survey is depicted in Figure 2. Section 2 deals with the necessary insights, terminologies and challenges of the topics involved i.e, SGs (Section 2.1), BC (Section 2.2) and ML (Section 2.3). Section 3 presents a review of works related to BC and SG, Section 4 presents a review of works related to ML and SG, and Section 5 presents a review of works that integrate BC, ML and SG. Further, Section 6 discusses the identified open challenges. Finally, in Section 7, the survey is concluded with a reflection of the observed gaps and findings.

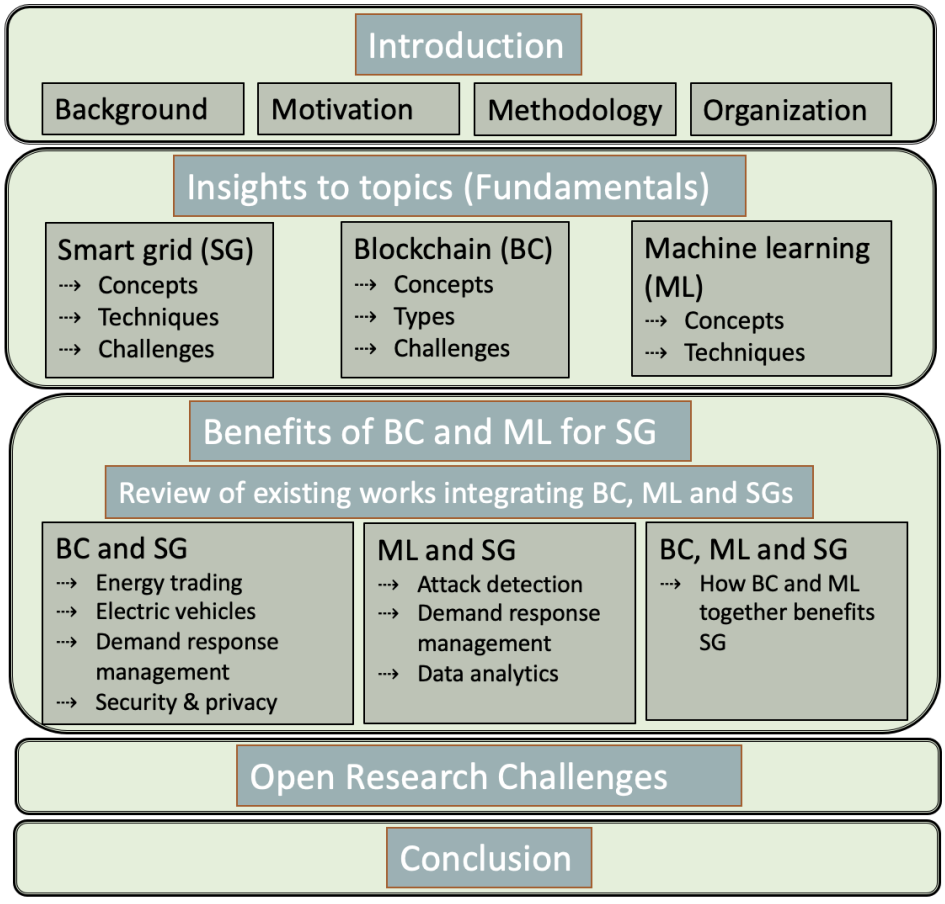

Figure 2. Outline of the paper.

2. Fundamentals

This section introduces the key concepts that are discussed throughout this article along with the associated challenges. A summary is provided at the end of the section.

2.1. Smart Grids

Traditionally, the term grid is referred to an electrical system that supports the generation, transmission, distribution and trading of electricity. Figure 3 shows an example of a traditional power grid. A traditional grid transports the electricity generated by large power plants to the electricity consumers. In the distribution network, the energy flow is only in one direction. However, there is a need to replace the electricity from fossil fuel (coal and gas mainly) and manage the increased electrification (EVs, but also in certain industrial processes) that results in higher consumption. Hence, alternative energy sources are required, i.e., RES. Traditional grids have only limited capability to incorporate these sources. Additionally, the introduction of several power converters in the grid give rise to power quality issues. Furthermore, the conventional grids lack controlling capabilities, automated analysis, response to rapidly changing loads and coordination between generated and consumed energy. All these issues will deteriorate the performance of the grid [34]. Changes in communication systems by taking advantage of internet achieve greater control and monitoring in the power system for flexible and efficient operation.

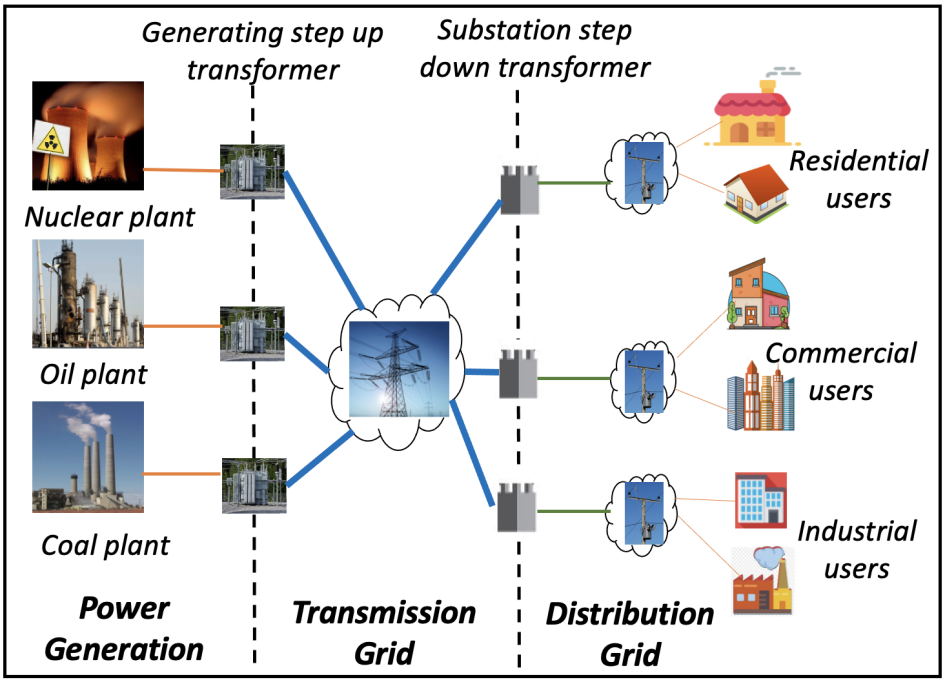

Figure 3. Traditional grid—example.

The smart grid utilizes information and communication technologies (ICTs) to revolutionize the traditional electric power system [35]. The term "smart grid" mainly refers to an improved or efficient power grid that allows the two-way flow of information and electricity. It can be considered the next generation of the power distribution system. Most of the governments and energy companies are performing extensive research on SG applications. The National Institute of Standards and Technology (NIST) [36] USA defines SG as "*A modernized grid that enables bidirectional flow of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications*". Authors in [37] define SG as "*an electric system that uses information, two-way, cyber-secure communication technologies, and computational intelligence in an integrated fashion across the entire spectrum of the energy system from the generation to the end points of consumption of the electricity*". SG enables more efficient integration of RESs, such as solar and wind. It employs digital technology that allows communication between devices, whereas a mechanical device is electrically operated in the traditional power grid, which does not allow communication between devices and self regulation. The power distribution from multiple plants and substations is possible in SGs, which aids in the overall load balance, avoids peak time strains and

minimizes the chance of power outages. Multiple sensors present throughout the line help to detect the exact location if a problem occurs and reroute power to where it is required, thereby limiting power interruptions. With these sensors and smart infrastructure, electrical companies can control and monitor power distribution and consumption effectively. Sensors can even detect issues on the transmission line and perform troubleshooting without external intervention. Figure 4 depicts the distributed structure of a smart grid. Some of the major advantages of SG over traditional power grid are listed in Table 1.

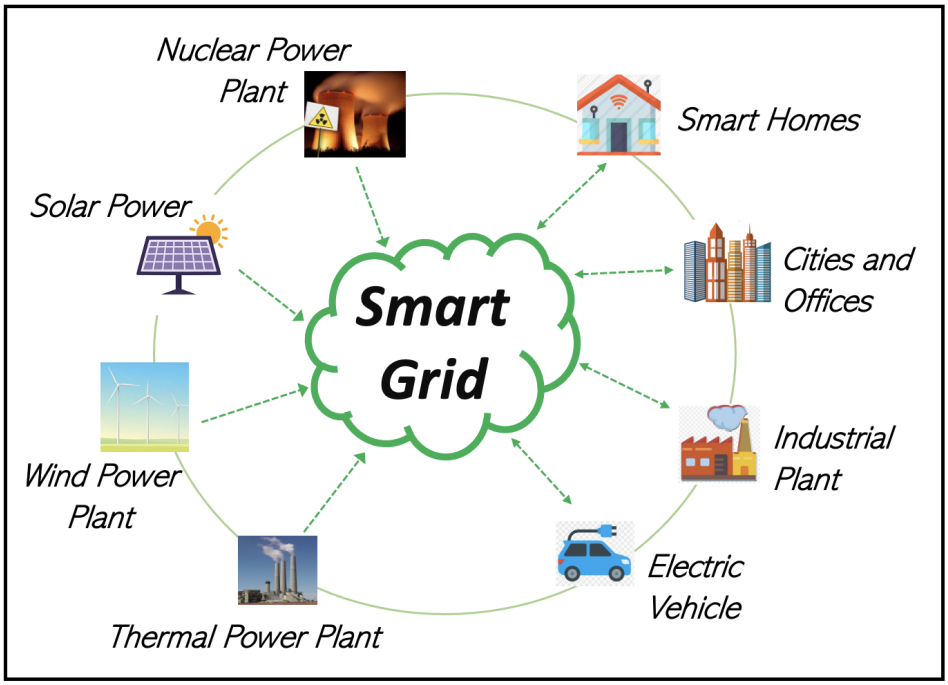

Figure 4. Smart grid—general example.

Table 1. Comparison between traditional and smart grid.

Characteristics	Traditional Grid	Smart Grid
Technology	Electromechanical	Digital
Sensors	Few sensors	Many sensors
Monitoring	Manual	Self
Restoration	Manual	Self-healing
Equipment	Failure and blackout	Adaptive and islanding
Control	Limited	Pervasive
Customer choices	Fewer	Many

Coordinating the needs of all generators, grid operators, users and electricity market stakeholders for operating all parts efficiently by minimizing costs and environmental impacts and maximizing system security and resilience is the main task of SG [38]. Some of the characteristics that are easier to execute with SG than with the existing technology are as follows:

- Enable consumer participation—Consumers can real-time monitor their electricity usage, which gives them choices to use their equipment efficiently.
- Distributed generation—Generators of all types and sizes can be accommodated. Micro-generations using RES are possible which help users to become prosumers.
- Power quality—Provides quality in power supply for varying grades. Advanced control techniques help to diagnose events that impact power quality, such as lightning, line faults, harmonics, etc.
- Optimize asset utilization and operating efficiency—With efficient asset management and delivery system, the assets can be used when they are needed.

- Enables new products and markets—Create an opportunity for users to choose among the available services. Access to various markets is opened due to the increased supply, transmission and DR initiatives.
- Resilient to disturbances, attacks and natural disasters—Self-healing capabilities help to reduce the number of power interruptions and provide better service.

2.1.1. Technologies in Smart Grid

(a) Smart meters—Smart meters are the new type of electricity meters installed by energy suppliers which helps users to save time, energy and money. These meters measure the amount of electricity used, allow to read them remotely, and displays the associated cost in the attached display device. The incorporation of smart meters has added a series of functionalities to the distribution systems, mainly automated meter reading, the automatic detection and isolation of issues, etc. [39]. Automated metering infrastructures (AMIs) are integrated with smart meters and communication networks, which allow two-way communication between customers and utilities. Additional features include tariff options, smart thermostat, tax credits, prepaid metering, appliance control and monitoring, etc.

(b) Vehicle to grid (V2G)—V2G refers to the process of feeding energy stored in the EV battery back to the main grid. This technology will help in keeping the grid balance at peak times. V2G helps a car battery to be charged and discharged based on different demand balancing needs. During demand response operations, energy can be fed to the grid from the EV battery, and during normal operations, EVs can charge their battery from the grid.

(c) Microgrids—Microgrids are a small power supply system that consists of distributed sources, such as solar, fuel cells, wind turbines, biogas, etc. These small grids can be connected to the utility grid (grid mode) or can be operated independently when isolated from the main grid (island mode) during any fault or disturbances. This increases the quality of the supply, efficiency and helps to provide customers cheaper and clean energy.

2.1.2. Challenges and Security Issues

The smart grid incorporates several advanced technologies to the conventional electric grid. However, it is still facing many technical and security challenges in deployment. These challenges are mainly associated with the incorporation of new technologies, lack of policies, infrastructure issues, socio-economic issues and lack of awareness.

(a) Security issues: Effective and secure communication should be met in all domains of SG, i.e., generation, transmission and distribution. All systems should satisfy the main security objectives, which are confidentiality, integrity and availability (CIA triad) [40]. Confidentiality refers to the protection of data from unauthorized access. Integrity refers to protecting the data from tampering. Availability ensures that the information is available to authorized users whenever needed. Most of the SG cyber attacks target one of the CIA triad [41]. Thus, for a secure system, strict authentication and access control should be enforced, attack detection and countermeasures must be used, security objectives should be defined in all layers, and the investigation of vulnerabilities should be performed.

(b) Centralization issues: In most countries, the existing grid does not have the potential to accommodate all the needs for SG. The incorporation of RESs for clean energy and distributed generation result in several challenges in the design, operation and maintenance of the grid [27]. The connectivity also becomes larger. Thus, the major challenge that arises is to accommodate a large number of transactions between prosumers and a large number of connections, such as distributed energy producers, consumers, EVs, and smart devices, within a centralized grid architecture. Controlling and managing all the activities using a centralized system would be very complex and challenging.

(c) Energy management: Demand response management is a major objective of SG. The goal is to allow network operators to manage the user electrical loads by providing incentives [42]. Residential users or other consumers receive incentives for shifting their electricity usage to non-peak times, thereby reducing the peak-to-average load in the grid. However, the interconnection of utility companies, consumer, and microgrids can be made possible only with efficient demand response management programs. The complex interactions between companies and users with proper pricing schemes makes this challenging.

(d) Handling massive data generated: Massive data are generated from the grids by many intelligent devices together and are transmitted over networks. These data include metering data, control messages and pricing/tariff information. The high volume of data generated from smart meters will increase system complexity and make analysis difficult [43]. Thus, these large amounts of data, termed "big data", must be processed and analyzed efficiently by implementing different security solutions.

(e) P2P energy trading: RESs give users chance to generate energy by themselves, and users can trade their surplus energy to others in a P2P manner without relying on traditional utility providers. However, the traditional energy market carries out most transactions using a centralized system. This type of market mechanism is not flexible enough, and the electricity price cannot fluctuate with the market demand [44]. Thus, a decentralized, flexible, P2P system for the effective buying and selling of electricity is missing.

(f) Integration of electric vehicles: BEV (battery electric vehicles) and PHEVs (plug-in hybrid electric vehicles) are gaining attention due to their mobile and highly dispersed character. They also integrate V2G communication, where the electricity from car batteries can be delivered to the grid, which in turn can help in demand-side management [4]. However, V2G is still at the conceptual stage and lacks practical and realistic frameworks for its implementation, which adds challenges to its adoption.

An efficient and reliable SG network requires secure communication, a P2P energy trading platform, the management of energy consumption/generation using DR programs, etc. For developing such networks, BC technology and ML techniques can be explored. The next two sections (Sections 2.2 and 2.3) explain these concepts in detail.

