network

MDPI

Review

Can Blockchain Strengthen the Energy Internet?

Charithri Yapa [1], Chamitha de Alwis [1] and Madhusanka Liyanage [2,3,*]

[1] Department of Electrical and Electronic Engineering, University of Sri Jayewardenepura, Gangodawila, Nugegoda 10250, Sri Lanka; charithriyapa@sjp.ac.lk (C.Y.); chamitha@sjp.ac.lk (C.d.A.)
[2] School of Computer Science, University College Dublin, D04 V1W8 Dublin, Ireland
[3] Centre for Wireless Communications, University of Oulu, 90014 Oulu, Finland
* Correspondence: madhusanka@ucd.ie or madhusanka.liyanage@oulu.fi

Abstract: Emergence of the Energy Internet (EI) demands restructuring of traditional electricity grids to integrate heterogeneous energy sources, distribution network management with grid intelligence and big data management. This paradigm shift is considered to be a breakthrough in the energy industry towards facilitating autonomous and decentralized grid operations while maximizing the utilization of Distributed Generation (DG). Blockchain has been identified as a disruptive technology enabler for the realization of EI to facilitate reliable, self-operated energy delivery. In this paper, we highlight six key directions towards utilizing blockchain capabilities to realize the envisaged EI. We elaborate the challenges in each direction and highlight the role of blockchain in addressing them. Furthermore, we summarize the future research directive in achieving fully autonomous and decentralized electricity distribution networks, which will be known as Energy Internet.

Keywords: energy internet; smart grid 2.0; blockchains; 6G; key directions; limitations and challenges

check for updates

Citation: Yapa, C.; de Alwis, C.; Liyanage, M. Can Blockchain Strengthen the Energy Internet? *Network* **2021**, *1*, 95–115. https://doi.org/10.3390/network1020007

Academic Editor: Chin-Tser Huang

Received: 26 May 2021
Accepted: 22 July 2021
Published: 26 July 2021

1. Introduction

The concept of smart grids emanated with the adoption of Internet of Things (IoT) devices and technologies, such as Internet connected advanced sensors and smart meters in electricity grids [1,2]. This facilitated bi-directional information flow to achieve near real-time grid operations while incorporating dynamic electricity pricing and effective Demand Response (DR) mechanisms [3]. Meanwhile, the energy requirement of the world is expected to grow continuously [4]. Catering to this requirement demands an increasing number of grid interconnections of Distributed Energy Resources (DER) contributing synergistically with one another. However, conventional smart grids, which are governed by a centralized authority, are not capable of facilitating this requirement. This urges the need for a more scalable, flexible and distributed grid architecture [4].

In response to this demand, the next iteration of the conventional smart grids, Smart Grid 2.0 (identified as the Energy Internet (EI) in this paper), is being realized to establish bi-directional energy and information transfer. This uses the electricity grid infrastructure and Internet Protocol (IP) based features of the Internet respectively [5]. This includes Distributed Network Protocol (DNP3) for maximizing the utilization of DERs and Transmission Control Protocol (TCP) based protocols, such as, IPv6 over Low-Power wireless Personal Area Networks (6LowPAN), to facilitate communication between compact, inexpensive, low-power, embedded devices and IEEE 802.15.4 networks. This is to enhance security features of the existing smart grids. Furthermore, EI facilitates real-time information exchange including energy usage data, dynamic pricing information and control signals through such implementations.

IoT devices, including smart meters and sensors, communicate real-time measurement data of the large-scale participation of the Distributed Generation (DG) [6].

This is envisaged to facilitate autonomous operation of energy grids, benefiting seamless integration of DG without the involvement of a third party compared to the conventional counterpart. Implementation of EI grids is proposed as an overlay of four layers:

namely, physical layer, communication and control layer, application layer and data analysis layer [5]. The former two are comprised of IoT devices and beyond 5G communication technologies, enabled through edge computing respectively. The latter two layers of the novel architecture incorporate the applications of the envisaged EI grid and data analysis technologies supported through big data management [7].

Applications of EI span beyond offering dynamic energy prices to the consumers and obtaining their contribution in DR initiatives. They also exhibit prospects in multi-dimensional aspects, including: (1) Peer-to-Peer (P2P) energy trading; (2) plug-and-play interfacing for DERs; (3) microgeneration; (4) Demand Side Integration (DSI); (5) automation and management of distribution networks; and (6) management of energy data. Figure 1 illustrates the interrelationship of these applications. Thus, EI grid architecture facilitates the paradigm shift from the monopoly vertical hierarchy towards a decentralized network configuration with bi-directional energy and information exchange across the grid and internet respectively. A comparison elaborating the significant differences of the conventional and next generation smart grids is presented in Table 1.

Table 1. Comparison of smart grids and EI grids [6,8,9].

Conventional Smart Grids	EI Grids/Smart Grid 2.0
Centralized power distribution	Decentralized power distribution
Integration of limited energy resources (i.e., conventional generation and a few Renewable Energy Sources (RES))	Integration of heterogeneous DER including RES, EVs and ESS
ine Utility-centric operations where utility governs the ownership of the grid Distribution System Operator (DSO)	Consumer-centric operations with equal level playing field for all participating stakeholders
ine Energy traded and information exchanged between the DSO and the customers	Energy traded and real-time information shared in a peer-to-peer manner
Closed proprietary and non-inter-operable Information and Communication Technology (ICT) is the disruptive technology enabler	Open and inter-operable technologies based on IP is the disruptive technology enabler
Impedes autonomous grid operation	Integrates AI and ML technologies to enable autonomous grid operations

Together with these applications, EI envisages autonomous grid operation where the central authority governing the grid under the current context will be overlooked [4]. Further, this would be protruding as consumers begin to gain liberalization in the energy market and actively participate in power production. Human intervention in the decision-making process will be automated through smart contracts, facilitated by Artificial Intelligence (AI) and Machine Learning (ML) algorithms.

However, as a consequence of delegation of authority among stakeholders and alleviating the contribution of the intermediary, trust establishment would become a key consideration regarding EI grids. Additionally, the cyber-physical system created by the increasing number of stakeholders connecting to the grid through the diverse applications of EI would result in innumerable access points and large data sets, which would elevate its vulnerability towards malicious attacks. Performing grid operations with a large number of heterogeneous access points will be challenging. This would require secure and reliable communication channels for control implementation using the aggregated data, which requires prevention from information leakage [4].