2.2. Blockchain Technology

Blockchain (BC) is a digital, decentralized (distributed) ledger that records all transactions occurring across a P2P network. BC concept was first introduced by Satoshi Nakomoto in a white paper titled "Bitcoin: A peer to peer electronic cash system" [9], but no clear evidence about the author's identity is available. This paper is the backbone of bitcoin cryptocurrency, and later more studies were performed to understand the underlying technology of the bitcoin system, i.e, BC technology. It was originally proposed to tackle double-spending problems in financial transactions. Later, the technology won a reputation for its two main critical factors: (1) data immutability; and (2) data indestructibility. In a simple definition, it is an interlinked and expanding chain of blocks which securely records data. Each block is connected to the previous block using secure hashing algorithms by generating a cryptographic hash value for each block. Altering a transaction in BC retroactively requires altering not only the current block hash, but also the cryptographic hash of all the blocks down the chain. The major techniques behind BC is the principle of hashing and consensus algorithms, which ensure security. A new block can be added only if consensus is achieved among the nodes. A distributed system such as BC holds benefits over centralized architectures, as it provides the same verified information to all network members [11]. Ethereum is an open-source BC platform with a Turing-complete scripting language to include smart contract functionality [45]. Ether is the second largest cryptocurrency after bitcoin, and it is among the most actively used BC platforms [46]. A smart contract is a computer script that can be deployed in BC and record conditions or events. When conditions are met or events are reached, the contract will be automatically

triggered and executed, which avoids centralized control [47]. Solidity, a high-level object-oriented programming language, is the primary language for writing these contracts [48]. Hyperledger is an open-source BC platform that uses permissioned BC networks, developed by the Linux foundation in December 2015 [49]. It can be used to develop various BC-based systems and applications for industrial use. However, it does not support cryptocurrencies, such as bitcoin and ethereum.

2.2.1. Blockchain Structure

Blockchain, as the name suggests is a chain of blocks. The typical structure of BC is shown in Figure 5. The main attribute of BC is that it can track changes in each block so that no block can be altered or removed from the chain. As seen in the figure, each block is linked to the previous block using a hash value. The first block in the chain is called the genesis block and the previous hash value will be zero since it is not linked to any preceding block. Each block in the chain consists of the block Id, nonce, previous hash, difficulty, merkle root hash, hash of the block, list of transactions and time stamp.

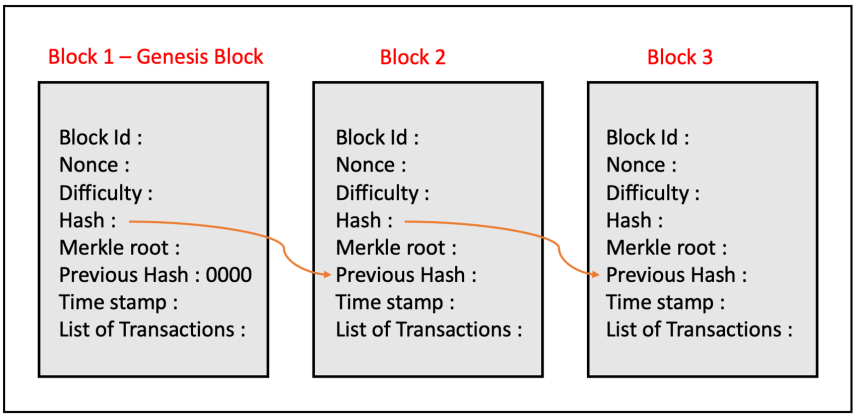

Figure 5. Blockchain structure.

The block Id is a unique identifier for each block in BC. The nonce value indicates the 32-bit integer calculated by miner to solve the intense proof-of-work consensus algorithm by meeting the defined level of difficulty. A hash code will be generated by a hash function that converts a specific input into a string of letters and numbers of fixed length. SHA-256 (secure hash algorithm) is one of the widely used hash functions. Inputs of any length will generate a fixed length output, and any small change in input will change the hash in an unpredictable way, i.e., if any data alteration happens, the hash value will change. As blocks are linked with previous blocks using the hash value, an attacker would have to recalculate all sets of hashes to hack the network, which is very difficult and makes the network immutable. Each block holds a list of transactions. The number of transactions that can be placed in a block are constrained, and the maximum block size for bitcoin is 1 megabyte. The merkle root is the hash of the hashes of all transactions in the block. It is formed by hashing pairs of transactions repeatedly until one final root hash (merkle root hash) is left. The timestamp indicates the block creation time.

2.2.2. Types of Blockchain

Generally, based on permissions given to users to participate in block creation and accessing block contents, BC can be divided into three types, namely public, private and consortium [18]. Table 2 summarizes the three types of BC.

Table 2. Comparison of different types of blockchain.

Property	Public Blockchain	Private Blockchain	Consortium Blockchain
Participants	Anyone anonymous, may be malicious	Single organization, identified and trusted	Multiple trusted organizations
Block creation	All miners	One organization	Selected set of nodes
Level of centralization	Low	High	Medium
Consensus process	Permissionless	Permissioned	Permissioned
Transaction speed	Slow	Lighter and faster	Lighter and faster
Main feature	Self established credibility	Efficiency and cost optimization	Transparency and traceability

2.2.3. Features of Blockchain

Some specific characteristics make BC different from other similar technologies. The main features include decentralization, immutability, transparency, security, auditability, fault tolerance, and anonymity.

- Decentralization—With the adoption of P2P communication among nodes, transactions are generated, recorded and validated by nodes itself without the need of centralized control. By this way, BC avoids the challenges caused due to centralized servers.
- Immutability—The records made on BC are irreversible and non-repudiable because of the one-way cryptographic hash functions. All the entries made are agreed and verified by peers. To alter any record, an attacker has to compromise the majority of the nodes, which is very difficult;
- Transparency—The complete copy of all transactions and records are stored and available to all the nodes on a public BC or to the permissioned nodes in a private/consortium BC. This transparency adds credibility to the BC data.
- Security—All transactions in BC are broadcast, verified, validated and linked by the nodes in a distributed network and use cryptographic techniques. This decentralized consensus adds more trust and difficulty to break.
- Fault tolerance—Any fault or data tampering can be easily detected due to the distributed nature, as all peers have the complete copy of BC ledgers.
- Auditability—All nodes in the public BC or permissioned BC hold the copy of BC and can audit, verify and trace all timestamped transaction records.
- Anonymity—In BC, the defined addresses are not associated with the real identity of users, which provides privacy to participating nodes to a large extent.

2.2.4. Consensus Mechanisms

A consensus mechanism ensures trust in any type of BC network. There is no central authority to verify transactions in BC, yet all transactions are secured and verified. This is achieved using suitable consensus algorithms, which is the key component in the BC network. These algorithms determine which block has to be added in the chain [50]. A set of miners/validators in the network will reach a common agreement about the present state of the system and decide whether the block is valid or not. Hence, it ensures that each added block is the true and only version, which is agreed by all other nodes in a distributed network. Some of the popular consensus algorithms used in BC are proof of work (PoW), proof of stake (PoS), delegated PoS (DPoS), practical Byzantine fault tolerance (PBFT) and proof of authority (PoA). A comparison of these algorithms is given in Table 3.

(a) Proof of work (PoW): In PoW, nodes race to solve a cryptographic puzzle that is difficult to solve, but easy to verify, to add a new block in the chain. It require large computational power, and the node which solves the puzzle first will win the race. By adjusting the nonce value, they have to achieve a target hash defined by the network. The calculation of the target hash by varying nonce requires large computational power, and it increases as the difficulty level increases. PoW is mainly adopted by bitcoin, and the transaction throughput per second (TPS) for bitcoin is 3–7. However, to attack the network, attackers need to accumulate a large amount of computational power to

create a longer chain than the valid chain, i.e., if the attacker has more than 50% of the computational power compared to the whole network, the BC will be compromised.

(b) Proof of stake (PoS): PoS was introduced to overcome the drawbacks of PoW. PoW is based on the computational power competition, whereas in PoS, the mining power is determined by the total number of coins owned by a user. So if the miner has more stakes or money, then it has a higher chance of mining a block. Hence, PoS is energy-saving compared to PoW; however, only the wealthier nodes get a chance to participate in the consensus, which makes the system centralized around those miners. Small bidders will not get a chance to create a block in PoS. In PoW, an attacker has to acquire 50% of the hash rate to attack, which may be easier, whereas in PoS, it is difficult and expensive to obtain more than 50% of the total coins, which makes it more secure.

(c) Delegated proof of stake (DPoS): It is a variant of PoS. Here, only selected "delegates" which are elected by other nodes can create and validate a block. By voting, stake holders give their right to the delegates they support for creating the block. This makes the verification process faster, compared to PoS. If the delegates fail to generate blocks, they will be dismissed, and new delegates will be selected. Compared to PoW and PoS, DPoSs are more efficient and low-cost consensus algorithms.

(d) Practical Byzantine fault tolerance (PBFT): PBFT is widely used in private and permissioned BC networks. It mainly involves five phases: request, pre-prepare, prepare, commit and reply. PBFT can handle up to 1/3 (33%) malicious nodes. Unlike other algorithms, PBFT does not require resources to achieve consensus, instead using the Byzantine fault tolerance approach. However, its scalability is significantly smaller, as the message complexity increases with the increase in number of nodes. This communication overhead makes it unsuitable for large-scale applications.

(e) Proof of authority (PoA): PoA can be viewed as a modified PoS algorithm which is specifically designed for permissioned BC. Here, the participant has to confirm its identity in the network for becoming an authority to publish a block. In PoS, validators should have more coins/stake, whereas in PoA identity of participant is considered as a stake. Network participants trust the authorized nodes and a block will be accepted if the majority of authorized nodes sign that block. Even though the method appears to be centralized, it is proving popularity in the energy sector. Energy web foundation [51], which can achieve a confirmation time of 3–4 s and can scale to almost a thousand transactions per second, makes use of the PoA algorithm.

Besides the above-mentioned popular consensus algorithms, there are many others which include proof of activity (PoAc), proof of burn (PoB), proof of elapsed time (PoET), ripple, and so on. However, based on applications, a suitable choice of consensus algorithm has to be made. There is no perfect protocol as such. There will always be a trade-off between consistency, availability and fault tolerance [50]. The choice of consensus protocol determines performance characteristics, such as scalability, transaction speed, transaction finality, security and the spending of resources, such as electricity.

Table 3. Comparison of different consensus algorithms.

Consensus Mechanism	PoW	PoS	DPoS	PBFT	PoA
Main idea	Computational power determines addition of block	Stakes in hand determines the chance of adding block	Voting and stakes of nodes determines chance of adding block	Based on Byzantine fault tolerance approach	Only set of authorized nodes are able to add blocks
Energy consumption	High	Low	Low	Low	Low
Scalability	Good	Good	Good	Bad	Good
Fault tolerance	50%	50%	50%	33%	50%
Level of centralization	Low	Medium	Medium	High	High
Application	Public	Public	Public	Private	Private

2.2.5. Challenges and Security Issues

The critical features of BC provide many benefits to solve the centralization and security issues in most of the sectors. Even though the main application of BC is in cryptocurrency, now many other sectors are exploring the advantages of applying BC in their field [52], such as markets, internet of things (IoT), health care, supply chain management, vehicular networks, energy sector and so on. Most of these applications are still immature, and extensive research is ongoing. Even though BC is being rapidly used in different application areas, as an emerging technology, it faces multiple challenges and problems.

(a) Blockchain forks: Forks is a condition where splits occur in the chain of blocks. This is mainly due to the diverging views of nodes regarding the present state of network. Forks arise due to the vulnerabilities in BC structure which may finally result in compromise of any BC based application [53]. These can be either hard forks or soft forks. Figure 6 shows a hard fork scenario. Hard forks are irreversible and may result in a permanent split within the chain. In soft forks, only one chain will remain valid. Resolving soft forks is comparatively easy. When all the blocks come to a consensus about the true state of the system, soft forks can be removed. However, resolving hard forks is challenging.
There are other forms of inconsistencies that occur in the BC that will leave valid blocks outside the long chain. These blocks are called stale blocks and orphaned blocks. Stale blocks are blocks that are successfully mined, but not accepted in the longest chain. This occurs mostly in public BC where many miners race to solve the puzzle and two or more miners will come up with the solution. From these blocks, network will choose one as winning block and neglect the others, resulting in stale blocks. Orphaned blocks are blocks which are linked to the previous block that is not in the longest chain. In Ethereum, these orphaned blocks are called uncle blocks.
Figure 7 shows stale and orphaned blocks in the chain. The bottom block 2 and block 4 are stale blocks, which are valid but not on the long chain. Block 5 is a orphaned block whose previous block is valid but not in the long chain. Stale blocks or orphaned blocks can be avoided by adjusting the networks' difficulty level.

(b) Issues in consensus algorithms: Consensus algorithms decide who can add a block in BC [50]. These algorithms will determine the performance characteristics of the system, mainly, scalability, transaction speed, security, the spending of such resources as electricity, etc. As seen in Section 2.2.4, there are many consensus algorithms. Even though PoW is the widely accepted algorithm and has high scalability, its main drawback is the high computational power requirement [54]. BBC news quoted that "Bitcoin consumes more electricity than Argentina" and it consumes around 121.36 terawatt-hours (TWh) in a year [55]. PoS was introduced to overcome the inefficiency of PoW and it has high fault tolerance (50%) since it is difficult to acquire more than 50% of the total coins. However, as block addition is dependent on the number of coins with the nodes, it is always rich validators that have the chance of making the poor nodes poorer. PBFT, which is different from PoW and PoS, is only suitable for private/permissioned BC applications because of its communication overhead as the number of nodes increases. Additionally, the system becomes compromised if the primary node is relaxed. In PoA, known validators validate the transactions in the blockchain network and do not involve any complex mining process as PoW. Hence, it does not require any computational power, and the energy consumption is minimal. However the method is partially centralized.
From all these observations, even though there are many consensus algorithms, no perfect algorithm can be found [56]. Each algorithm has its own benefits and limitations. Depending on the requirement and application, a proper choice has to be made.

(c) Blockchain Trilemma: It addresses the challenges faced by the BC developers while implementing a secure, decentralized and scalable BC system, without compromising any one [57]. Security defines the ability to defend against attacks and bugs; decentralization avoids a central point of control; and scalability determines the ability to handle

large number of transactions. If decentralization and security are more prioritized, then scalability becomes a challenge, i.e, number of transactions a chain can handle will be less. Likewise, security can be compromised with network shifts which offer scalability. Hence the trilemma says that it is difficult to achieve all three properties simultaneously. There are several techniques that are being adopted to improve this, mainly, improved consensus protocols, sharding, light networks and sidechains.

(d) Transaction confirmation time: In blockchain, when a transaction is made, it takes some time to add that transaction to the chain of blocks. This waiting time depends on the type of consensus algorithm and blockchain platform [58]. For example, Bitcoin with the PoW consensus takes 10 min to add a new block. This is because, in PoW, numerous miners are racing each other to solve a cryptographic puzzle and only the winner adds the transaction to the block. For PoS-based networks, miners are replaced with stakers and the node with highest stake adds the transaction to block. Hence, Ethereum with PoS takes much less time to mine a block. PoA-based networks can process transactions at a faster rate since only a few number of trusted validators are involved in adding transactions to the block.

(e) Issues due to peer to peer architecture:

- Selfish mining: Some selfish miners will deliberately keep their blocks private without broadcasting it to the public when created and continue the mining process to build a longer chain [59]. Selfish miners will publish their blocks when the length of their private chain starts approaching the public BC length and reap the rewards. If their computational power is high, they can win the race easily. This will leave the honest miners into an inconsistent state by rejecting all their transactions. Introducing unforgettable timestamps and preference of recent blocks can somehow manage selfish mining issues.
- Majority attack (51% attack): This type of attack occurs when a single or group of malicious nodes in the network acquires the majority of the network hash rate to make changes in the blockchain. If these nodes attain 51% or more computing power, then they can calculate the nonce value relatively faster than other nodes and decide on block additions. This will prevent other miners from adding their blocks and may create a fork condition in the chain. The monopoly created by malicious nodes can result in fraudulent transactions added to the chain. Many modifications to PoW design was explored to counter majority attacks [53].
- Distributed denial of service (DDoS): These are most common attacks in online services. The majority attack or 51% attack can lead to denial of service (DoS) in the network. When a group of malicious nodes acquires more than half of the hashing power, they can deny other miners from adding their mined blocks to the chain, perform false transactions, modify ongoing transactions and can finally cause service failure in the BC network [53]. Intentional forks due to selfish mining may also result in DoS in the network.

(f) Ingestion and anonymity: Public BCs are open to everyone and provide open data accessibility to the public. This may reveal the personal information to an attacker when the network is compromised, and this is called BC ingestion, which may not be desirable to the users. One of the main features of BC is anonymity, as users are defined using addresses which are not linked to their real identity. However, this property has become a threat within cryptocurrencies, which makes them a major source of money transferring for illegal activities associated with the deep web [53]. Using real/fiat currencies for transfer can be tracked by law/government. Since cryptocurrencies preserves anonymity, transfers will not leave any traces of the real user, which results in increased illegal transactions. This is one of the reason why various countries have banned cryptocurrencies.