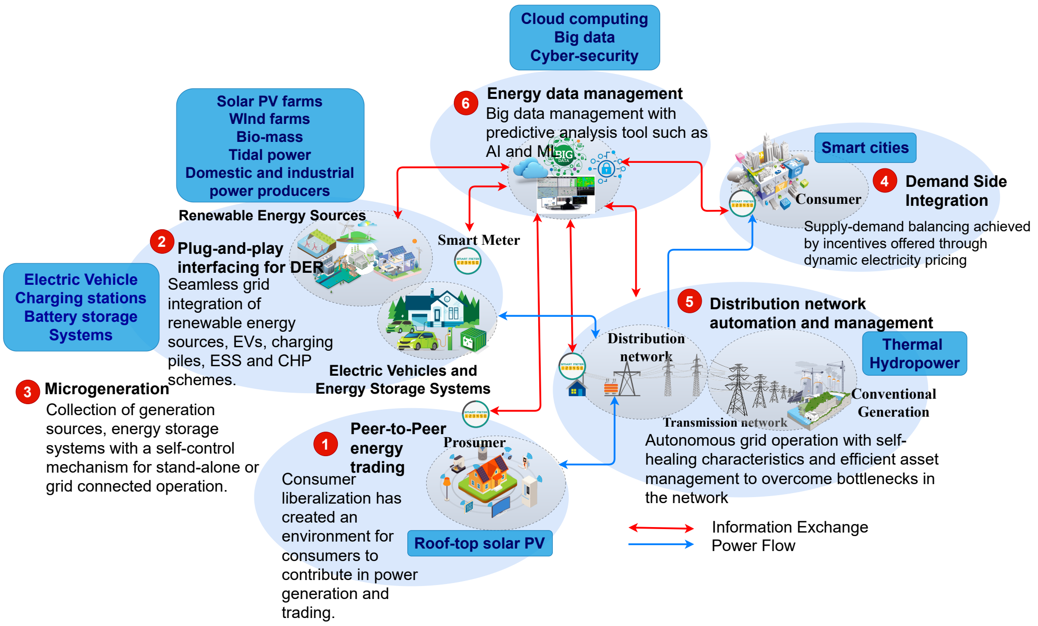

Figure 1. Overview of the bi-directional energy and information flows in the applications of the envisaged EI grids.

EI will be enabled through blockchain, which is a Distribute Ledger Technology (DLT) with inherent features including immutability, transparency, distributed verification/storage and decentralized authority over a peer-to-peer network [10]. Security features and privacy-preserving techniques incorporated with blockchains offer solutions to mitigate cyber-physical attacks and privacy violations within the operations of the EI grid. Smart contracts enable autonomous operations of the EI grid with the execution of programmed scripts upon the fulfilment of the defined prerequisites [11]. Some processes could be automated through the utilization of smart contracts implemented upon blockchain platforms. These include billing for the energy consumption, invocation and revocation of certificates to authorize heterogeneous DER integration, authorizing payments upon energy trading, dynamic price signalling and monitoring IoT devices to identify node tampering [12–14]. Realization of EI is also envisaged to be facilitated through the developments of beyond 5G and 6G communication networks through inherent features. These include DLT/blockchain, ultra-massive machine-type communication, extremely low-power communication, extremely reliable low-latency communication, AI and ML, big data management and distributed processing through edge intelligence [15–20].

Even though blockchain is expected to become a key enabler of EI, the integration of blockchain platforms with EI has not been investigated to a considerable extent [4,8,21]. This offers research directives in abundance and to address the identified research gap, this paper presents six key directions of blockchain utilization in EI grid realization. These are (1) energy sustainability through heterogeneity; (2) improved trust, security and privacy; (3) ultimate grid reliability and stability; (4) decentralized scalability; (5) advanced big data management; and (6) grid intelligence. The significance of inherent features of the blockchain, utilized towards realization of the next generation of smart grids in the identified directions, have been illustrated in Figure 2. Challenges pertaining to each identified direction and the role of blockchain utilization have been discussed, summarizing the future research directive in achieving fully autonomous and distributed electricity distribution networks [15]. Hence, this paper aims to present a clear insight of blockchain utilization for strengthening EI grids to deliver maximum benefits to all participating stakeholders.

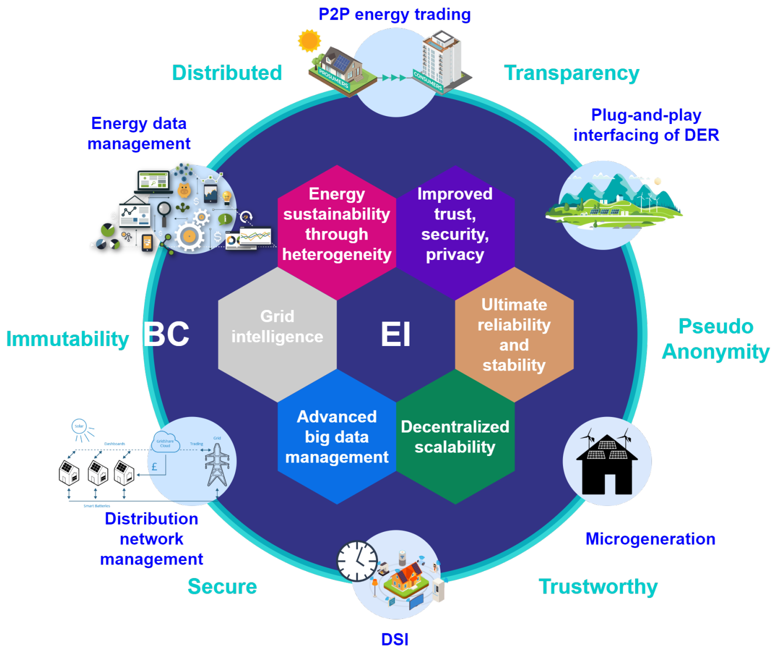

Figure 2. Key directions of blockchain utilization in EI realization.

The rest of the paper is organized as follows: Section 2 provides an insight regarding how blockchains can facilitate futuristic electricity distribution to be sustainable through heterogeneity. Section 3 highlights the improvement achieved in security, privacy and trust establishment without the involvement of a third party, related to operations of the future EI grids. The benefits identified through the integration of blockchains include mitigating cyber-physical attacks leading to disruptions in the electricity supply, preventing breaches of privacy and instating trust in distributed operation. Section 4 signifies the contribution of blockchain-based EI grids towards achieving grid stability and reliability, while Section 5 discusses the benefits offered through improved scalability to cater to the increasing number of stakeholders connecting. Sections 6 and 7 elaborate on the role of blockchain to facilitate predictive data analysis integrated with EI data management. Each of these sections highlight the role of blockchains in this progression and the way forward in each individual aspect.

2. Energy Sustainability through Heterogeneity

Conventional power grids rely mostly on limited variants of energy sources for the fulfillment of the demand [22]. Renewable energy generation, intermittent in nature, geographically dispersed and located in the close proximity of the load centres, is replacing fossil fuel–based generation with a high carbon footprint [5,23]. Energy Storage Systems (ESS) are utilized with the intention of maximizing the benefits of the renewable sources [8]. Energy security is diversified through the implementation of Combined Heat and Power (CHP), using fuel cells where the waste heat from electricity production is utilized for space heating. Consumers who have gained more authority under the envisaged grid context can trade the excess power production from their domestic installations, achieving the benefit of the dynamic real-time energy prices. Electric Vehicles (EV) are receiving attention as a green transportation alternative while the charging stations are located across a large geographical area to facilitate their usage [4]. Incorporating these heterogeneous energy sources from various stakeholders into a single platform would improve the sustainable energy usage.

However, the following challenges can be identified in the road map of integrating heterogeneous energy sources to enable envisaged EI grid operations.

2.1. Key Challenges

1. **Seamless grid integration:** How can we facilitate seamless grid integration of DERs in order to achieve a decentralized, customer-centric grid architecture [23]?
2. **Decentralized marketplace:** How is it possible to achieve a decentralized marketplace with dynamic price signaling and maximized consumer satisfaction [24]?
3. **Secure communication:** How can we manage secure communication links and storage for large energy data aggregation arising from the increasing number of grid interconnections in a decentralized and secure platform?
4. **Transient and dynamics:** How can we mitigate the transient over voltages and undesirable dynamics resulting from bi-directional energy routing and uncoordinated grid interconnections of DG, ESS and EV [25]?
5. **Improving interoperability:** How can we achieve interoperability of heterogeneous energy sources that adopt different grid interconnection standards?

2.2. Role of Blockchain

Smart contracts can be utilized to ensure seamless integration of DERs through invocation of certificates and revocation of them upon request. Blockchain establishes a trusted environment in a decentralized marketplace, which provides confidence for the prosumers to engage in P2P energy trading while avoiding the risk of non-repudiation and double spending [12]. Microgrid implementations such as Brooklyn microgrid [26] and Power Ledger [27] in Australia could be identified as promising, decentralized blockchain-based solutions facilitating P2P trading. Furthermore, Share & Charge in Germany and Juice Net of North America are milestone projects in dencentralized energy markets for P2P EV charging [13]. Inherent cryptographic encryption of blockchain would enable user authentication without third-party intervention. Blockchain could further function as a secure and reliable data communication link and storage platform for efficient management of large data sets associated with these diverse EI applications. Energy sustainability is assured with transparent exchange of heterogeneous forms of energy [12].

However, mitigation of transient overvoltages and issues related to interoperability, which arise while the implementation of heterogeneous EI grids cannot be facilitated through a blockchain platform itself. Adequate standards need to be implemented with the intention of sustaining desirable grid operations.

2.3. Future Directions

The incentive-based benefits obtained through real-time dynamic electricity pricing are receiving attention in the grid integration of DERs beyond small scale capacities at different voltage levels of the grid [28]. This will be facilitated through 5G and beyond 5G technologies, offering ultra-reliable, low-latency communication and edge intelligence supporting remote communication for intermittent connectivity respectively. Blockchain would provide an overlay with distributed storage facility. Precision decision-making, incorporating AI along with reliable communication and data processing through edge devices, as envisaged with 6G, would enable the realization of next-generation electricity networks [29].

Lessons: Decentralized energy trading is a well-established research area with several approaches proposed and real-world scenarios being implemented [26,27,30–34]. Examples include P2P trading of renewable energy [33,35,36]. Communication links are expected to be made secure through proposed blockchain integrated architecture, which, however, has room for improvement with novel Smart Grid 2.0–specific security threats to be addressed [37]. Meanwhile, facilitating seamless grid integration of DGs [12] and their interoperability [8,21] are the challenges with future research prospects considering the existing work, which would require collaborative technological approaches facilitated through blockchain.

3. Improved Trust, Security and Privacy

Future energy grids have envisaged seamless peer-to-peer connectivity with the autonomous operation in contrast to conventional smart grid context. This is where the Distribution System Operator (DSO) governs the ownership and authority over the management of infrastructure, certificate invocation and revocation for DER integration and supervision of energy exchange with the grid [26,38]. Consumers liberating in the envisaged EI grids would promote microgeneration where energy is traded between two nodes of the network without the involvement of a third party, reducing the losses and additional cost incurred. A mechanism which could establish the trust factor with minimal middle-man involvement would drive the energy grids towards the expectations.

Furthermore, EI grid operation aggregates data related to real-time energy consumption through smart meters, electrical measurements obtained by IoT sensors, bids to trade excess energy, requests to fulfil demand deficit and control signals for grid regulation. The key considerations that strengthen the future energy network would be privacy-preserving protocols to eliminate the risk of revealing individual energy usage patterns, exposing consumer identity and disclosing information to a third party without the consent of the user. Additional key considerations would be secure operations through reduced vulnerabilities of the grid towards physical attacks, software attacks, network attacks, control-related attacks and encryption attacks [39]. The increase in the number of access points connected to the network and the heterogeneity of the devices observed would have a direct impact over the management of trust, security and privacy issues of the speculated EI grids [40].

The following challenges were identified, impeding the secure and privacy-protected operations of EI grids for which a blockchain platform would be a promising solution.

3.1. Key Challenges

1. **Device tampering:** How can we prevent tampering and unauthorized accessing of smart meters and smart sensors to ensure integrity of the obtained energy measurements [40]?
2. **Man-in-the-Middle attacks in EI grids:** How can we establish a secure communication link between the prosumer and the consumer during energy trading and prevent Man-in-the-Middle attacks causing data manipulation?
3. **DDos attacks in EI grids:** How will it be possible to detect Distributed Denial of Service (DDoS) attacks causing deliberate traffic of energy requests and depriving the legitimate users from consuming energy [41]?
4. **Privacy issues:** Can a consumer participate in DSI initiatives while preserving the privacy of energy consumption data which can trace back to the behavioral patterns of the user?
5. **Authentication:** How can the identity of a node in the energy grid be verified in a decentralized architecture without revealing the connection between the energy signature and the owner's name and location?
6. **AI and ML related-attacks:** How can we mitigate data poisoning attacks related to integration of AI and ML techniques in predictive data analysis [42,43]?

3.2. Role of Blockchain

Blockchain platform inherently establishes trust with minimal external interventions while offering a secure and transparent mechanism to create a reliable link between the nodes participating in energy trading. Transactions are recorded in an immutable and transparent format while each node holds a copy of the current ledger [21], preventing data modification and false data injection. Smart contracts could automate processes such as billing and finance settlement without the requirement of a trusted third-party intervention at a cost, while blockchains with the inherent use of Public Key Infrastructure (PKI) would enable identity authentication with pseudo-anonymity, privacy preservation of the participating nodes and protection of data integrity [44]. The Lightning Network and Smart Contract (LNSC) model proposed in [45] offers a security model comprising of registration, scheduling, authentication and charging phases. This integrates security options for user authentication, facilitating secure mechanisms for charging and discharging EVs. Guardtime, a US-funded project, has utilized a keyless authentication scheme for scalable EI grids with hash-function cryptography and digital signature authentication [21].