(g) Vulnerabilities in smart contracts: A smart contract is a piece of program that automates the activities in BC, mainly Ethereum. If these contracts are not properly written, it can be a surface of attack in the BC network [56]. Deficiencies in the code and execution

environment may lead to series of attacks. Smart contracts are mostly written in solidity language. A small mistake while writing the code may create a large impact [60]. For example, if a user is not updating the balance in the account after a transfer, an attacker can steal money by recursive function calls [53]. There are many similar issues associated with smart contracts. However, writing the contract properly by avoiding programming mistakes and eliminating issues with the associated platform can solve these issues.

Blockchain technology is transforming most fields. However, as an emerging technology, it is also facing some challenges. Most of the issues in BC are interrelated and arise due to the BC structure and P2P architecture. Proper choices of the blockchain type, consensus algorithms and encryption techniques related to the application of interest are required to overcome these issues.

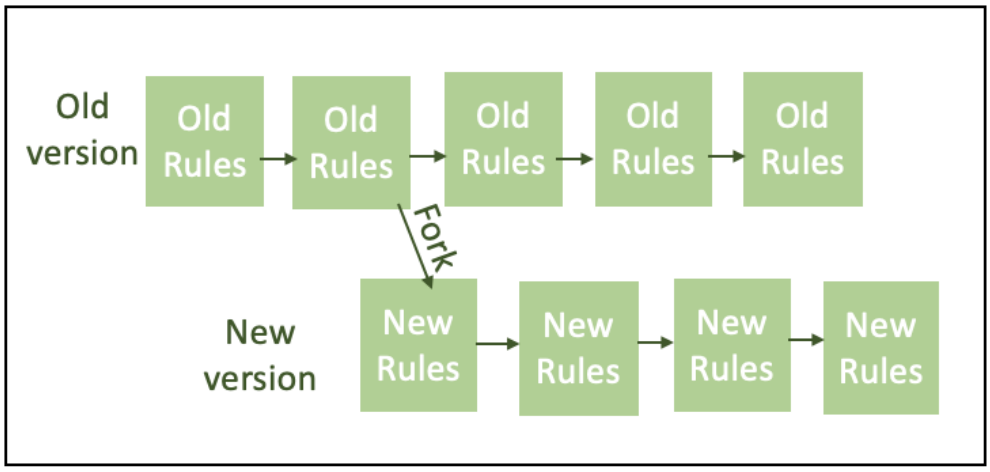

Figure 6. Blockchain forks.

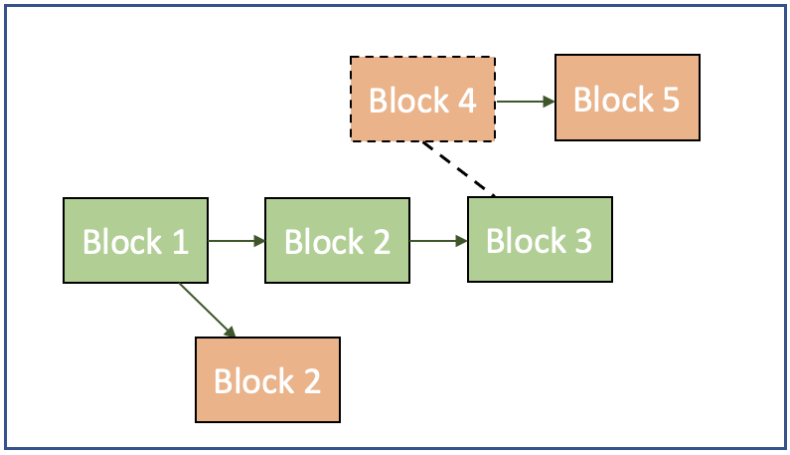

Figure 7. Stale blocks and orphaned blocks.

2.3. Machine Learning

Machine learning will give computers the ability to learn without being explicitly programmed. A better definition for ML was given by Tom M. Mitchell as "a computer program is said to learn from experience E with respect to some class of tasks T and some performance measure P, if its performance on T, as measured by P, improves with experience E" [24]. More clearly, as computers/models are exposed to a set of new data, they will adapt independently and learn from previous patterns to interpret available data and identify hidden patterns. ML adopts techniques from diverse set of disciplines that include philosophy, probability, information theory, statistics, control theory, artificial intelligence and so on [23]. ML algorithms are being used in various applications domains, such as financial services, marketing and sales, government, healthcare, transportation, and so on.

ML techniques can be generally classified into four categories: (1) supervised learning; (2) unsupervised learning; (3) semi-supervised learning; and (4) reinforcement learning. Figure 8 classifies different ML techniques.

(a) Supervised learning algorithm: Here, the machine is taught based on a set of labeled datasets to construct a model that represents relationships between input and output for predicting future output values [61]. The algorithm needs to find hidden patterns in the data and learn from observations to make predictions. Thus, the main objective is to come up with a mapping function that maps input data to output data, using this function to determine outputs for new unknown inputs. Depending on the type of output variable, supervised learning problems are of two types: the classification problem when output is categorical, and the regression problem when outputs are continuous values in a range. A list of some of the supervised learning algorithms includes linear regression, support vector machines (SVM), logistic regression, decision trees, neural network and k-nearest neighbor.

(b) Unsupervised learning algorithm: Here, the machine studies data to identify hidden patterns from the set of unlabeled input data. The algorithm tries to organize the data to describe the structures. The main idea of unsupervised algorithms is to classify the dataset into different sets based on similarity between them. Widely used learning techniques are clustering, which involves the grouping of similar data and dimension reduction that reduces the number of variables being considered [61]. A list of some of the unsupervised learning algorithms includes hierarchical clustering, K-means clustering, mixture models, neural networks, expectation–maximization algorithm and principal component analysis (PCA).

(c) Semi-supervised learning algorithm: This type of learning algorithm is a mix of supervised and unsupervised learning algorithms. Here, most of the training data samples are unlabeled and some are labeled. So, by utilizing the labeled data, these learning algorithms can improve learning accuracy compared to unsupervised learning algorithms [24].

(d) Reinforcement learning algorithm: Unlike other learning algorithms, the reinforcement learning algorithm focuses on finding the best path to select in a situation that maximizes rewards. It is a sequential algorithm, where each step it takes is to maximize the reward, and these rewards can be either positive or negative. The ML algorithm is provided with a set of actions, parameters and end values, and tries to explore different options and possibilities to determine the optimal output solution, i.e., by the trial and error method. These models learn from experiences and adapt the approach based on responses in different situations. Q-learning is the most popular reinforcement learning algorithm, where a Q-function is used to learn [24]. Some of the applications of reinforcement algorithms are computer-played board games (chess), self-driving cars and robotic hands.

ML techniques are mainly categorized into four categories and are widely used in various fields. In the energy sector, ML techniques can be used to predict energy user behavior based on usage patterns, and analyze the big data generated from smart meters, energy forecasting, power quality measurement and DRM. However, the choices of a suitable algorithm, datasets and processing techniques have to be made effectively.

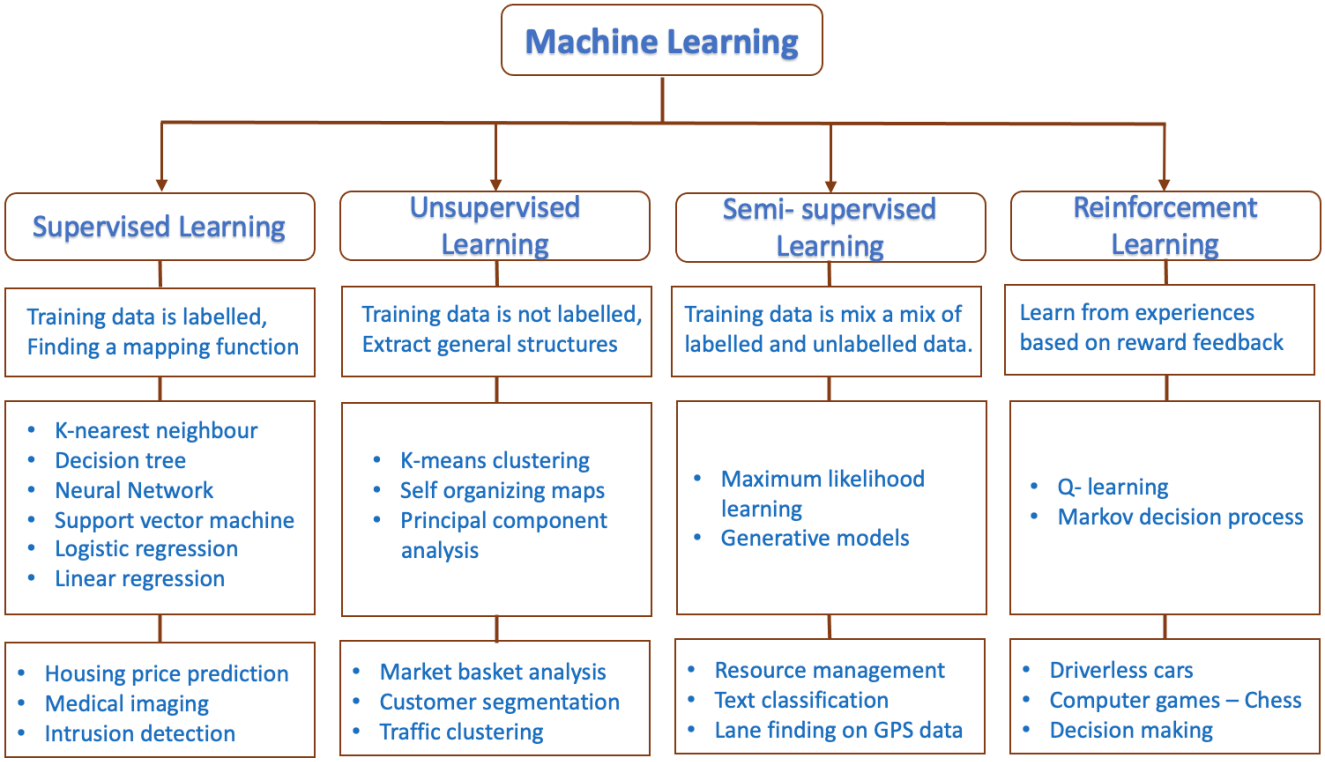

Figure 8. Machine learning algorithms—overview.

3. Review of Blockchain in Smart Grids

The use of BC technology in the energy sector is a key research topic nowadays. As the energy industry is undergoing tremendous transformations with the adoption of ICT, it has become a prominent research area. Intelligent grid implementation with minimal power loss, high power quality, reliability and security are the main goals to be attained. Many research works introduce BC technology in the energy sector for achieving these goals [6,18,27,28,32]. However, more research is required. In this section, the main idea of SG and BC integration, its benefits and potential opportunities related to several existing works is discussed.

The distributed architecture of SG is depicted in Figure 4. However, maintaining all these distributed functionalities by a single centralized server is complex and highly vulnerable [6]. The ultimate aim of all the transformations in the grid is to reform the existing energy industry by bringing producers and consumers closer to each other using distributed generation and resources. In centralized systems, all the users, energy operators and market system interactions are dependent on central entities. These intermediaries can monitor, control and support all activities within the elements in the grid [18]. Additionally, the long-distance transmission network is opted to deliver energy to end users through distribution stations. The increase in the number of elements associated with the grid raises some concerns [27], which include scalability, reliability, availability, communication overhead and so on. All of these issues point toward the need for a decentralized structure for energy grids to create a more dynamic and flexible grid structure [50].

Security, energy management, EV charging and energy trading are also some of the areas to be transformed and implemented effectively. As users are becoming prosumers through distributed generation, they can trade electrical energy to other grid users. Traditional methods fail to provide a secure and flexible energy trading platform [44] where users can trust each other. Due to privacy and security concerns, most of the users show less interest in participating in energy trading. Hence, a decentralized platform which can create a trust environment for secure energy trading is required. Indeed, the penetration of EVs also has effects, as energy trading between EVs can also be done [62]. EV users have concerns about charging their vehicle from anywhere because of security reasons. At the

same time, the proper scheduling of EV charging is also necessary for balancing the entire grid, which is a problem to be addressed.

All these issues, mainly, the need for decentralization, security and in building the trust platform for trading without third party intervention, point toward the use of emerging BC technology [63]. Applying BC technology in the energy sector has many potential benefits and can avoid most of the bottlenecks in the development of smart grid. Many studies and industry experts believe that BC adoption will eventually help for a smooth shift toward smart grid [6,18,29,63,64]. Figure 9 represents a model for blockchain-enabled future smart grid.

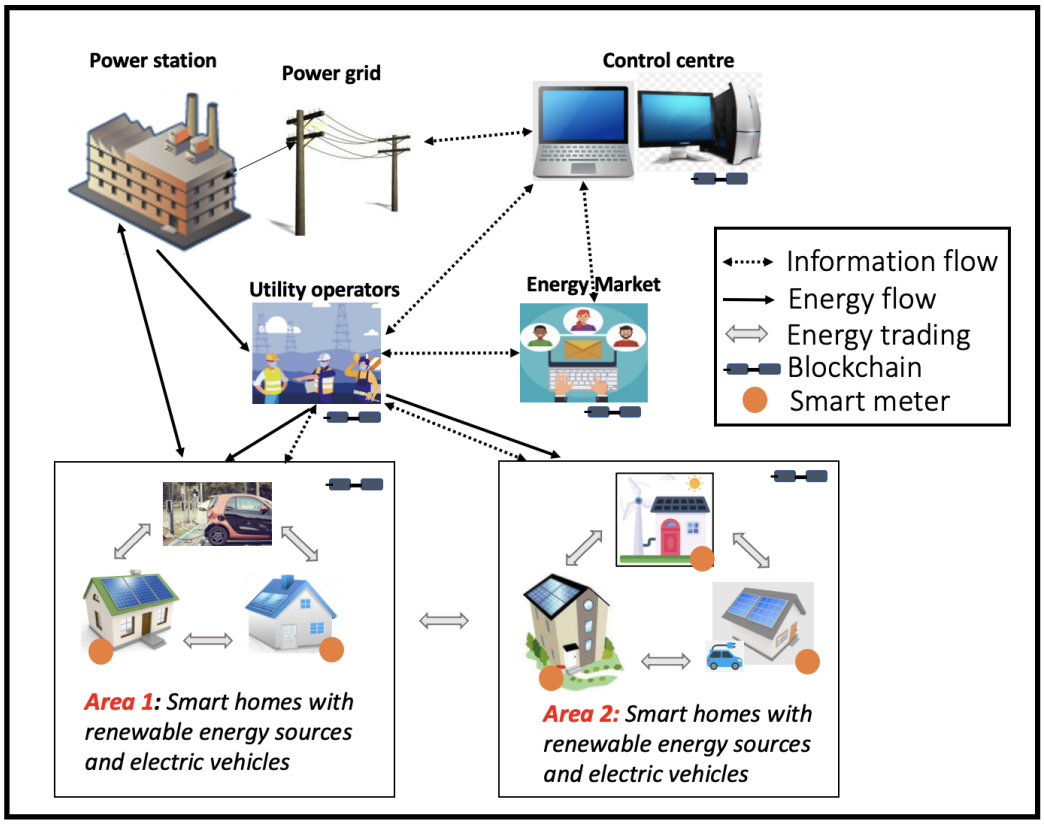

Figure 9. Blockchain-enabled future smart grid.

The main motivation of applying BC technology is to achieve an increased level of security [65]. Since BC uses cryptographic techniques and a ledger is shared among all peer nodes, data alteration is not possible unless the majority of the nodes become malicious. As all the network nodes can verify the transactions and records, it adds transparency to the system. Due to secure hashing algorithms, any malicious activity or faults in the communication network are easily identifiable and recovered easily, which makes the system resilient to attacks. Above all, the most important benefit comes from the secure scripting using smart contracts, which can automate the transactions by automatically executing them when certain conditions are met. Thus, with all these critical features and cryptographic techniques, BC adoption promises to be a suitable alternative to traditional centralized systems with increased security, resilience, privacy and trust [66].

The United States (US) is the first country in the world that has applied combined energy and blockchain to practical applications [67]. Applied engineering projects combining energy and blockchain in the US are Brooklyn microgrid, Filament, Shared EV charging pile and Omega grid. There have been many other implementations made in several other countries, but research and advancements are still ongoing. Table 4 lists some of the existing projects related to SG and BC.