Cryptanalysis, in which breach of encryption algorithm is observed, can be addressed through the digital signatures incorporating private-public key pair, which is unique to each stakeholder. AI and ML models introduce a new set of adversaries, including data poisoning attacks, model evasion, extraction and inversion–related ML techniques utilized in EI grid realization [42]. Data poisoning can be mitigated through the incorporation of blockchain distributed data storage, while alternatives such as adversarial machine learning, moving target defence and defensive distillation would provide resilience against adversaries identified in ML models [42].

Even though tampering of IoT devices and undesirable data traffic in communication channels cannot be fully addressed through blockchain initiatives, such platforms can be utilized to monitor the scenario and execute corrective measures to minimize the damage. Further, the existing security and privacy-preserving mechanisms incorporating cryptography and 51% attacks on the blockchain-based applications are vulnerable to advancements in quantum computing, thus demanding for quantum-resilient security alternatives [46–48].

3.3. Future Directions

Under the current blockchain context, immutability of the distributed ledger has been exploited to establish the trust factor and verify information security. However, the developments emerging with 6G technology facilitate distributed computing utilizing edge devices, which could further enable consolidation of resources to achieve computational efficiency [49]. Such collaborations would pose a risk of accumulating 51% authority over the peer nodes, thereby gaining capabilities for modification of the past records. Such adversaries should be addressed in the envisaged grid operation.

Further, integrity and confidentiality of the information, along with the identity of the user, could be compromised through the revealing of the public and private keys used in PKI. This could be mainly due to the prolonged usage of the keys and as a result of the malicious attempts to reveal these cryptographic text patterns utilizing quantum computing, which is the most recent development enabling extensive computational capabilities [8]. Ensuring security and privacy with technological progressions would be challenging in future grid implementations [50].

Lessons: Blockchain integration with Smart Grid 2.0 has facilitated in mitigating software and network related attacks, including Man-in-the-Middle and DDoS adversaries [37]. Further, the existing work has proposed different user authentication and privacy-preserving approaches, which have been implemented through cryptographic techniques used in blockchain [45,51–56]. The most widely adapted approach could be identified as cryptographic encryption–based digital signatures for user verification [37]. However, modern smart grids, which are to incorporate predictive data analytic tools for intelligent decision, are vulnerable to AI and ML–related attacks [15,16]. These adversaries would overlay the security threats governing Smart Grid 2.0, which would require accelerating the existing research initiatives.

4. Ultimate Reliability and Stability

Future consumers would heavily rely on electricity through the utilization of smart appliances with the onset of smart buildings, while the future electricity grids are envisaged to rely more on intermittent generation, including renewable power production incorporated with ESS [1]. Grid stability and reliability of the power supply become vital factors of the speculated EI architecture [57].

The intermittent operation of the renewable generation and the energy consumption patterns of the dynamic loads are difficult to predict. Stability achieved through the grid surveillance performed using IoT devices, facilitated by Deep Learning (DL) techniques, would drive the expectations of the future electricity grids while managing the dynamic nature of both generation and loads [58].

Delivering a reliable power supply with the stochastic nature of the electricity generation and consumer demands real-time monitoring through IoT devices, precise decision-making capabilities empowered through AI and ML-enabled big data management, efficient information exchange, data processing through advanced communication protocols and distributed computing. These would further be the pillars that strengthen the future EI grids [16].

However, the following challenges have to be addressed in order to ensure stable and reliable grid operations.

4.1. Key Challenges

1. **Supply-demand balancing:** How can we facilitate seamless integration of DG to achieve dynamic response in power output to rectify supply-demand mismatch [23]?
2. **Intermittent generation:** What will the possibility be of securing stable and reliable grid operation in a decentralized architecture with no third-party involvement and heterogeneous grid interconnections?
3. **Secure communication:** How can we facilitate secure communication links to improve the exchange of energy data and control signals between peers to improve stability and reliability of a distributed grid?
4. **Intelligent decision-making:** How do we arrive at intelligent decisions for optimal generation allocation to improve grid stability management?
5. **Energy theft:** How can we prevent energy theft, ensuring the consumer a reliable energy supply?
6. **Power quality management:** How can we mitigate the issues related to non-compliance of power quality standards by the prosumer, DG owner and consumer?

4.2. Role of Blockchain

Blockchain and smart contracts can be utilized to invoke certification for seamless grid integration of renewable energy generation upon fulfillment of the prerequisites. This would decrease the latency and improve grid stability [59,60]. Lightweight blockchain platforms would further provide means of increasing the transaction throughput of the energy grid. Efficient correction of supply-demand mismatch through precision decisions arrived upon predictive analysis would facilitate reliable future grids. Blockchains would be the means for secure storage and broadcasting of energy bids and demand requests, enabling the predictive analysis on aggregated EI data. The integrity of data sets used for the application of AI and ML technologies could be ensured through the cryptographic encryption methods incorporated with blockchain [29]. The Spanish renewable initiative Iberdrola is utilizing blockchain for tracking of wind power generation and is expected to contribute in seamless grid integration of DER by issuing origin certification [13]. The decentralized solution eliminates the need for a third party as a middle man.

Blockchain, however, cannot be identified as the ultimate solution for ensuring stability and reliability of futuristic decentralized grid architecture with no central authority. Advanced control strategies need to be proposed in this aspect, with blockchain facilitating them from the rear end by providing secure data transmission and storage. Deployment of smart contracts would enable autonomous execution of the control strategies for securing grid stability.

4.3. Future Directions

Grid stability and reliability are expected to progressively advance through AI and ML algorithms, enhancing the capabilities of the future grids beyond expectations. Deployment of Virtual Power Plants (VPP) and Autonomous Vehicles (AV) contributing in Vehicle-to-Grid (V2G) and Vehicle-to-Vehicle (V2V) interactions match the supply with the demand.

Meanwhile, smart cities that integrate smart buildings with intelligent appliances would reshape the future grid architecture, with autonomous stability and reliability management approaches being a requisite [4,61].

Lessons: Elimination of energy theft through double auction and other mechanisms has been presented in the existing literature [12,15,51,56,62]. However, securing communication channels to offer a reliable electricity supply while addressing the challenges related to intermittent generation of DGs have research prospects for maximization of renewable energy utilization in Smart Grid 2.0 [12,37]. This would enable matching the supply with the demand; however, maintaining the power quality within the allowable limits [51] would be another challenge to overcome in the envisaged grid architecture, with little research being carried out related to this aspect.

5. Decentralized Scalability

EI envisages millions of seamless interconnections of independent producers, microgeneration comprising of solar PV, wind, fuel cells, ESS for maximizing the benefits of intermittent renewable generation and EVs with their charging stations dispersed in a large geographical area [3]. IoT devices connected to this network would, thereby, aggregate large volumes of transaction and energy information. These access points increase in their numbers, owing to the attention received by the EI concept in the future grid architecture where decentralized scalability would be a role player. 6G-enabled distributed processing by edge computing, cloud data storage, AI and ML–based competent control algorithms, information security and privacy-protected data can be identified as the facilitators of decentralized scalability of the envisaged EI grids [16,57].

Challenges to be addressed in terms of achieving decentralized scalability, with the onset of increasing numbers of grid interconnections, have been discussed below.

5.1. Key Challenges

1. **Scalable, decentralized EI grids:** How can we offer scalable solutions for decentralized energy grids which would facilitate integration of large numbers of heterogeneous generation sources and extending the customer base [4]?
2. **Low-latency grid synchronization:** How can we achieve low-latency decision-making for the synchronization of large numbers of connected DGs [60]?
3. **Scalable data management:** How can we mange the large energy data set generated by the continuously expanding consumer base of future EI grids?

5.2. Role of Blockchain

Inherent features of blockchain enable the delegation of processing to edge nodes and cloud storage platforms through a trustless trust establishment. Low latency and high throughput can be achieved through distributed processing which further provides solutions to intermittent connectivity in remote areas in a store and forward manner. PETCON, a secure P2P trading mechanism for plug-in hybrid EVs [63], and Guardtime, a permissioned blockchain-based approach, are considered to be scalable solutions for complex data exchange in EI grids.

Further, with the incorporation of off-chains, side-chains, sharding and edge computing to offload the computational burden, better results have been obtained to cater for the increase of nodes connected with minimum trust issues. This would be further empowered with the speculated advancements in communication infrastructure by deployment of 6G technologies, enabling edge intelligence [29]. DL and big data analysis applied on the data aggregated in cloud storage would be controlled and managed through a secure mechanism utilizing blockchain platforms. Leakage of information would be shielded and better control over the data can be achieved through such approaches [16].

Scalability issues related to EI grid implementations, however, have not been fully overcome through the blockchain platforms. These can be identified as future research prospects for the improvement of the applicability of blockchain for energy grid management.

5.3. Future Directions

Achieving distributed scalability at the cost of compromising information security and privacy of the user respectively defies the expectations of the future grids. The blockchain trilemma would receive attention in the pathway towards successful implementation of the futuristic grid infrastructure [64]. The vulnerabilities in grid security would expand beyond the current extent with the scalable, decentralized operations. Thus, proper measures would be a necessity to instate the trust in the EI grids.

Further, connectivity has a major impact in reaching the scalability goals, which can be addressed through advancements such as 5G and 6G technologies. The former would enable low-latency communication channels while the latter would address the intermittent connectivity in rural geographical locations by utilizing edge devices [29].

Lessons: Scalability of EI grids are partly addressed through off-chain and side-chain implementations [65] as well as suitable selection of the blockchain platform [21,32,66]. This includes scalable initiatives such as NRG Xchange [32] and analytical selection of the blockchain platform such as HyperLedger over Ethereum [64]. Energy data management with the increasing number of consumer connections would be a challenge to be addressed, while facilitating low-latency grid synchronization of DERs has not been discussed in the existing literature [12,65,67].

6. Advanced Big Data Management

Big data management facilitates performing of predictive analysis on aggregated large data sets using AI and ML algorithms [68]. Such data set will be of utmost value to a large community of stakeholders. In the instance of the energy sector, this includes power producers, consumers, utilities and non-power participants such as policymakers, investors and financial institutions. The data set can be utilized in various applications in order to facilitate EI grid transformation [4]. Grid stability and reliability of power supply are secured through the predictive analysis of this aggregated data using AI and ML approaches and, further, by stimulating autonomous operations [16]. Energy sustainability achieved through the heterogeneity of the sources is managed and coordinated using the effective utilization of measurements obtained from the connected IoT devices.

However, the aggregated data should be protected against malicious attacks which could manipulate the information, sabotaging the grid operations while preventing leakage of information to external parties. Big data management would, thus, be considered as an important entity, driving the practical realization of the future grids [4].

6.1. Key Challenges

1. **Data silos:** How can we overcome data silos and establish trust between prosumers, microgrids and large power plants for better coordination?
2. **Secure communication:** How can we achieve secure communication channels between smart meters/smart sensor nodes and the Energy Management System (EMS) [40]?
3. **Secure data storage:** How can we provide secure, privacy-preserving and scalable storage for the aggregated large data sets containing generation and consumption patterns of consumers and prosumers respectively?
4. **Data integrity protection:** How can we ensure the integrity of the stored energy data utilized for AI model development, training, validation through ML techniques, testing and deployment [40]?
5. **Data ownership:** How can we ensure ownership of the aggregated energy consumption/production pattern data to prevent privacy-violations arising from unauthorized trading of these sensitive data to a third party?
6. **Scalable grids:** How can we facilitate the management of large data volumes while offering scalabilty for grid expansion with numerous grid integration of prosumers, microgrids, EVs and collaborative consumers participating in DSIs?

6.2. Role of Blockchain

Communication technologies are progressing towards delivering an efficient, ultra-reliable, low-latency service to the consumer through 5G, thereby facilitating the data aggregation process. Further, 6G network operation enables delegation of the computational capabilities for the processing of information to multiple edge devices [20,29]. Blockchain will be an integral part of both of these scenarios and its integration would enable secure data, control signal transmission and trust establishment for distributed processing using edge computing respectively [69].

Data aggregation further involves secure data storage on cloud-based platforms, in which blockchain would ensure cyber-security, information security and network security, preventing malicious attacks that could modify data. The hash function incorporated in blockchain ensures the integrity of the stored data. Moreover, privacy could be enacted, gaining control over the information through the deployment of smart contracts for data sharing while maintaining anonymity [70,71].

Predictive analysis upon the aggregated data will be facilitated through AI and ML, in which blockchains could contribute as a trusted mediator. This would ensure the integrity of the data incorporated and the algorithms compiled [16] while deploying autonomous operations through smart contracts.

Blockchain alone, however, cannot facilitate scalable platforms for big data management. This demands alternative distributed storage platforms supported by the blockchain from the back end, which include utilization of off-chain storage and Inter-Planetary File System (IPFS).

6.3. Future Directions

Blockchains in collaboration with smart contracts could extend the utilization of the aggregated data set where individual stakeholders (consumer, prosumer and individual power producers) would trade the information to potential investors, asset managers such as financial institutions, utilities and policy makers to obtain financial benefits. The secure and transparent link will be established through 6G architecture and the blockchain platform [72].

Lessons: Future EI grids will be integrated with AI and ML for predictive data analysis, giving rise to a new set of challenges which were not encountered in previous generations of smart grids [70]. Blockchain integration with EI grids have facilitated data integrity protection through cryptographic hashing [37] and is well addressed in the existing literature. However, addressing the challenges, including data silos [73], facilitating secure, scalable data communication and storage with privacy-preserving data ownership [21,74], would require further research attention.