Table 4. Different energy and blockchain projects.

Name	Company	What They Do?
Exergy [68]	Lo3 energy and ConsenSys	Buy/sell locally generated renewable energy over P2P network
Power Ledger [69]	Power Ledger pty ltd	Develop blockchain based P2P energy trading system
SolarCoin [70]	SolarCoin Foundation	Cryptocurrency to provide rewards to solar power producers
Energy Web chain [51]	Energy web foundation	Energy blockchain platform for low-carbon and user centric energy transactions
Pylon network blockchain [71]	Pylon network	Blockchain platform for energy sector
Sunchain [72]	greenTech Verte	Blockchain platform for solar energy exchange
Share & charge [73]	Share & charge	Open charging network (OCN) for electric vehicles
EnergyCoin [74]	EnergyCoin foundation	Cryptocurrency for secure green energy trading
WePower Blockchain platform [75]	WePower [75]	Platform connecting energy suppliers, corporate buyers and energy producers for easy, direct green energy transactions.
Grid+ [76]	GridPlus [76]	Decentralized energy trading

Blockchain can be extensively used in most of the smart grid areas [30]. Research results shows that many papers are coming up with blockchain-based proposals for energy trading, advanced metering infrastructure (AMI), the managing and charging of electric vehicles, demand response management, issue of green certificate, microgrids and information security. The authors in [28] reviewed around 140 BC projects and start ups in the energy sector and classified each work based on BC use cases in energy sector according to the field of activity, blockchain platform used and consensus mechanism used. BC use cases in energy sector were classified into eight main groups according to the activity field: (1) metering/billing and security; (2) cryptocurrencies, tokens and investment; (3) decentralized energy trading; (4) green certificates and carbon trading; (5) grid management; (6) IoT, smart devices, automation and asset management; (7) electric e-mobility; and (8) general purpose initiatives and consortia. Their systematic study results based on activity field, platform used and consensus mechanism used shows that (1) in BC use-case classification according to the activity field, 33% was for decentralized energy trading, (2) in BC use-case classification according to the platform used, 50% was built on Ethereum, and (3) in BC use case classification according to the consensus algorithm used, 55% was based on the PoW algorithm.

In the following subsections, the use cases of blockchain in smart grids, mainly energy trading, electric vehicles, demand response management, security and privacy, are discussed using several references.

3.1. Energy Trading

Blockchain plays a very significant role in energy-trading applications. BC technology is most widely used in decentralized energy-trading application compared to all others [28]. In Figure 10, we show a model of energy trading using BC technology. The main reasons for BC adoption in energy trading are transformation from centralized to distributed resources, the need for a secure P2P trading platform among prosumers avoiding third parties, building trust and privacy in the trading platform and managing the needs of all grid users. Some of the existing BC-based energy trading works are summarized in Table 5.

Table 5. Summary of existing works related to energy trading using blockchain.

Ref	Major Contribution	Technologies Used
[77]	Decentralized energy trading framework using multi-signatures, blockchain and encryption techniques that provide security and privacy to negotiate energy prices (PriWatt system)	PoW, anonymous messaging streams, smart contracts, elliptic curve digital signature algorithm (ECDSA)
[44]	Enables the energy producers and consumers to directly negotiate the energy price by developing a routing method on top of blockchain for distributed trading by introducing meta-transactions and private authentication method to verify smart meters.	Public blockchain, Distributed time-based consensus (DTC)
[78]	Proof of concept (PoC) implementation of SPB [44] on Ethereum private network for energy trading	Ethereum testnet, Raspberry Pi to mimic smart meter and solar panel operation
[79]	Establish an energy BC for secure energy trading using consortium BC, credit based payment scheme and optimal pricing strategy	Energy coins, PoW, game theory
[80]	A BC model for secure data storage and access with miner node selection algorithm and transaction handling scheme	PoW, energy coins
[81]	Implements a privacy preserving BC enabled trading model (PBT) for energy trading with consortium BC, account mapping techniques and tokens	Hyperledger Fabric 1.0, PBFT
[82]	BC based P2P energy trading framework using Cipher text policy-based encryption (CP-ABE) scheme, Redactable BC and access control mechanism	Artificial neural networks (ANN) encryption techniques, Redactable BC with chameleon hash, smart contract
[83]	Explains an energy trading framework using smart contracts which avoids intermediaries	Smart contracts, PoW

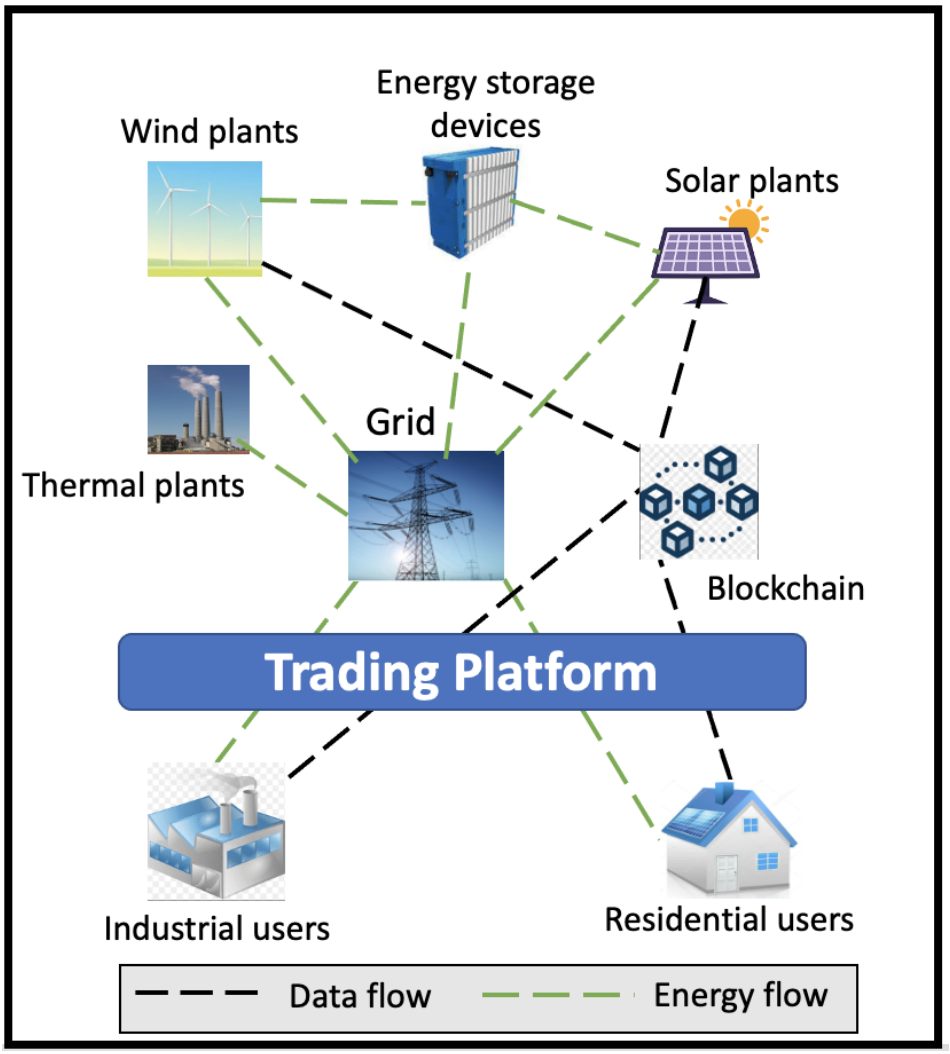

Figure 10. Model of energy trading using blockchain.

In [77], a PriWatt system, a token-based energy trading system which uses a multi-signature technique, BC technology and anonymous messaging streams that provide security and privacy in decentralized energy trading, is introduced. They use the PoW consensus algorithm and elliptic curve digital signature algorithm (ECDSA) to validate

transaction authenticity as in bitcoin. The main advantages of the PriWatt system are that it avoids single point failure, privacy and anonymity are preserved, and the use of authentication techniques. However lack of routing and message redundancy may lead to scalability issues. Ref. [44] proposes a secure private blockchain (SPB) based solution for energy trading by building a routing method on top of BC using atomic-meta transactions and private authentication methods to verify smart meters. A lightweight consensus algorithm called distributed time-based consensus (DTC) is proposed to overcome the BC processing overhead, where each miner has to wait for a random time prior to mining a block rather than solving a complex cryptographic puzzle. A proof-of-concept (PoC) implementation of SPB [44] on the Ethereum private blockchain to explain their applicability in energy trading is performed in ref. [78]. They evaluate the performance of SPB by comparing with a baseline over 100 runs of the experiments using different metrics, mainly end-to-end delay, cost, throughput and size of BC. Results indicate that SPB gives better performance than the baseline compared with end-to end delay, monetary cost and transactions per minute. Ref. [79] explains a secure energy trading platform using consortium BC and a credit-based payment scheme with optimal pricing strategy based on game theory for attaining faster transactions. The security analysis shows that the proposed energy blockchain achieves secure energy trading, and the numerical results illustrate that the energy blockchain and the credit-based payment scheme are effective and efficient for energy trading. In Figure 11 we depict the credit-based payment scheme [79] via a sequence diagram.

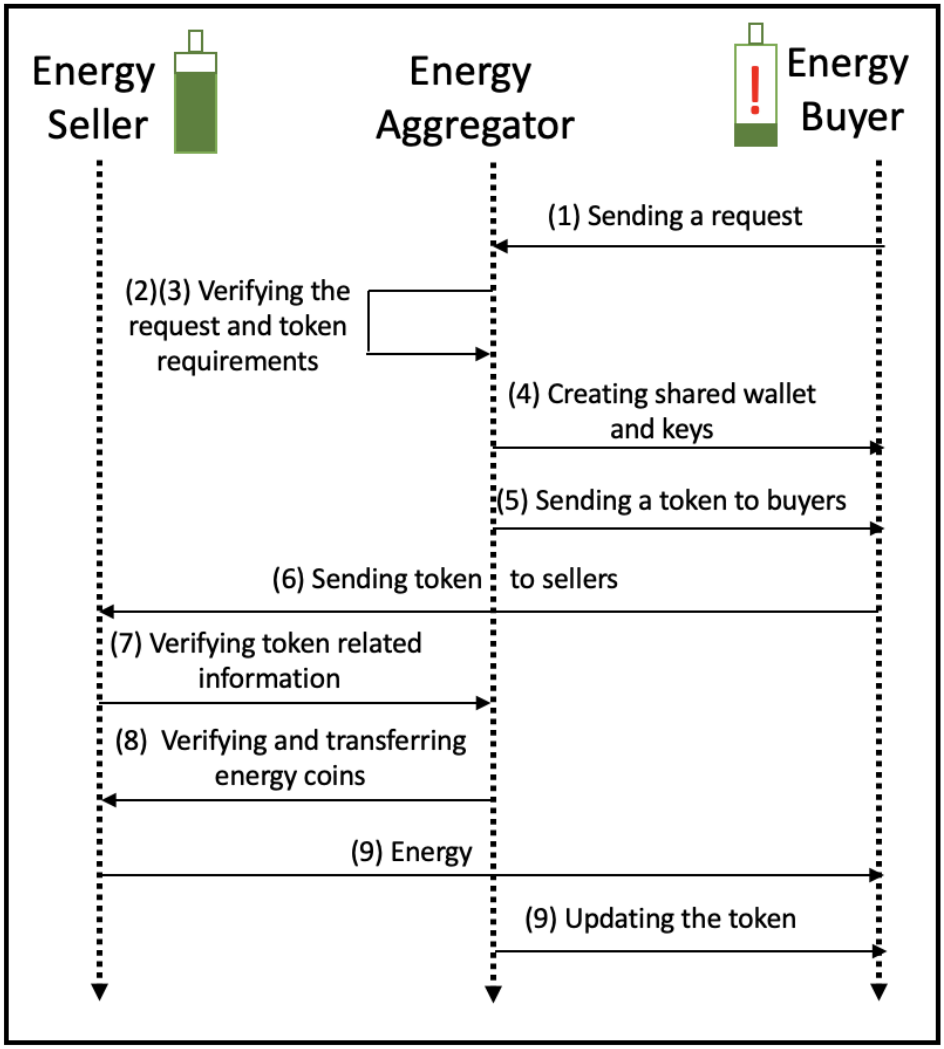

Figure 11. Main steps of credit-based payment scheme.

In [80], EnergyChain, a BC-based model for secure data storage, access and energy trading in SG environment, is introduced. It includes two types of nodes, miner nodes and normal nodes. EnergyChain uses the PoW consensus algorithm, where the miner node solves the mathematical problem of nonce calculation and the winner reaps the rewards. They explain the security evaluation results with respect to the communication cost and computation time. Paper [81] proposes a privacy preserving BC-enabled energy trading (PBT) model using consortium BC in the SG ecosystem. We depict the main steps proposed in the PBT model in Figure 12. Their main operating principle is to create noises to prevent adversarial activities in the network. It uses account mapping techniques to avoid data mining and linkage attacks. A comparison with other differential mechanisms shows that PBT can effectively handle assumed attacks. Ref. [82] explains a BC-based P2P energy trading framework using the Cipher text policy attribute-based encryption (CP-ABE) scheme for establishing P2P energy trading. It also introduces a redactable blockchain with chameleon hash, which allows users (data owners) to modify their personal information uploaded in blockchain. A simulation was conducted by constructing a private Ethereum chain and tested using PoW and PoA consensus algorithms. However, based on the results, they concluded that a more suitable consensus algorithm to ensure low latency has to be selected.

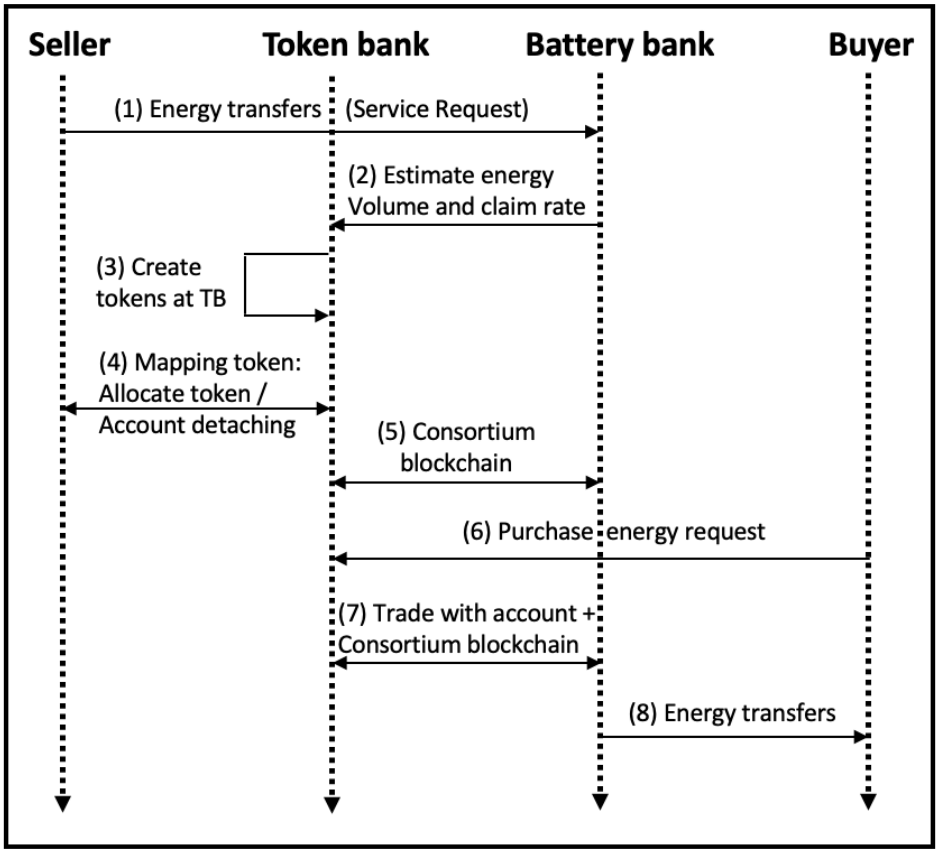

Figure 12. Main steps of trading in PBT.