7. Grid Intelligence

The trends of the future energy grids have been speculated as autonomous power delivery operation, self-healing fault recovery, efficient fault location identification to reduce system downtime, minimized human interactions in the decision-making process and accurate demand forecasting [61]. AI and ML have been recognized as prospective candidates in these domains, which would stimulate the emergence of intelligent electricity grids. The former would facilitate automated network control through Zero-touch network and Service Management (ZSM) [42] while predictive models will be enabled through ML techniques. Process automation includes automated billing, renewable integration through certificate invocation upon request and revocation owing to noncompliance with the grid prerequisites, supply-demand balancing, speculation of the load patterns for the scheduling of the DERs, asset management and fault resilience [75].

However, AI itself has security and privacy issues which can be a potential instrument for launching intelligent attacks.

7.1. Key Challenges

1. **Data manipulation:** How can we mitigate manipulation of energy input data (electricity consumption and production data obtained through smart meters) and validate the authenticity of the information?
2. **ML:** How can we prevent the model inversion, poisoning pertaining to training and deployment of ML models, used for adaptive decision-making processes in automated generation allocation of EI grids [42]?
3. **Ethical data aggregation:** How can we ensure ethical use of aggregated energy production/consumption data for AI model training and prevent unauthorized data sharing with compliance to privacy preservation?
4. **Transparency:** How can we improve transparency in model development, training, testing and deployment, resulting in algorithms that are reliable for diverse applications with grid integration of heterogeneous energy sources?
5. **Automation:** How can we assure security in AI-based automation of network control and orchestration with it [42]?
6. **Trust management:** How can we establish trust among stakeholders participating in energy trading in EI grids and improve transparency in process automation through the deployment of AI models [76]?
7. **Accountability:** How do we ensure the accountability of the AI algorithms for automated decision-making processes responsible for generation coordination, distribution network management and fault recovery?

7.2. Role of Blockchain

Intelligent grids arrive at decisions based on the aggregated data set obtained through IoT devices and incorporation of AI and ML techniques [77]. The integrity of the data used in ML models and preventing data poisoning would be the key consideration, which directly impacts the decision-making process. With blockchain being an immutable DLT, this would ensure data integrity by preventing data manipulation, injection and corruption [70,78]. Privacy preserving of the large data sets can be achieved through distributed edge computing, facilitated by blockchain platforms where raw data will remain closer to its origin, assuring confidentiality [42].

Nevertheless, the authenticity of the algorithms generated through the incorporation of AI and ML cannot be verified through the blockchain platform. Security and privacy preservation in AI based systems, however, cannot be fully facilitated by blockchain platforms and, thus, will require AI-resilient measures. At the same time, this would affect the control decisions obtained for the stable and reliable operations of the decentralized architecture. Standardization and regulatory enforcement are required to overcome such issues arising in the envisaged electricity grids.

7.3. Future Directions

The advancements in big data and computing technologies have facilitated the emergence of DL techniques for pattern recognition from the aggregated information [79]. This would, thereby, enable accurate demand forecasting for optimal load scheduling and load balancing to reduce peak electricity demand, facilitate energy trading and sharing, state estimation of the power grid and perform grid diagnostics for the detection of energy theft. The higher precision achieved in the energy demand speculation would benefit in maximizing the utilization of DER to cater for the demand requirements while maintaining grid stability [80]. Further, fast blockchain-based data-feeding models need to be introduced to facilitate the development of efficient and accurate ML models.

Initiatives towards collaborative model development approaches using AI and ML techniques have given rise to Federated Learning (FL), in which individual data storage on a decentralized network is encouraged [81–83]. This facilitates predictive data analysis through training of a shared model using different data sets, offering capabilities of generalized model development with the benefit of privacy preservation of the user data. Blockchain facilitates trust establishment and prevents data poisoning, improving transparency in training, validation, testing, deployment and storage of training data sets for such shared models. Smart contracts enable the automation of iterative processes, improving the flexibility of model development and data analysis. However, challenges raised through the blockchain architecture relating scalability and smart contract security, need to be addressed further to expand the capabilities of FL techniques [83].

xAI (explainable AI) is gaining attention in the current context of AI integration with IoT for predictive data analysis. This could improve the transparency of the AI models associated with demand forecasting, evaluation of energy usage patterns, renewable energy modeling and automated grid operation with optimum generation allocation and load scheduling. xAI unravels the black box AI models, thereby improving transparency in predictive data analysis and establishing trust in the decisions arrived through such approaches [76,84].

Lessons: Grid intelligence would dominate the future autonomous and the challenges arising from AI-integrated smart grids are seldom addressed through the existing literature [70]. Improving transparency to ensure accountability of ML models [15,85] and trust management in the decisions arrived through the models [21,85] would be EI grid–specific challenges to be addressed in future research.

8. Discussion

The envisaged EI grids intend to integrate a diversity of distributed resources in order to achieve decentralized, autonomous operations. This facilitates consumer liberalization while enhancing reliability, stability through a secure and privacy-preserving platform. Blockchain is identified as an eminent factor driving the transformation from the hierarchical architecture towards an open market. Blockchain facilitates the realization of the intelligent grid architecture at the benefit of real-time operation with minimal involvement of an intermediary [86].

The paper discusses six directions of future EI architecture realization through the integration of blockchain platforms. Enhanced energy diversity catered with an improved security and privacy-preserving mechanism utilizes the inherent features of the blockchain-based architecture. Grid intelligence along with the EI data management, facilitate the near real-time decision making through predictive data analysis [77]. The ultimate goal of the blockchain integrated EI grids would be to ensure a reliable and stable power supply while maximizing consumer participation in electricity distribution [87]. Further, it is envisaged to achieve delegated authority with the distributed operation, which eliminates the threat of single-point failure.

The key challenges related to each direction discussed in the previous sections are summarized in Table 2. The applicability of inherent blockchain features to address these challenges is visually represented. The contribution of the existing work in addressing the key challenges identified for each driving trend has been categorised according to its level of impact. Among the identified challenges, establishment of a decentralized, P2P marketplace is a well established research area having many real-world implementations. Securing communication links, adversarial handling related to privacy, authentication, data manipulation and energy theft, attention given in establishing scalable grids having data integrity preserved are addressed through the existing work up to a reasonable extent. However, further developments are required to fully overcome the challenges present. Challenges which require significant research consideration include facilitating seamless grid integration for DERs enabled with low-latency grid synchronization, ensuring interoperability, power quality management with high penetration of DG, improving accuracy of intelligent decision making, efficient smart grid data management, accountability and trust management. AL and ML related attacks require attention in future grids in the way forward, facilitating predictive data analysis tools.