More works on BC-based energy trading are present. Table 5 shows that the commonly used consensus algorithm is PoW, despite its computational power requirement. The PriWatt system in [77] addresses the issues of transaction security as well as user privacy in trading environment; however, no detailed discussion about the miners in PoW and rewards given to them is given. To overcome the inefficiency of PoW, a distributed time-based consensus is proposed in [44], and a PoC implementation and the results of the same logic are explained in [78]. The credit-based payment scheme introduced in [79] improves the delay in transaction confirmation occurring in bitcoin PoW, which allows nodes to obtain energy coin loans from credit banks to achieve faster payments. Still, they fail to provide a

formal proof for the double-spending attacks and implementation details. Similarly, ref. [80] explains an EnergyChain with a miner node selection algorithm and transaction handling scheme, but proper implementation details are not well-discussed; instead, they claim their superiority by comparison results. The noise-based differential privacy scheme proposed in [81] protects user privacy by hiding data patterns to avoid data mining and linkage attacks. They use the consortium BC and PBFT algorithm and implementation is performed using hyperledger. Due to the decreased scalability and communication overhead of PBFT, it may not be suitable for large-scale applications. The redactable BC-based scheme in [82] allows users to modify their sensitive information if needed, while the normal BC is immutable. However, this modification is secured by signature algorithms, and it may result in some malpractices as well. In some of these works [77,82,83], smart contracts were used in trading applications. The review shows that the main problems to overcome are the scalability and latency issues. Privacy is also a concern for users participating in trading. Who can be miners in the network which is decided by consensus algorithms and the type of BC to use should be the main consideration in energy-trading applications.

3.2. Electric Vehicles

EVs play a significant role in the smart grid infrastructure and they also solve some of the environmental problems by facilitating green travel. However, EV users are facing challenge in charging, as the number of EVs are increasing while the number of available charging stations are decreased. Additionally, short communication ranges, the need for frequent communications and mobility of EVs add new security and privacy concerns [84]. On the other hand, the high penetration of EVs and less-coordinated charging schedules might lead to overloading in the grid. Hence, there in an open challenge to integrate all these EVs in the grid, schedule the charging operations effectively and develop a transparent and secure charging system. Many researchers adopt decentralized BC technology to solve these issues and enhance the use of EVs and its charging management [62,85–91]. These works are summarized in Table 6.

Table 6. Summary of existing works related to electric vehicles using blockchain.

Ref	Major Contribution	Technologies Used
[62]	Explains decentralized, bidirectional, P2P electricity trading between Plug-in Hybrid Electric Vehicles (PHEVs) for buying and selling energy thereby balancing the grids (PETCON)	Consortium BC, PoW, smart contracts, double auction mechanism
[85]	Investigate authentication mechanisms for EVs and build a decentralized security model to protect transactions between EVs and charging stations	Smart contracts, Elliptic curve cryptography (ECC), Burrows–Abadi–Needham (BAN) logic
[86]	Proposes an EV charging scheme in a BC-enabled SG system which minimizes power fluctuation level in grids and charging cost for EV users (AdBev scheme)	Ethereum, smart contracts
[87]	Introduces a reliable, automated and privacy preserved charging station selection for EVs based on pricing and distance to EV.	Smart contracts
[88]	Explains a contract-based EV charging scheme in a smart community.	Permissioned BC, smart contracts, reputation based delegated Byzantine fault tolerance (DBFT) consensus
[89]	Reviews the lightning network proposed in [85] and explains a modified secure charging scheme for EVs	Hyperledger, Burrows–Abadi– Needham (BAN)logic, security verification using the AVISPA tool
[90]	Proposes a local V2V energy trading architecture using consortium BC to balance the EV charging and discharging operations.	Consortium BC, DPOSP consensus (combining PBFT and DPOS)
[91]	Focuses on preserving EV privacy and builds a BC-based differential privacy approach that prevents linkage and data mining attacks	Ethereum, smart contracts, MATLAB

Ref. [62] exploits consortium BC to develop a secure P2P energy trading system for EVs (PETCON). Electricity pricing and the amount of electricity traded are calculated using an iterative double auction mechanism for maximizing social welfare in electricity trading. Consortium BC ensures that only authorized nodes (LAGs) perform consensus process. The double auction mechanism allows users to negotiate the energy, bidding and transactions between EVs. Security analysis and numerical results show the defense ability of PETCON against many security attacks. Ref. [85] explains a decentralized security model called lightning network and smart contracts (LNSC) to improve the security of transactions between

EVs and charging stations. The model involves four phases, namely registration, scheduling, authentication, charging. The experimental results show that the model is capable of achieving increased security in energy trading between EVs and charging stations, and it can also incorporate scheduling mechanisms. However, the explained security goals are not much relevant when a BC-based system is considered. The authors in [86] proposed an adaptive EV charging scheme in a decentralized BC-enabled smart grid system (AdBev) which minimizes power fluctuation level in grids and entire charging cost for EV users. To improve EV charging/discharging, an iceberg order execution algorithm is used. The Ethereum platform is used to deploy the AdBEV scheme and compare it with the benchmark GA algorithm. The simulation results show that the proposed system has less power fluctuation level (PFL) compared to the benchmark system. The computational cost is compared using gas values associated with running a contract in EVM, which is observed to be lesser for the AdBEV scheme compared to the benchmark algorithm as the number of nodes increases. However, the paper does not explain how user identity is verified. Ref. [87] introduces an autonomous, transparent and privacy-preserved method that helps EVs to find the cheapest and nearest charging stations depending on the energy price and distance to the charging station. It can be seen that privacy is preserved, as none of the other participants can know the location of EV, none of the participants except the EV and selected charging stations know the purchased energy price, and involved EVs cannot be tracked. However, no detailed discussion about scalability (possibility of incorporating large number of EVs) and how BC handles payments is given. Ref. [88] focuses on building a smart contract based permissioned BC to develop a secure charging framework for EVs integrating RES and smart grid in a smart community. A reputation-based delegated Byzantine fault tolerance (DBFT) consensus algorithm is introduced to achieve efficient and fast consensus in the permissioned system that allows only authorized EVs to participate in the verification process. However, no discussion about who performs transaction validation and who provides incentives for validators is given. Ref. [89] proposes a secure charging system for electric vehicles based on BC and Hyperledger. They critically review the existing lightning network and smart contract (LNSC) method [85] and demonstrate their security weakness and inefficiencies. The authors aim to propose an EV charging scheme which solves these security weaknesses and flaws. The performance of the proposed scheme was compared with different related works based on computation cost and communication cost. However, the explained security goals are not much relevant for a BC-based system. In [90], a local V2V trading model based on consortium BC and fog computing is proposed, and the paper addresses the balancing problem due to charging/discharging interests of PHEVs. The paper improves the PBFT consensus algorithm by combining it with the DPoS algorithm to design an efficient consensus mechanism called DPOSP. The aim of such a consensus mechanism is to reduce the latency involved in verification and achieve faster transactions. Authors compare the proposed consensus algorithm with other mechanisms based on energy saving, fault tolerance, error node processing and block cycle. In future, they plan to design smart contract for processing transactions automatically. Ref. [91] mainly focuses on preserving EV privacy by proposing a blockchain based differential privacy approach. Differential privacy on top of consensus energy management is used to secure the broadcast information. However, there is no clear discussion about how the authentication of EVs is performed and how verification is carried out. As future work, their idea is to explore neighboring energy trading where dynamic pricing is an issue for charging EVs and more security aspects to prevent privacy breach.

The rapid rise of EV remains as a threat to the grid, because the current grid structure is not capable of managing all the energy needs, which causes a grid imbalance. The proper scheduling of EV charging, accurate predictions based on charging data, etc., are critical. Above all, security is also a major concern. Even though there are many related works to solve these issues, optimally managing EV charging by maintaining the overall grid balance is still a problem being faced.

3.3. Demand Response Management

Several research works explore different techniques to develop an innovative DRM system with the adoption of BC technology. The main idea of most of the works was to develop a secure trading platform for distributed prosumers and EVs. Smart contracts which can execute upon reaching desired conditions gained great acceptance in the DR application [92–99]. Some of the works which aims to develop better DR prototypes are listed in Table 7.

Table 7. Summary of existing works related to demand response management using blockchain.

Ref	Major Contribution	Technologies Used
[86]	Proposes an EV charging scheme in a BC-enabled SG system which minimizes power fluctuation level in grids and charging cost for EV users (AdBev scheme)	Ethereum, smart contracts
[92]	Investigate use of BC mechanism in demand management by setting up decentralized P2P energy flexible marketplace	Smart contracts
[93]	Design a BC based secure energy trading framework (SETS), having security and privacy preservation to manage demand response management (DRM)	Ethereum, smart contracts, Etcoins
[94]	Explains an algorithm for secure DRM in SGs using BC that helps to take efficient energy trading decisions for managing overall grid load	Energy coins, PoW
[95]	Proposes a secure model for energy trading using BC, contract based incentive mechanism for load balancing and route optimization algorithm to reduce EV traveling time.	Consortium BC, Proof of Work based on Reputation (PoWR), shortest route algorithm
[96]	Proposes a decentralized cooperative DR framework to manage the daily energy exchanges within a community of Smart Buildings and allows participants to decide on day-ahead community power profile, subsequently ensures the forecast tracking during the next day.	Ethereum, smart contracts
[97]	Proposes an energy scheduling scheme among multiple microgrids, EV energy scheduling integrated with microgrid operation and introduces a contribution index to prosumers and whole microgrids for prioritizing in auction.	Smart contracts
[98]	Introduces a BC-based transactive energy(TE) auction model with incorporated DR techniques for increasing social welfare.	Smart contracts
[99]	Addresses the sustainable microgrid design problem by leveraging BC technology to provide the real time-based demand response programs.	Smart contracts
[100]	Proposes an optimal power flow based DRM system without any central authority	Smart contracts

Ref. [92] reviews the use of BC in DRM programs. They use BC for storing transactions in a tamper-proof manner and smart contracts to define expected energy levels and rules for balancing grid. The model is validated and tested using a prototype developed in the Ethereum BC platform based on U.K. buildings' power consumption and production datasets. Their results shows that it is possible to adapt electricity demand in real time based on initiated DR events. However, a description on how anonymity in energy profiles is preserved is not present. Ref. [93] compares the traditional energy trading system (TETS) which relies on centralized system with a secure energy trading system (SETS) which uses blockchain technology. In SETS, all local prosumers are connected in a local/microgrid for becoming a node, and payments are made using Etcoins, which are purchased from the BC controller. Performance is evaluated using computational cost and computational time paradigms. However, the paper does not explain the consensus mechanisms used, how prosumer/consumer verification is done, and more security issues of the system. Ref. [94] explains an algorithm for energy trading and demand response management in SGs using BC technology with an algorithm for miner node selection. Security aspects for the system are also evaluated. However, their results depict higher throughput and lower consumption time for one of the selected datasets. The authors claim that it is because the concerned dataset is structured as compared to the other. Thus, in their future, the main aim is to test the proposed scheme using bigger datasets. Inspired from the works in [94,101], the authors in [95] propose a secure energy trading model using BC, a contract-based incentive mechanism for load balancing, and route optimization algorithm to reduce the EV traveling time. They use a PoW based on reputation (PoWR) consensus for energy trading to meet the time complexity of the BC-based system. Ref. [96] presents a decentralized cooperative DR framework to manage daily energy exchanges in a smart community which adopts RES. It provides flexibility to users to decide on their day-ahead power profile and

ensures the efficient tracking of the next day requirements. The simulation results show that under a special tariff structure, the peak demand can be reduced. Scalability analysis shows that it is applicable up to a group of 100 smart buildings. However, details about prediction accuracy and security aspects are not explained. Ref. [97] presents an energy scheduling mechanism among multiple microgrids (MGs) and EVs integrated with MGs. An incentive-based contribution index is introduced which gives priority to prosumers with high production points. However, they fail to explain how the verification of bids is performed. Ref. [99] addresses the problems in microgrid design using BC technology for providing a real time demand response while considering the economic, environmental and social goals. However, their prototype using smart contracts is similar to the self enforcing smart contracts idea for demand response explained in [92]. A fully decentralized and cost effective optimal power flow (OPF) based DRM solution for smart grids is proposed in [100]. The implementation of the OPF model in a private blockchain using smart contracts is explained in detail. Their execution cost results indicate that the proposed scheme provides a much cheaper execution for a complex problem. Ref. [98] proposes a BC-based transactive energy (TE) P2P trading platform and distributed auction mechanisms will make all the peers capable of becoming an auctioneer. The main concentration of the system is on social welfare, where all implementations (TE auction model and DR) aim to improve the overall living standard.

Most of the works try to apply demand response by implementing secure P2P trading between prosumers, EVs and using self-executing smart contracts. However, developing a completely decentralized grid structure with DRM programs is still a topic of research. Developing accurate day-to-day prediction for energy generation based on energy consumption data and managing the overall balance securely with proper scheduling techniques is challenging.

3.4. Security and Privacy

Smart meters placed at each home in a smart grid provide real-time information about electricity consumption and pricing. This information may contain aspects about users which are private and thus require mechanisms to preserve privacy. If a malicious attacker gains access to this data, they can track the energy usage behavior of users based on their consumption profile. The major concern for every user or entity in the SG environment is privacy, and the associated security of such information exchange [65]. Most of the works discussed in previous sections (Sections 3.1–3.3) aim to provide security and privacy in smart grid operations using BC technology. Similarly, security of power information system is also an important area of research. SG incorporates several communications for proper functioning and power delivery, and this information has to be stored securely. If the system is hacked, it may impact the grid and create unpredictable effects in the grid, leading grid operators toward making wrong energy decisions, eventually resulting in interruptions or even large-scale blackouts. Providing security for all parts of the SG is critical. The use of BC alone does not directly guarantee security and privacy; however, adding advanced cryptographic mechanisms such as multi-signatures, elliptic curve cryptography, etc., are also needed.

3.5. Research Challenges and Solutions in Integration of Blockchain and Smart Grids

So far, a complete review of SGs, BC, their overview and individual challenges was given. Additionally, the advantages and applications by combining BC technology with SG were discussed in detail. However, as an emerging concept, BC-based solutions for future SG are facing challenges in their complete incorporation. Some of the challenges are related to SGs (Section 2.1.2) and some are BC-specific (Section 2.2.5). In this section, the challenges faced while moving toward a decentralized SG using BC and possible solutions will be discussed.

1. Inefficiencies of consensus mechanisms: Consensus mechanisms are an integral part of a BC system, as they help to decide who can verify and add blocks. These mechanism

determine most of the performance characteristics of the involved BC system, such as scalability, fault tolerance, throughput and overall security. PoW is the widely accepted consensus mechanism which is adopted in bitcoin, but high computational power makes it unsuitable for energy applications. From the review of related works, it is understood that PoW and its modifications are widely used by researchers in energy sectors. In [44], a distributed time-based consensus is proposed, which modifies the PoW computational puzzle solving to a random waiting time for reducing the processing overhead. In [95], a reputation-based PoW is introduced that assigns a positive reputation to honest nodes and negative reputation to malicious nodes. The PBFT mechanism is also used in some works ([81,89]); however, less scalability and communication overhead make it unsuitable for large-scale applications. A modified PBFT version, DBFT, which is a reputation-based delegated Byzantine fault tolerance, was introduced in [88] for attaining faster consensus in permissioned BCs. PBFT and DPoS was combined in [90] to develop the DPOSP consensus mechanism that aims to reduce transaction latency. PoA, which allows only authorized entities to participate in network consensus is used by energy web foundation [51] that achieves confirmation time in 3–4 s. As the consensus mechanism is important while developing a BC-based application, many researchers are working on modifying existing algorithms or implementing new ideas of consensus for achieving high scalability and high transaction speed with minimal energy consumption. Developing such mechanisms will be challenging, and this has great research interest.

2. Smart contracts designing: As discussed, smart contracts are pieces of code that execute by themselves when certain conditions are met. However, these may be vulnerable to malicious attacks since they are built on programming codes. The designing of a smart contract for a critical application should be done with the utmost care. Small bugs or programming errors open it to several malicious activities [102]. For example, in 2016, around 3.6M ether was stolen from a decentralized autonomous organization (DAO) by taking advantage of the inefficiencies in the smart contract. Here, an attacker uses an empty malicious contract that contains a fallback function, and with successive recursive calls, they can empty the complete balance in the DAOs account. This occurs mainly due to the programming methods used by DAO, and making modifications in call functions may help to avoid such errors. Hence, it is clear that the designing of smart contracts plays an important role if it is used for the decentralized applications.
3. Chances of centralization: In an energy application, the number of users is very high. If a public BC structure is used, many users will be involved in the consensus process at the same time. As the number of node increases, the efficiency of the system decreases, which in turn increases the response time. However, by using a permissioned BC structure, the number of nodes and participants can be limited to authorized users. From the review of related works, it is understood that in most of the BC-enabled SG cases, a private or consortium BC is used rather than public BC. However, this results in a semi-centralized structure, as there are certain authorized nodes that decide about the network, thus moving toward a complete decentralized highly scalable system.
4. Deployment and operational costs: Implementation of BC based system requires high infrastructural costs since it requires re-architecting the current grid network, upgrading smart meters, developing the ICT infrastructure and other related advanced metering interfaces [30].
5. Legal and regulatory support: As of now, there are a large number of technical solutions developed for the BC-based SG system. However, wide acceptance from the legal and regulatory bodies is missing and are lacking supporting standards. These regulatory bodies do support user participation in energy markets and community energy structures, but energy trading between prosumers and consumers using distributed ledgers is not widely supported [30]. The integration of smart meters, EVs, and other IoT devices is possible; however, interoperability between them is lacking [18]. Before

moving toward a complete decentralized grid structure without a trusted central authority, new standardization rules are essential to avoid disputes.

4. Review of Machine Learning in Smart Grids

Smart grids are becoming large-scale and complex with the integration of RES, EVs, smart meters and other smart devices. The advancement in smart grids is fast, and it is challenging to model such complex smart grids [31]. Additionally, unlike conventional systems, smart grids allow two-way information and power flow. Hence, conventional mathematical models are not suitable for smart grids. ML, which can be implemented when system models and parameters are inadequately supplied, gains importance at this point, as it can improve performance and system intelligence through experience.

ML techniques are being widely used in smart grids for enhancing power system performance, accurate load forecasting, efficient energy supply management, demand response, fault detection and data protection [7,8,19–22,103,104]. Table 8 summarizes these works.

Table 8. Summary of existing works related to machine learning and smart grids.

Ref	Major Contribution	Technologies Used
[20]	Proposes two machine learning based techniques for detecting false data injection.	Support vector machine Principle component analysis
[19]	Introduce a framework for modeling time-varying operations in energy system using clustering techniques	Clustering algorithms like k-means, k-medoids, DBA, hierarchical etc.
[103]	Proposes an intelligent attack detection and identification model in cyber–physical grid that can classify attacks based on attack types	Autoencoder, Decision tree, neural network and random forest
[22]	Study on application of big data and machine learning in smart grids	-
[104]	Proposes an electrical theft detection algorithm using big data analytics technique	Adaptive synthesis(ADASYN), Convolutional neural network, Deep siamese network, LSTM
[7]	Outlines the design, development and testing of an energy management system with demand response capabilities.	Prediction algorithms
[21]	Compares the use of two ANN based load forecasting techniques: Feed forward neural networks and Echo state networks.	Feed forward networks Echo state networks K-means clustering
[8]	Reviews the applications of machine learning in building load prediction algorithms	-

In the following subsections, some of the important use cases for the integration of smart grids and machine learning, mainly attack detection and security, data analysis and demand response management, are discussed in the context of existing research.

4.1. Attack Detection and Security

Ref. [20] addresses the problem of false data injection in smart grid and ML-based techniques to detect such attacks. Information exchanges in SG are mainly unidirectional, for example, information to control centers based on measurements. These data should be clearly monitored for studying malicious behaviors in the SG. Their work mainly uses two ML techniques to detect attacks in SG (supervised and unsupervised techniques) and classify normal data and tampered data. Ref. [19] uses clustering methods to find representative periods for optimizing energy systems. Ref. [103] explains an attack identification and detection model for cyber–physical grids based on an ensemble of ML models named ensemble representation learning classifier (ERLC) for maximizing the performance of attack detection. They combine multiple classifiers (decision tree and random forest), neural networks (feed forward ANN) and an attack localization algorithm (based on chi-square metric). Their results indicate the efficacy of the proposed ERLC algorithm for attack detection and classification. In the future, their idea is to test the algorithm in multiple systems with varying topology and also incorporate real-time data using recurrent neural networks (RNNs), such as the long short-term memory (LSTM) neural network.

4.2. Data Analysis

In [22], a comprehensive study on the application of big data and ML and the associated security concerns in the electricity grid is presented. The massive data generated from

the grid, termed 'Big Data', require proper optimization from generation to distribution side and have to be processed/analyzed by implementing effective security solutions. Two major concerns regarding any data generated in SGs are processing the gathered data by satisfying the time limits and overcoming the involved security concerns [22]. ML techniques can be applied to predict the usage patterns and preferences of users in SG. Solar power plants and other RESs are affected greatly by seasonal changes. Thus, a system that can predict, in advance, solar energy information is required to minimize the operational costs caused. Cyber security challenges in SG and solutions using ML are also reviewed in [22]. Cyber attacks in SG cause power supply interruption, operational failures, financial damages, data theft and complete blackouts. False data injection attack (FDIA), where attackers aim to modify original data, will cause negative effects in the grid. Thus, the security of data is crucial in SG, and many works have already been conducted on the detection of threats and protection mechanisms to solve them using ML. Based on their study, they discuss the scope of future work in this field: validating the current grid structure using mathematical modeling for moving toward SG architecture; meet the challenges in the transition toward a renewable energy-centric distributed grid; better forecasting techniques for demand and generation, mainly for RES in SG; and more solutions for security and cyber attacks related issues. This paper provides a good insight into the security concerns of SG- and ML-based solutions.

In [104], a big data analytics technique is proposed to solve the electricity theft detection problem. They use an adaptive synthesis (ADASYN) to handle the imbalance class problem of data and convolutional neural network (CNN) and LSTM integrated deep Siamese network (DSN) to discriminate features of honest and fraudulent consumers. Data analytics is performed on different train–test ratios of real-time smart meter data. Their simulation results shows that proposed model is effective when compared with other benchmark models (SVM, random, logistic regression, and CNN–LSTM) in terms of area under curve, F_1-score, accuracy and recall.

4.3. Demand Response Management

Ref. [7] studies demand response algorithm implementation for SG residential buildings using ML models. They combine the optimization technique and ML models to find the optimal strategy for DRM and use metered data to train and test the algorithm. Two demand response algorithms—rule-based and predictive-based (ML-based)—were deployed and evaluated using a common demand price scheme. Ref. [21] compares two ANN-based load forecasting techniques: echo state network (ESN) and feed forward neural networks (FFNN) for demand response programs in SGs. The novelty of their method is that they compare two ANN techniques over a complete and heterogeneous data set which are pre-processed with adaptive clustering techniques for achieving optimized forecasting performance. Their work can help power system planners for forecasting user-based profiles and implement DR programs. Ref. [8] reviews ML techniques in building load prediction. They review most of the existing ML-based load prediction methods and identify the gaps for future trends and development. Some of the future works are building load prediction for DR and building grid interactions (inter-dependency of loads), uncertainty quantification of faults on building energy, integration of smart sensors with ML algorithm for building load prediction and active learning in building load prediction.

Although there are many techniques and models using ML techniques, there are many more to be explored. Unusual weather conditions will increase the complexity of daily load relationships, which makes prediction difficult. Mapping the correlation between variables is required in such cases [31]. Additionally, the vast amount of data generated by widely deployed metering devices call for more sophisticated data analysis and intelligent decision-making techniques in SGs. For cyberattacks and fault data detection, ML techniques can be used. However, ML techniques are highly dependent on the available data and processing techniques used.

5. Integration of Blockchain and Machine Learning for Smart Grids

Combining BC and ML for various applications is increasing. The learning capabilities of machine learning can be applied with blockchain to make the chain smarter [105]. Additionally, the computational power for ML models can minimize the time taken for the nonce calculation. On the other hand, using the decentralized data architecture of blockchain, better ML models can be built. The main benefits of combining BC and ML are (a) security, (b) improving energy consumption, (c) improving the smart contracts, (d) data trading and more. BC is a continuously growing data ledger, whereas ML requires large volumes of data. Both techniques complement each other and have high potential when combined for different applications.

With the decentralized and immutable structure, BC builds a trust environment without third parties for any transactions occurring. ML-based solutions mainly help in demand management using prediction techniques and help in handling large amount of data from smart meters [33]. Additionally, optimization techniques can be used for scheduling the energy usage of users. Applying BC into ML systems helps such systems to use information collected by BCs to clear problems quickly, and applying ML techniques to BC adds powerful intelligence to BC systems for data processing and other intensive applications [24]. The storing of large-scale data in a secure and tamper-proof manner by BC-based systems ensures the confidentiality and auditability of the collaborative data training process and trained model using cryptographic techniques. Additionally, it enables decentralization that ensure access control with central authorities. Smart contracts and Dapps allow to model interactions between entities in the decentralized ML application. In the same way, adding ML helps the BC system to achieve energy efficiency, scalability, security and intelligent smart contracts. As ML can predict and speedily calculate data, it provides a feasible way for miners in selecting important transactions. Using predictive analysis can ensure energy and resource requirements to be met and improve overall efficiency. Hence, considering the future SG scenario, both BC and ML can together solve the issues regarding energy trading, EV charging and scheduling, load prediction, DRM, security and privacy concerns. Table 9 summarizes the existing works that combine BC, ML and SGs.

Table 9. Summary of existing works related to BC, ML and SGs.

Ref	Major Contribution	Technical Resources
[25]	Evaluate the development of a decentralized EV charging infrastructure using BC, AI and SGs	-
[106]	Proposes a decentralized electricity trading framework (DETF) for connected EVs.	Hyperledger, smart contracts, predictive bidding
[107]	Proposes DeepCoin, a BC and DL based framework to protect SGs from cyber attacks.	Recurrent neural networks, Hyperledger, PBFT
[108]	Explains P2P trading system for sustainable power supply in SGs using BC and ML	Hyperledger, smart contract, PBFT, Predictive model using LSTM
[109]	Explains an intelligent EV charging system for new energy companies using consortium BC	Smart contracts, Limited Neighborhood Search with Memory (LNSM) algorithm
[110]	Proposes an energy trading approach using machine learning and blockchain technology	Smart contracts K-nearest neighbor

In [25], the authors evaluate the integration of BC, artificial intelligence (AI) and SGs for developing a decentralized EV-charging infrastructure. In their view, the main challenges faced by an EV are vulnerable charging stations and non-optimal charging schedules. In the context of EV charging, AI adds solutions to implement optimal charging schemes based on the drivers' charging behavior, and BC can solve security and privacy issues in the charging infrastructure. Their main idea is to combine both and attain the best of both technologies to develop a decentralized EV-charging infrastructure. They also discuss several future research directions of this integration.

Ref. [106] explains an advanced decentralized electricity trading framework (DETF) for connected EVs (CEVs) and parking lots using consortium BC, game theory and ML. They implement a smart contract based auction model and HLcoin (Happy Light coin)

using hyperledger for trading electricity. A smart contract is made between all stakeholders and deployed in BC. CEV sellers will submit the amount of energy to be sold out, and other CEV bidders will submit their bids. The smart contract runs an auction model to determine the winner and amount. The selected bidder is awarded electricity and the seller receives the corresponding HLcoin. Their algorithm HLProfitX was compared with PETCON [62], and the results show that their method outperforms it. In the future, they aim to extend the work by adding RES and a microgrid architecture.

Ref. [107] proposes DeepCoin, a deep learning (DL) and BC-based framework for protecting SGs from cyber attacks. The proposed framework is composed of a BC-based system and a DL-based system. It consists of four entities: energy buyer, energy vendor, BC and intrusion-detection system (IDS). The BC-based system provides a secure environment for the energy system and the DL-based scheme detects network attacks and fraud transactions. The DeepCoin framework uses the PBFT consensus algorithm in the BC system and recurrent neural networks (RNN) in the DL system. The performance was evaluated using three different datasets, and the efficiency of the framework was discussed. For the future study, their aim is to add edge computing to the DeepCoin framework and study the performance in SG.

Ref. [108] explains a P2P trading mechanism based on BC and ML for sustainable power supply in SGs. It contains two modules: a BC-based energy trading module with real-time energy consumption monitoring, energy trading, reward model, and a smart contract enabled predictive analysis module for building a prediction model using energy consumption data. Predictive analysis is implemented using deep learning approaches based on recurrent neural networks and Hyperledger fabric is used for building the P2P trading platform with the PBFT consensus algorithm. Their results show that the proposed method is better in terms of latency and throughput. However, discovering hidden patterns from data using predictive model is difficult. In the future, they plan to consider more features for the optimization algorithm.

In [110], an efficient energy trading approach using machine learning and blockchain is explained. The K-nearest neighbor (KNN) ML algorithm is used to calculate the distance between the EV and charging station. Energy brokers/aggregators find the nearest charging station for EV when an energy request is received and calculate the amount of time required for EV charging. All the communications between EVs and charging station are secured using the blockchain-based proposed authentication process. Smart contract maintains the secure energy trading, and the transaction cost is calculated from the used gas price. In the future, their aim is to compare the proposed method with other charging schemes and implement real time models.

These works show that combining BC and ML techniques provides benefits in the development of SGs. The main concern is whether these solutions help in building a fully fledged SG infrastructure that satisfies the need for secure P2P trading, managing balance in the grid by proper scheduled energy usage and EV charging. From the previous sections, the applications offered by BC and ML individually become clear, although with certain limitations. These combined can offer benefits to each other and to the overall system. For example, BC technology can benefit ML techniques for data and model sharing, security and privacy, decentralized intelligence and trustful decision making [24]. Similarly, ML techniques can also benefit BC technology, i.e., it can optimize energy and resource efficiency, optimize scalability, improve security and privacy and develop intelligent smart contracts [26]. As research on integrating BC and ML is in progress, there are some open issues and challenges to be addressed.

6. Open Research Challenges

In this section, we identify and highlight key open research challenges in related research for BC, ML and SG.

1. How can we manage the energy consumption of consensus algorithms in energy applications?

The review shows that many consensus algorithms are present and most of the works use different algorithms based on different needs. Mainly PoW, PBFT, PoA and its variants are used by researchers in energy applications. Table 3 compares these algorithms. However, building an efficient consensus algorithm is still an open research and requires some trade-offs. Bitcoin and Ethereum use the PoW consensus mechanism. The study conducted by Cambridge's Center for Alternative Finance estimates that the electricity consumption of Bitcoin is around 145 TWh, which would rank it among the top energy consumers if it were a country [111]. Hence, for energy applications, BC-based solutions that uses the PoW consensus are not well-suited and have to be avoided. Additionally, the scalability and performance of developed systems are closely related to the consensus algorithms used [112]. The authors in [32] identify the need for building scalable blockchains that handle transactions at a faster rate. The energy web chain uses the PoA consensus mechanism, which is based on a permissioned BC, where the group of trusted nodes validates transactions and creates blocks [51].
Many researchers have used ML techniques for implementing efficient consensus algorithms. The proof of learning, introduced in [113] is a BC-based consensus mechanism using ML techniques. They implement WekaCoin, a P2P cryptocurrency that uses the proof of learning consensus. Here, the main actors in the network are trainers, suppliers and validators. Rather than using hash-based complex puzzles, ML tasks are used to achieve consensus, which reduces computational power and energy usage. However, the idea of who can be trainers, suppliers and validators and their selection is not clearly mentioned. Proof of deep learning (PoDL), introduced in [114], explains a similar idea to proof of learning [113]. Their idea is to recycle energy consumed while mining a block by introducing PoDL, i.e., miners train DL models, and the block generated by miners that properly trained the DL model will be accepted. This can be considered an improved PoW model, where miners have to find a best-fit DL model which makes better use of nodes' energy and computing resources. As training a DL model takes more time, the latency involved in block creation cannot be avoided, which is not considered by them. Hence, more studies have to be conducted in this part as well.
There are other works combining ML and BC for building consensus algorithms. Even though the potential of ML-based consensus algorithms is clear from these works, most of them lack solid ways of explaining and modeling appropriately [24]. In an energy application, the number of users is high, and transactions are to be processed with minimal delay and minimal energy consumption. Thus, the choice of the consensus mechanism has a significant impact. Hence, more exploration should be done to solve the existing issues of consensus mechanisms while using them with energy applications.

2. How can the big data generated in the smart grid be processed without compromising the security and scalability of systems?