In addition, Table 3 summarizes the level of impact of each identified directions on broad applications of EI grids. Further, the benefits of integrating blockchains in each instance have been elaborated. Practical implementations and examples related to EI grid applications have been considered in this analysis, which verifies the benefits of blockchain integration in future energy grid realizations and signifies the way forward.

Table 2. Research direction for blockchain integrated EI grids [88].

Challenges	Blockchain Features						Related Work	
	Decentralization	Traceability	Immutability	Consensus Mechanism	Digital Currency	Smart Contracts	Citations	Contribution
Energy sustainability through heterogeneity								
Seamless grid integration	H	L	L	M	L	H	[12]	Low
Decentralized marketplace	H	H	H	M	H	H	[26,27,30–34]	Very High
Secure communication	M	H	H	L	L	L	[56,89]	High
Transient overvoltages and dynamics	L	L	L	M	L	H	[69,90]	High
Improving interoperability	L	L	L	H	L	H	[8,21]	Low
Improved trust, security and privacy								
Device tampering	L	H	H	L	L	L	[15,37,89,91]	Low
Man-in-the-Middle attacks	H	H	H	L	L	H	[89]	Medium
DDoS attacks in EI grids	H	H	L	L	L	H	[12,37,51]	Low
Privacy issues	H	H	H	M	L	H	[45,51–56]	High
Authentication	L	H	H	L	L	H	[45,52,55,62]	High
AI and ML related attacks	L	H	H	L	L	M	[15,16]	Very Low
Ultimate reliability and stability								
Supply-demand balancing	H	M	L	H	H	H	[12,56,73]	Medium
Intermittent generation	L	H	L	H	L	H	[26,92,93]	Medium
Secure communication	L	H	H	H	L	M	[12,37]	Low
Intelligent decision making	H	M	M	H	L	H	[12,15,73]	Low
Energy theft	L	H	H	H	L	M	[12,15,51,56,62]	High
Power quality management	L	H	H	M	H	H	[51]	Low
Decentralized scalability								
Scalable, decentralized EI grids	H	H	H	H	L	H	[21,32,66]	Medium
Low-latency grid synchronization	L	H	L	H	L	H	[4,8]	Low
Scalable data management	H	H	H	M	L	M	[12,65,67]	Low
Advanced big data management								
Data silos	H	H	H	L	L	M	[21]	Low
Secure communication	M	H	H	M	L	H	[21]	Medium
Secure data storage	H	H	H	M	L	L	[8]	Low
Data integrity protection	H	H	H	H	L	L	[52,62]	High
Data ownership	H	H	H	H	L	L	[94]	Low
Scalable grids	H	H	H	H	L	H	[74]	High
Grid intelligence								
Data manipulation	H	H	H	H	L	H	[51,89]	High
ML attacks	H	H	H	M	L	L	[70]	Very Low
Ethical data aggregation	H	H	H	H	L	L	[62]	High
Transparency	H	H	H	H	L	L	[15,85]	Low

Table 2. *Cont.*

Challenges	Blockchain Features						Related Work	
	Decentralization	Traceability	Immutability	Consensus Mechanism	Digital Currency	Smart Contracts	Citations	Contribution
Automation	H	H	H	H	H	H	[34,95]	Medium
Trust management	H	H	H	H	L	H	[21,85]	Low
Accountability	H	H	H	H	L	M	[21,85,95,96]	Low

H High impact M Medium impact L Low impact

Table 3. Benefits of blockchains in each EI application [4,9].

EI Application	Energy Sustainability through Heterogeneity	Improved Trust, Security and Privacy	Ultimate Reliability and Stability	Decentralized Scalability	Advanced Big Data Management	Grid Intelligence	Benefits Attained through Blockchain Integration	Practical Implementations/Examples
P2P energy trading	H	H	M	H	H	H	Reliable, low-latency communication links Less DSO intervention in trust establishment and supply-demand balancing	NRGcoin [32] Bankymoon [97] Pylon [8]
Plug-and-play interfacing of DER	H	H	H	H	H	H	Low-latency grid stability management Trusted, secure and privacy-preserving trading environment Automated certificate invocation and revocation for seamless integration	Greeneum [34] WePower [8] DAJIE blockchain platform [8] Iberdrola [13] Share & Charge [35] Juicenet [33]
Microgeneration	H	H	H	H	H	H	Autonomous supply-demand balancing for standalone operation Trustworthy, secure and privacy-assured P2P trading mechanism Maintaining stability and reliability with minimal DSO participation	Brooklyn microgrid [26] Powerledger [27]
Demand Side Integration (DSI)	L	H	L	L	H	H	Data silos preventing optimal load/generation scheduling Transparency in dynamic electricity pricing and incentive schemes	PETCON [12]
Distribution network automation and management	L	H	H	M	H	H	Asset management and optimal generation scheduling with less DSO participation Efficient and secure communication links to reduce system downtime during a fault Accurate fault diagnostics for automated protection schemes	PROSUME [91] PONTON [21]
Energy data management	M	H	H	H	H	H	Reliable, secure and privacy-assured data communication channels and storage options Authenticity of algorithms developed for data analysis	Enervalis, Jouliette, Energy Bazaar [21]

H High impact M Medium impact L Low impact

However, the attention received by these novel electricity grids has attracted more stakeholders where scalability becomes effective. Decentralized scalability is a requisite to cater to the demands of the distributed grid operation with minimal third-party involvement; hence trust establishment mechanism should be transparent. Existing blockchain platforms have not reached the level of maturity to cater to the extensive numbers of stakeholders integrating with the EI grid [64]. Secure and privacy-preserving techniques, which do not trade-off scalable blockchain solutions, need to be considered for future electricity distribution networks to attain maximum benefits. Decentralization, scalability and security/privacy trilogy should be equalized for successful grid transformation from conventional top-down hierarchical architecture to open electricity markets offering the benefit of consumer liberalization.

Further, blockchain specific security attacks which are identified during the operations should be eliminated for interruption-free power delivery. The distribute operation and increased consumer participation observed in the electricity trading would lead towards the development of a 51% authority of collective stakeholder contribution, thereby assume charge over the blockchain platform [98]. AI and ML integration in blockchain-based EI grids would trigger security threats related to massive data set [70].

The latency observed in consensus-based transaction verification incorporated in blockchains will create adverse impacts on the real-time operations of the envisaged EI networks [99]. Further, the limitations in the storage availability of the distributed ledger platform have to be managed to align with the increase of stakeholder integration with Smart Grid 2.0 [74].

Maintenance of blockchains to overcome such challenges related to extensive involvement of diversified stakeholders would require customized platforms, which is seldom discussed in the research literature. An energy grid-specific blockchain platform could better contribute towards efficient implementation of EI grids, ensuring the decentralization, security and scalability trilogy. Integration of big data management with AI and ML based predictive data analysis leads the way forward towards demand-operative, autonomous, real-time grid operations where trust establishment would be facilitated through a customized blockchain platform.