The data generated from SGs, mainly smart meters, contain users' sensitive information, consumption data, etc., and these can be used for a wide range of applications, namely, cyber security, anomaly detection, day-ahead prediction and others. By reading smart meters every half an hour, 17,500 readings are generated yearly [115]. If we assume each smart meter reading is 10 kilobytes, then around 175 megabytes of data are generated by each smart meter per year. In Sweden, approximately 5.5 million electricity meters are installed [116], then around 962 terabytes of information has to be processed, analyzed and stored by utility companies every year. The main challenge here is to store, process and analyze the large amount of data while offering scalability, security and data integrity . In this context, BC integration will enable security for data and build trust for distributed processing [117]. The secure data storage in cloud-based platforms relying on BC ensures cyber security and prevents data modification. However, the large storage space and computing resources required by these large datasets add a challenge while adopting BC solutions [24]. Further analysis on the smart meter data for building prediction models can be facilitated through ML-based prediction models. However, collecting and processing the large amount of unlabeled or uncategorized

data causes significant challenges in building accurate ML models [23]. Moreover, due to the scalability issue of BC, which has been an open research topic for a long time, it cannot facilitate scalable platforms for managing big data [117]. Most of the current BC applications are not capable of handling a large number of transactions in a short time and low cost [24]. To overcome this, many techniques, mainly sharding, pruning, lightning protocols, etc., were introduced by researchers [118]. However, distributed scalability can be achieved only with the cost of information security and privacy, which is not suitable in the case of data from smart grids [57]. Methods have to be explored to overcome this BC trilemma when considering the smart grid scenario. The benefits of ML for balancing BC scalability was investigated by researchers [23]. For data processing, alternative distributed storage platforms supported by BC are also a feasible solution. Hence, as we move toward a distributed grid platform, ways to handle the generated data in the required security level and by preserving data integrity using scalable platforms require further research attention.

3. How can we overcome the security and privacy issues by combining blockchain and machine learning?
   Security and data privacy are important in every application where data are exchanged over a public network. As an evolving technology, certain security challenges are faced by SG networks and BC technology. As seen from Section 2.1.2, all systems should satisfy the main security objectives (CIA triad). These objectives should ensure that the involved communications are secure, data from smart meters are true and unaltered, and information is available for authorized users when in need. Most of the cyber attacks, mainly eavesdropping, man-in-the-middle attack, false data injection, etc., target one of the CIA triad, which causes adverse effects in the grid [40]. BC-based solutions gain importance at this stage because of their properties (data immutability and data indestructibility), which inherently build a distributed trust platform. BC solutions are applicable to most SG applications, such as energy trading, EV charging, demand management, etc. However, it is difficult for a BC-based system to achieve security, decentralization and scalability at the same time [57]. Improved security can be achieved only at the cost of distributed scalability or computational power as in the case of bitcoin. Hence, a trade-off is necessary. The objective while working with BC should be to achieve required security level while maintaining scalability and energy-consumption limits.
   Some other attacks faced by BC due to its architecture are discussed in Section 2.2.5. For instance, a hard fork in a DAO (decentralized autonomous organization) built on Ethereum, resulted in 50 million ether being stolen [53]. ML plays a vital role in building attack detection systems that add security. Many works have focused on anomaly detection, fault detection and intrusion detection especially in SG domain [20,26,107]. However, even though these models give accurate attack detection, they still face certain challenges in implementation, i.e., for a large dataset with both benign and malicious data, attack detection systems should deal with high dimensionality for pre-processing data to extract features [24]. Additionally, training ML models with a large data source in a real-time fashion is challenging. However, by developing solutions that combine BC and ML, some of the above challenges can be overcome [24]. Hence, careful study is needed in both BC and ML systems to build secure SG systems.
4. How can we maintain grid stability by scheduling energy consumption of prosumers and electric vehicle (EV) users?
   The integration of RES helps to minimize the effects of coal-fired power plants which reduce the carbon emissions from the electricity sector. The rise of EVs also helps to reduce the CO_2 emissions. The report by Siemens says that if all the vehicles run on renewable electricity, then about six gigatons of CO_2 emissions can be reduced [119]. With the integration of RES, energy users are becoming energy producers (prosumers), and therefore, more green energy is being generated and injected into the grid. However, the problem here is whether the existing grid network is sufficiently capable

of coping with the increased penetration of RES, prosumers and EVs. Additionally, when more EVs charge at the same time, it is more likely that the grid will be overloaded [119]. Moreover, the unpredictable nature of renewable sources, the energy generation/consumption of prosumers and charging pattern of EVs cause several challenges in the grid architecture [120]. A large amount of energy injected to the grid or consumed from the grid without proper management creates peaks in the demand load curve. Most commonly, high peaks are seen during the morning and evenings due to the high energy demand, which causes an imbalance in the grid network. The increased penetration of EVs adds to this, which may impact the voltage stability and operating costs of the grid. As seen in earlier sections, the security, privacy, charging schemes, demand management, etc., related to energy trading and EV charging was well researched with more focus on building secure trading and charging systems. Along with these, the energy generation/consumption of energy users and EVs, more specifically, injecting the renewable energy generated to the grid or when consuming a large amount of energy from the grid, or the charging of EVs have to be properly scheduled considering the grid capacity. Based on the usage patterns and electricity consumption/generation, a system which can schedule the real-time energy usage of EVs and users will have a great impact on balancing the grid, which is a main challenge to be overcome [8]. Hence, more focus on scheduling the energy usage without compromising security and privacy is required.

5. How can we establish the interoperability of blockchain networks?
   BC technology is making significant changes in many industries, such as healthcare, supply chain, energy, etc., in addition to cryptocurrencies. However, present networks do not have the functionality to transmit tokens or data between different blockchain networks, i.e, interoperability between blockchain networks is lacking [121]. Additionally, BC smart contracts do not have the capability to access data or write data from or to any external APIs. As BC is growing, an infrastructure for exchanging data and tokens between BC networks is required. BC interoperability allows different BC networks to communicate between them by sharing data and tokens [122]. Interoperability has the potential to solve some of the biggest BC research challenges, for example, it can improve scalability by offloading transactions to other BC networks via sharding techniques. When two applications are running on the same BC platform, data exchange between them is simple; however, when the BC networks are different, then the process is difficult.
   In the energy industry, interoperable smart contracts help to exchange data between private and public BCs, BC networks in different regions or microgrids and BC-based EV charging platforms. For instance, considering the case of EV charging, the interoperability of charging stations is less, which creates a burden for EV users when traveling long distances. Hence, a method that helps in the universal charging process is required. BC-based identity management systems can create a flexible charging system for EVs, using certification and authentication mechanisms [123]. However, most of the reviewed works do not consider the mobility aspect while developing EV-charging systems, and it has significant research scope. To achieve BC interoperability, there are several techniques proposed, such as sidechains, oracles, chainlink and so on [121]. However, it is still unclear how these networks can work together and thus requires significant research.

7. Conclusions

Smart grid (SG) is a vast interconnected system with many new emerging technologies. Several features of SG include communications, demand response, microgrid, the integration of RES, security and EVs. However, achieving the full benefits of SG still remains a challenge. Major challenges faced are the integration of RES, data management, cyber security, energy balancing and stability. There is no reasonable solution found; however, several research approaches are under investigation. Additionally, the solution to many

technical, security and socio-economical issues have to be found for the better realization of the smart grid. The advancements in blockchain (BC) and machine learning (ML) add benefits to the electricity grid for building an improved grid architecture. Hence, in this review, the potential of BC technology in SG, ML applications in SG and applications of BC and ML integration in SG is investigated. Some of the relevant research in the field of BC, ML and SGs is critically reviewed, and challenges as well as open issues are identified. As discovered, BC provides several solutions to SG in the field of energy trading, EVs and DRM by providing security and privacy. However, the scalability issues of BC, energy consumption and stability of the grid were not well addressed in most of them. For example, an EV charging system should be secure and capable of building a trustful environment for EV users with proper scheduling techniques by managing the variations in the power grid. Such a system requires both BC technology and ML techniques. To the best of our knowledge, this is the first review article that combines BC and ML techniques in the context of energy applications.

BC solutions create a trust environment by building decentralized secure networks. ML techniques provide increased insight in the operation of SG which helps in better prediction and scheduling. This is done by finding patterns from large amount of data, which is challenging. Additionally, the involved computational power and scalability of networks have to be addressed. Hence, after this review, we conclude that for integrating BC solutions and ML techniques to develop secure and stable SG architecture, there remain certain challenges to overcome. The requirements for building a secure and stable SG architecture is not yet clearly understood and careful study has to be conducted in both BC and ML fields. Specifically, areas that need further research are as follows: (1) developing a consensus mechanism that can reduce energy consumption and latency while maintaining security; (2) developing electricity prediction models from large amount of real-time or non-real-time consumption data patterns, thereby balancing the grid using self-executing smart contracts; (3) developing a universal charging and scheduling system specifically for EVs; (4) microgrids design—including prosumers in residential homes, buildings, and EVs; and (5) the interoperability of blockchain platforms.

Author Contributions: Conceptualization, V.K.M., S.S. and C.Å.; methodology, V.K.M.; formal analysis, V.K.M., S.S. and C.Å.; writing—original draft preparation, V.K.M.; writing—review and editing, V.K.M., S.S. and C.Å.; supervision, C.Å. and S.S.; funding acquisition, C.Å. All authors have read and agreed to the published version of the manuscript.

Funding: The researcher(s) would like to thank Stiftelsen Rönnbäret for funding this research (https://skelleftea.se/platsen/campus-skelleftea/startsida-campus-skelleftea/forskning--innovation/stiftelsen-ronnbaret).

Data Availability Statement: Not applicable.

Acknowledgments: We would like to thank Math Bollen, department of Electric Power Engineering, Luleå university, for his valuable feedback, comments and insights regarding power grids.

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

Abbreviations

The following abbreviations are used in this manuscript:

AMI	Advanced Metering Infrastructure
BC	Blockchain
Dapp	Decentralized Application
DL	Deep Learning
DoS	Denial of Service
DPoS	Delegated Proof of Stake
DR	Demand Response
DRM	Demand Response Management
EV	Electric Vehicle

EVM	Ethereum Virtual Machine
ICT	Information and Communication Technologies
IoT	Internet of Things
ML	Machine Learning
P2P	Peer to Peer
PBFT	Practical Byzantine Fault Tolerance
PHEV	Plug in Hybrid Electric Vehicles
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
RES	Renewable Energy Sources
SG	Smart Grid
V2G	Vehicle to Grid

References

1. US Department of Energy. The Smart Grid. 2021. Available online: https://www.smartgrid.gov/the_smart_grid/smart_grid.html (accessed on 20 July 2021).
2. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980. [CrossRef]
3. Siano, P. Demand response and smart grids: A survey. *Renew. Sustain. Energy Rev.* **2014**, *30*, 461–478. [CrossRef]
4. Falvo, M.C.; Graditi, G.; Siano, P. Electric vehicles integration in demand response programs. In Proceedings of the 2014 International Symposium on Power Electronics, Electrical Drives, Automation and Motion, Ischia, Italy, 18–20 June 2014; pp. 548–553. [CrossRef]
5. Bollen, M. *The Smart Grid: Adapting the Power System to New Challenges*; Morgan & Claypool Publishers: San Rafael, CA, USA, 2011. . 00/S00385ED1V01Y201109PEL003. [CrossRef]
6. Musleh, A.S.; Yao, G.; Muyeen, S.M. Blockchain Applications in Smart Grid-Review and Frameworks. *IEEE Access* **2019**, *7*, 86746–86757. [CrossRef]
7. Pallonetto, F.; Rosa, M.D.; Milano, F.; Finn, D.P. Demand response algorithms for smart-grid ready residential buildings using machine learning models. *Appl. Energy* **2019**, *239*, 1265–1282. [CrossRef]
8. Zhang, L.; Wen, J.; Li, Y.; Chen, J.; Ye, Y.; Fu, Y.; Livingood, W. A review of machine learning in building load prediction. *Appl. Energy* **2021**, *285*, 116452. [CrossRef]
9. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2021. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440802 (accessed on 15 July 2021).
10. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717. [CrossRef]
11. Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
12. Khalil, A.A.; Franco, J.; Parvez, I.; Uluagac, S.; Shahriar, H.; Rahman, M.A. A Literature Review on Blockchain-enabled Security and Operation of Cyber-Physical Systems. In Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), Los Alamitos, CA, USA, 27 June–1 July 2022; pp. 1774–1779. [CrossRef]
13. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef]
14. Chang, S.E.; Chen, Y. When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications. *IEEE Access* **2020**, *8*, 62478–62494. [CrossRef]
15. Sun, Y.; Zhang, L.; Feng, G.; Yang, B.; Cao, B.; Imran, M.A. Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment. *IEEE Internet Things J.* **2019**, *6*, 5791–5802. [CrossRef]
16. Xia, L.; Sun, Y.; Swash, R.; Mohjazi, L.; Zhang, L.; Imran, M.A. Smart and secure CAV networks empowered by AI-enabled blockchain: The next frontier for intelligent safe driving assessment. *IEEE Netw.* **2022**, *36*, 197–204. [CrossRef]
17. Cheng, R.; Sun, Y.; Mohjazi, L.; Liang, Y.C.; Imran, M.A. Blockchain-Assisted Intelligent Symbiotic Radio in Space-Air-Ground Integrated Networks. *arXiv* **2022**, arXiv:2211.05902.
18. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 18–43. [CrossRef]
19. Teichgraeber, H.; Brandt, A.R. Clustering methods to find representative periods for the optimization of energy systems: An initial framework and comparison. *Appl. Energy* **2019**, *239*, 1283–1293. [CrossRef]
20. Esmalifalak, M.; Liu, L.; Nguyen, N.; Zheng, R.; Han, Z. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Syst. J.* **2017**, *11*, 1644–1652. [CrossRef]
21. Mansoor, M.; Grimaccia, F.; Leva, S.; Mussetta, M. Comparison of echo state network and feed-forward neural networks in electrical load forecasting for demand response programs. *Math. Comput. Simul.* **2021**, *184*, 282–293. [CrossRef]
22. Hossain, E.; Khan, I.; Noor, F.U.; Sikander, S.S.; Sunny, M.S.H. Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. *IEEE Access* **2019**, 13960–13988. [CrossRef]

23. Tanwar, S.; Bhatia, Q.; Patel, P.; Kumari, A.; Singh, P.K.; Hong, W.C. Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward. *IEEE Access* **2020**, *8*, 474–448. [CrossRef]
24. Liu, Y.; Yu, F.R.; Li, X.; Ji, H.; Leung, V.C. Blockchain and machine learning for communications and networking systems. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1392–1431. [CrossRef]
25. Elhusseini, H.; Assi, C.; Moussa, B.; Attallah, R.; Ghrayeb, A. Blockchain, AI and Smart Grids: The Three Musketeers to a Decentralized EV Charging Infrastructure. *IEEE Internet Things Mag.* **2020**, *3*, 24–29. [CrossRef]
26. Mylrea, M. AI enabled blockchain smart contracts: Cyber resilient energy infrastructure and IoT. In Proceedings of the AAAI Spring Symposium Series, Stanford, CA, USA, 26–28 March 2018.
27. Wu, J.; Tran, N.K. Application of blockchain technology in sustainable energy systems: An overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
28. 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]
29. Hassan, N.U.; Yuen, C.; Niyato, D. Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges, and Solutions. *IEEE Ind. Electron. Mag.* **2019**, *13*, 106–118. [CrossRef]
30. Alladi, T.; Chamola, V.; Rodrigues, J.J.P.C.; Kozlov, S.A. Blockchain in Smart Grids: A Review on Different Use Cases. *Sensors* **2019**, *19*, 4862. [CrossRef]
31. Farhoumandi, M.; Zhou, Q.; Shahidehpour, M. A review of machine learning applications in IoT-integrated modern power systems. *Electr. J.* **2021**, *34*, 106879. [CrossRef]
32. Khan, H.; Masood, T. Impact of Blockchain Technology on Smart Grids. *Energies* **2022**, *15*, 7189. . [CrossRef]
33. Kumar, N.M.; Chand, A.A.; Malvoni, M.; Prasad, K.A.; Mamun, K.A.; Islam, F.; Chopra, S.S. Distributed Energy Resources and the Application of AI, IoT, and Blockchain in Smart Grids. *Energies* **2020**, *13*, 5739. [CrossRef]
34. List of Major Power Outages. 2021. Available online: https://en.wikipedia.org/wiki/List_of_major_power_outages#cite_note-5 (accessed on 5 June 2021).
35. Baimel, D.; Tapuchi, S.; Baimel, N. Smart Grid Communication Technologies. *J. Power Energy Eng.* **2016**, *4*, 1–8. [CrossRef]
36. NIST Framework and Roadmap for Smart Grid Interoperability Standards. 2021. Available online: http://www.nist.gov (accessed on 10 June 2021).
37. Gharavi, H.; Ghafurian, R. Smart Grid: The Electric Energy System of the Future. *Proc. IEEE* **2011**, *99*, 917–921. [CrossRef]
38. Farmanbar, M.; Parham, K.; Arild, Ø.; Rong, C. A widespread review of smart grids towards smart cities. *Energies* **2019**, *12*, 4484. [CrossRef]
39. Da Silva, R.M.; Schettino, S.; de Lima, P.M.R.; Adriano, F.C. Smart grid: Evaluation and trend in Brazil. *Indep. J. Manag. Prod.* **2014**, *5*, 752–776. [CrossRef]
40. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 107094. [CrossRef]
41. Fan, X.; Gong, G. Security Challenges in Smart-Grid Metering and Control Systems. *Technol. Innov. Manag. Rev.* **2013**, *3*, 42–49. [CrossRef]
42. Bari, A.; Jiang, J.; Saad, W.; Jaekel, A. Challenges in the smart grid applications: An overview. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 974682. [CrossRef]
43. Feng, Y.; Qian, Y.; Hu, R.Q. Smart Grid Communication Infrastructures: Big Data, Cloud Computing, and Security. 2018. Available online: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119240136 (accessed on 20 July 2021).
44. Dorri, A.; Luo, F.; Kanhere, S.S.; Jurdak, R.; Dong, Z.Y. SPB: A Secure Private Blockchain-Based Solution for Distributed Energy Trading. *IEEE Commun. Mag.* **2019**, *57*, 120–126. [CrossRef]
45. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
46. Ethereum. 2021. Available online: https://ethereum.org/en/ (accessed on 8 July 2021).
47. Buterin, V. A next-generation smart contract and decentralized application platform. *Ethereum White Pap.* **2014**, *3*, 1–36.
48. Solidity. Introduction to Smart Contracts. 2021. Available online: https://docs.soliditylang.org/en/v0.8.17/ (accessed on 8 July 2021).
49. Dhillon, V.; Metcalf, D.; Hooper, M. The Hyperledger Project. In *Blockchain Enabled Applications*; Springer: New York, NY, USA, 2017. [CrossRef]
50. Zhang, S.; Lee, J.H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, *6*, 93–97. [CrossRef]
51. Energy Web Foundation. 2021. Available online: http://energyweb.org/ (accessed on 9 July 2021).
52. Chen, W.; Xu, Z.; Shi, S.; Zhao, Y.; Zhao, J. A survey of blockchain applications in different domains. In Proceedings of the 2018 International Conference on Blockchain Technology and Application, Halifax, NS, Canada, 30 July–3 August 2018; pp. 17–21. [CrossRef]
53. Muhammad, S.; Jeffrey, S.; Laurent, N.; Charles, K.; Sachin, S.; DaeHun, N.; David, M. Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1977–2008. [CrossRef]
54. Sedlmeir, J.; Buhl, H.U.; Fridgen, G.; Keller, R. The Energy Consumption of Blockchain Technology: Beyond Myth. *Bus. Inf. Syst. Eng.* **2020**, *62*, 599–608. [CrossRef]
55. BBC News. 2021. Available online: https://www.bbc.com/news/technology-56012952 (accessed on 10 May 2021).

56. Homoliak, I.; Venugopalan, S.; Reijsbergen, D.; Hum, Q.; Schumi, R.; Szalachowski, P. The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 341–390. [CrossRef]
57. The Blockchain Trilemma: Decentralized; Scalable; & Secure? 2021. Available online: https://medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3 (accessed on 13 October 2021).
58. What Are Blockchain Confirmations and Why Do We Need Them? 2022. Available online: https://originstamp.com/blog/what-are-blockchain-confirmations-and-why-do-we-need-them/ (accessed on 16 December 2022).
59. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
60. Kolb, J.; AbdelBaky, M.; Katz, R.H.; Culler, D.E. Core concepts, challenges, and future directions in blockchain: A centralized tutorial. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–39. [CrossRef]
61. Types of Machine Learning Algorithms and Their Applications. 2021. Available online: https://medium.com/mlearning-ai/types-of-machine-learning-algorithms-and-their-applications-1dc384f840f8 (accessed on 29 June 2021).
62. Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3154–3164. [CrossRef]
63. Agung, A.A.G.; Handayani, R. Blockchain for Smart Grid. *J. King Saud Univ. Comput. Inf. Sci.* **2020**, *34*, 666–675. [CrossRef]
64. Ante, L.; Steinmetz, F.; Fiedler, I. Blockchain and energy: A bibliometric analysis and review. *Renew. Sustain. Energy Rev.* **2021**, *137*, 110597. [CrossRef]
65. Kim, S.K.; Huh, J.H. A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. *Energies* **2018**, *11*, 1973. [CrossRef]
66. Hertz-Shargel, B.; Livingston, D. Assessing Blockchain's Future in Transactive Energy. 2019. Available online: http://www.jstor.org/stable/resrep24585.1 (accessed on 23 September 2022).
67. Zhao, Y.; Peng, K.; Xu, B.; Liu, Y.; Xiong, W.; Han, Y. Applied engineering programs of energy blockchain in US. *Energy Procedia* **2019**, *158*, 2787–2793. [CrossRef]
68. Ļ Energy. 2021. Available online: https://lo3energy.com/ (accessed on 10 May 2021).
69. Power Ledger Whitepaper. 2021. Available online: https://www.powerledger.io/ (accessed on 10 May 2021).
70. SolarCoin. 2021. Available online: https://solarcoin.org/ (accessed on 10 May 2021).
71. Pylon Network Blockchain. 2021. Available online: https://pylon-network.org/ (accessed on 10 May 2021).
72. Sunchain. 2021. Available online: https://www.sunchain.fr/ (accessed on 10 May 2021).
73. Share and Charge. 2021. Available online: https://shareandcharge.com/ (accessed on 10 May 2021).
74. EnergyCoin Foundation. 2021. Available online: https://www.energycoinfoundation.org (accessed on 10 May 2021).
75. WePower. 2021. Available online: https://wepower.com/ (accessed on 10 May 2021).
76. GridPlus. 2021. Available online: https://gridplus.io/ (accessed on 10 May 2021).
77. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852. [CrossRef]
78. Dorri, A.; Hill, A.; Kanhere, S.; Jurdak, R.; Luo, F.; Dong, Z.Y. Peer-to-Peer EnergyTrade: A Distributed Private Energy Trading Platform. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Republic of Korea, 14–17 May 2019; pp. 61–64. [CrossRef]
79. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3690–3700. [CrossRef]
80. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Jindal, A.; Dua, A.; Kumar, N. EnergyChain: Enabling Energy Trading for Smart Homes Using Blockchains in Smart Grid Ecosystem. In Proceedings of the 1st ACM MobiHoc Workshop on Networking and Cybersecurity for Smart Cities, Los Angeles, CA, USA, 25 June 2018. [CrossRef]
81. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
82. Yang, W.; Guan, Z.; Wu, L.; Du, X.; Lv, Z.; Guizani, M. Autonomous and Privacy-preserving Energy Trading Based on Redactable Blockchain in Smart Grid. In Proceedings of the GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
83. Aloqaily, M.; Boukerche, A.; Bouachir, O.; Khalid, F.; Jangsher, S. An energy trade framework using smart contracts: Overview and challenges. *IEEE Netw.* **2020**, *34*, 119–125. [CrossRef]
84. Fraiji, Y.; Azzouz, L.B.; Trojet, W.; Saidane, L.A. Cyber security issues of Internet of electric vehicles. *IEEE Wirel. Commun. Netw. Conf.* **2018**, *2018*, 1–6. [CrossRef]
85. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access* **2018**, *6*, 13565–13574. [CrossRef]
86. Liu, C.; Chai, K.K.; Zhang, X.; Lau, E.T.; Chen, Y. Adaptive Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform. *IEEE Access* **2018**, *6*, 25657–25665. [CrossRef]
87. Knirsch, F.; Unterweger, A.; Engel, D. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Comput. Sci. Res. Dev.* **2018**, *33*, 71–79. [CrossRef]

88. Su, Z.; Wang, Y.; Xu, Q.; Fei, M.; Tian, Y.C.; Zhang, N. A secure charging scheme for electric vehicles with smart communities in energy blockchain. *IEEE Internet Things J.* **2019**, *6*, 4601–4613. [CrossRef]
89. Kim, M.; Park, K.; Yu, S.; Lee, J.; Park, Y.; Lee, S.W.; Chung, B. A secure charging system for electric vehicles based on blockchain. *Sensors* **2019**, *19*, 3028. [CrossRef] [PubMed]
90. Sun, G.; Dai, M.; Zhang, F.; Yu, H.; Du, X.; Guizani, M. Blockchain-Enhanced High-Confidence Energy Sharing in Internet of Electric Vehicles. *IEEE Internet Things J.* **2020**, *7*, 7868–7882. [CrossRef]
91. Samuel, O.; Javaid, N.; Shehzad, F.; Iftikhar, M.S.; Iftikhar, M.Z.; Farooq, H.; Ramzan, M. Electric vehicles privacy preserving using blockchain in smart community. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Antwerp, Belgium, 7–9 November 2019; Springer: Cham, switzerland; pp. 67–80.
92. Pop, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors* **2018**, *18*, 162. [CrossRef]
93. Kumari, A.; Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. When Blockchain Meets Smart Grid: Secure Energy Trading in Demand Response Management. *IEEE Netw.* **2020**, *34*, 299–305. [CrossRef]
94. Jindal, A.; Aujla, G.S.; Kumar, N.; Villari, M. GUARDIAN: Blockchain-Based Secure Demand Response Management in Smart Grid System. *IEEE Trans. Serv. Comput.* **2020**, *13*, 613–624. [CrossRef]
95. Yahaya, A.S.; Javaid, N.; Javed, M.U.; Shafiq, M.; Khan, W.Z.; Aalsalem, M.Y. Blockchain-Based Energy Trading and Load Balancing Using Contract Theory and Reputation in a Smart Community. *IEEE Access* **2020**, *8*, 22168–22218. [CrossRef]
96. Cutsem, O.V.; Dac, D.H.; Boudou, P.; Kayal, M. Cooperative energy management of a community of smart-buildings: A Blockchain approach. *Int. J. Electr. Power Energy Syst.* **2020**, *117*, 105643. [CrossRef]
97. Meghana, P.; Yammani, C.; Salkuti, S.R. Blockchain technology based decentralized energy management in multi-microgrids including electric vehicles. *J. Intell. Fuzzy Syst.* **2022**, *42*, 991–1002. [CrossRef]
98. Kalakova, A.; Zhanatbekov, A.; Surash, A.; Nunna, H.K.; Doolla, S. Blockchain-based decentralized transactive energy auction model with demand response. In Proceedings of the IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2–5 February 2021; pp. 1–6. [CrossRef]
99. Tsao, Y.C.; Thanh, V.V.; Wu, Q. Sustainable microgrid design considering blockchain technology for real-time price-based demand response programs. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106418. [CrossRef]
100. Merrad, Y.; Habaebi, M.H.; Toha , S.F.; Islam, M.R.; Gunawan, T.S.; Mesri , M. Fully Decentralized, Cost-Effective Energy Demand Response Management System with a Smart Contracts-Based Optimal Power Flow Solution for Smart Grids. *Energies* **2022**, *15*, 4461. [CrossRef]
101. Zhou, Z.; Wang, B.; Guo, Y.; Zhang, Y. Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles. *IEEE Trans. Emerg. Top. Comput. Intell.* **2019**, *3*, 205–216. [CrossRef]
102. Vivar, A.; Castedo, A.; Orozco, A.; Villalba, L. An analysis of smart contracts security threats alongside existing solutions. *Entropy* **2020**, *22*, 203. [CrossRef]
103. Sakhnini, J.; Karimipour, H.; Dehghantanha, A.; Parizi, R.M. Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach. *Phys. Commun.* **2021**, *47*, 101394. [CrossRef]
104. Javaid, N.; Jan, N.; Javed, M.U. An adaptive synthesis to handle imbalanced big data with deep siamese network for electricity theft detection in smart grids. *J. Parallel Distrib. Comput.* **2021**, *153*, 44–52. [CrossRef]
105. Combining Blockchain with Machine Learning: Benefits and Challenges. 2022. Available online: https://www.knowledgenile.com/blogs/combining-blockchain-with-machine-learning-benefits-and-challenges/ (accessed on 6 December 2022).
106. Said, D. A decentralized electricity trading framework (DETF) for connected EVs: A blockchain and machine learning for profit margin optimization. *IEEE Trans. Ind. Inform.* **2020**, *17*, 6594–6602. [CrossRef]
107. Ferrag, M.A.; Maglaras, L. DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids. *IEEE Trans. Eng.* **2020**, *67*, 1285–1297. [CrossRef]
108. Jamil, F.; Iqbal, N.; Imran, S.A.; Kim, D.H. Peer-to-Peer Energy Trading Mechanism Based on Blockchain and Machine Learning for Sustainable Electrical Power Supply in Smart Grid. *IEEE Access* **2021**, *9*, 39193–39217. [CrossRef]
109. Fu, Z.; Dong, P.; Ju, Y. An intelligent electric vehicle charging system for new energy companies based on consortium blockchain. *J. Clean. Prod.* **2020**, *261*, 121219. [CrossRef]
110. Ashfaq, T.; Khalid, M.I.; Ali, G.; Affendi, M.E.; Iqbal, J.; Hussain, S.; Ullah, S.S.; Yahaya, A.S.; Khalid, R.; Mateen, A. An Efficient and Secure Energy Trading Approach with Machine Learning Technique and Consortium Blockchain. *Sensors* **2022**, *22*, 7263. [CrossRef]
111. Cryptocurrency Mining and Renewable Energy: Friend or Foe? 2021. Available online: https://www.smart-energy.com/magazine-article/cryptocurrency-mining-and-renewable-energy-friend-or-foe/ (accessed on 13 October 2021).
112. Blockchain Energy Consumption Should be Transparent in Europe—Call. 2021. Available online: https://www.smart-energy.com/industry-sectors/energy-efficiency/blockchain-energy-consumption-should-be-transparent-in-europe-call/ (accessed on 13 October 2021).
113. Bravo-Marquez, F.; Reeves, S.; Ugarte, M. Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions. In Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 4–9 April 2019; pp. 119–124. [CrossRef]
114. Chenli, C.; Li, B.; Shi, Y.; Jung, T. Energy-recycling blockchain with proof-of-deep-learning. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Republic of Korea, 14–17 May 2019; pp. 19–23. [CrossRef]

115. The Data Impact of Smart Metering. 2021. Available online: https://www.ibi.com/blog/james-cotton/16610/ (accessed on 12 October 2021).
116. Swedac Places New Demands on the Country's Electricity Meters. 2021. Available online: https://www.swedac.se/swedac-staller-nya-krav-pa-landets-elmatare/ (accessed on 19 October 2021).
117. Yapa, C.; de Alwis, C.; Liyanage, M. Can blockchain strengthen the energy internet? *Network* **2021**, *1*, 95–115. [CrossRef]
118. Hafid, A.; Hafid, A.S.; Samih, M. Scaling blockchains: A comprehensive survey. *IEEE Access* **2020**, *8*, 125244–125262. [CrossRef]
119. How Many EVs Can the Power Network Cope with? 2021. Available online: https://new.siemens.com/global/en/company/stories/infrastructure/2020/e-mobility-how-many-evs-can-the-power-network-cope-with.html (accessed on 20 October 2021).
120. Tavakoli, A.; Saha, S.; Arif, M.; Haque, M.; Mendis, N.; Oo, A. Impacts of grid integration of solar PV and electric vehicle on grid stability, power quality and energy economics: A review. *IET Energy Syst. Integr.* **2020**, *2*, 243–260. [CrossRef]
121. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; Correia, M. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Comput. Surv.* **2021**, *54*, 1–41. [CrossRef]
122. Lisk. 2022. Available online: https://lisk.com/blog/research/blockchain-interoperability-how-does-it-work (accessed on 2 November 2021).
123. Ferreira, J.C.; da Silva, C.F.; Martins, J.P. Roaming Service for Electric Vehicle Charging Using Blockchain-Based Digital Identity. *Energies* **2021**, *14*, 1686. [CrossRef]