9. Conclusions and Future Research Directions

The paper analyzes six directions of blockchain utilization for facilitating the realization of the envisaged, intelligent, autonomous EI grids. Energy sustainability through heterogeneity, improved trust, security and privacy, ultimate reliability and stability, decentralized scalability, advanced big data management and grid intelligence are identified as these directives while challenges and the future research for maximizing the benefits of the envisaged architecture are elaborated with respect to each identified key direction.

The paper presents a clear insight of the successful integration of blockchain technologies with AI and ML based predictive analysis in future electricity networks to reshape the energy industry to fully-autonomous, self-resilient grids. xAI, federated ML and DL would enable trusted and transparent grid intelligence in future smart grids. AV era would be realizable through such intelligent smart grids. Beyond 5G communication architecture would facilitate the integration of edge intelligence for distributed processing thereby, offer scalable, efficient and responsive EI grids.

Blockchain offers great flexibility in providing security solutions through the inherent features. However, challenges have been identified in the areas of AI and ML integration, which would require alternatives beyond blockchain.

Author Contributions: Conceptualization, C.Y., C.d.A. and M.L.; methodology, C.Y.; formal analysis, C.Y., C.d.A. and M.L.; investigation, C.d.A.; writing—original draft preparation, C.Y.; writing—review and editing, C.d.A. and M.L.; visualization, C.Y.; supervision, C.d.A. and M.L.; project administration, C.d.A. and M.L.; funding acquisition, C.d.A. and M.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was jointly funded by the framework of 6Genesis Flagship (grant 318927) and the grant awarded by the University Grants Commission, Sri Lanka to develop a COVID-19 Self-Quarantine Monitoring and Tracking Platform.

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

Abbreviations

The following abbreviations are used in this manuscript:

5G	Fifth Generation
6G	Sixth Generation
AI	Artificial Intelligence
AV	Autonomous Vehicles
BC	Blockchain
CHP	Combined Heat and Power
DDoS	Distributed Denial of Service
DER	Distributed Energy Resources
DG	Distributed Generation
DL	Deep Learning
DLT	Distributed Ledger Technology
DNP	Distributed Network Protocol
DR	Demand Response
DSI	Demand Side Integration
DSO	Distribution System Operator
EI	Energy Internet
ESS	Energy Storage Systems
EMS	Energy Management System
EV	Electric Vehicles
FDI	False Data Injection
FL	Federated Learning
ICT	information and Communication Technology
IoT	Internet of Things
IP	Internet Protocol
IPFS	Inter Planetary File System
6LowPAN	IPv6 over Low power wireless Personal Area Network
ML	Machine Learning
PKI	Public Key Infrastructure
PV	Photovoltaic
P2P	Peer-to-Peer
RES	Renewable Energy Sources
TCP	Transmission Control Protocol
VPP	Virtual Power Plants
V2G	Vehicle-to-Grid
V2V	Vehicle-to-Vehicle
xAI	Explainable AI
ZSM	Zero-touch network Service Management

References

1. Perera, C.; Liu, C.H.; Jayawardena, S. The Emerging Internet of Things Marketplace from an Industrial Perspective: A Survey. *IEEE Trans. Emerg. Top. Comput.* **2015**, *3*, 585–598. [CrossRef]
2. Kabalci, E.; Kabalci, Y. Chapter 7—Internet of Things for Smart grid applications. In *From Smart Grid to Internet of Energy*; Kabalci, E., Kabalci, Y., Eds.; Academic Press: Cambridge, MA, USA, 2019; pp. 249–307.
3. Kabalci, E.; Kabalci, Y. Chapter 9—Roadmap from Smart Grid to Internet of Energy Concept. In *From Smart Grid to Internet of Energy*; Kabalci, E., Kabalci, Y., Eds.; Academic Press: Cambridge, MA, USA, 2019; pp. 335–349.
4. Miglani, A.; Kumar, N.; Chamola, V.; Zeadally, S. Blockchain for Internet of Energy Management: Review, Solutions, and Challenges. *Comput. Commun.* **2020**, *151*, 395–418. [CrossRef]
5. Shahinzadeh, H.; Moradi, J.; Gharehpetian, G.B.; Nafisi, H.; Abedi, M. Internet of Energy (IoE) in Smart Power Systems. In Proceedings of the 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), Tehran, Iran, 28 February–1 March 2019; pp. 627–636.

6. Wang, K.; Yu, J.; Yu, Y.; Qian, Y.; Zeng, D.; Guo, S.; Xiang, Y.; Wu, J. A Survey on Energy Internet: Architecture, Approach, and Emerging Technologies. *IEEE Syst. J.* **2017**, *12*, 2403–2416. [CrossRef]
7. Hussain, H.M.; Narayanan, A.; Nardelli, P.H.; Yang, Y. What is Energy Internet? Concepts, Technologies, and Future Directions. *IEEE Access* **2020**, *8*, 183127–183145. [CrossRef]
8. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.Y.; Zhang, X.; Ghias, A.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
9. Wu, J.; Tran, N.K. Application of Blockchain Technology in Sustainable Energy Systems: An Overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
10. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on Blockchain based Smart Contracts: Applications, Opportunities and Challenges. *J. Netw. Comput. Appl.* **2020**, *177*, 102857. [CrossRef]
11. Di Silvestre, M.L.; Gallo, P.; Guerrero, J.M.; Musca, R.; Sanseverino, E.R.; Sciumè, G.; Vásquez, J.C.; Zizzo, G. Blockchain for Power Systems: Current Trends and Future Applications. *Renew. Sustain. Energy Rev.* **2020**, *119*, 109585. [CrossRef]
12. Alladi, T.; Chamola, V.; Rodrigues, J.J.; Kozlov, S.A. Blockchain in Smart Grids: A Review on Different Use Cases. *Sensors* **2019**, *19*, 4862. [CrossRef]
13. Wang, Q.; Su, M. Integrating Blockchain Technology into the Energy Sector—From Theory of Blockchain to Research and Application of Energy Blockchain. *Comput. Sci. Rev.* **2020**, *37*, 100275. [CrossRef]
14. Cao, Y. 3—Energy Internet Blockchain Technology. In *The Energy Internet*; Su, W., Huang, A.Q., Eds.; Woodhead Publishing: Sawston, UK, 2019; pp. 45–64.
15. De Alwis, C.; Kalla, A.; Pham, Q.V.; Kumar, P.; Dev, K.; Hwang, W.J.; Liyanage, M. Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research. *IEEE Open J. Commun. Soc.* **2021**, *2*, 836–886. [CrossRef]
16. Hossain, E.; Khan, I.; Un-Noor, F.; 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**, *7*, 13960–13988. [CrossRef]
17. de Alwis, C.; Arachchi, H.K.; De Silva, V.; Fernando, A.; Kondoz, A. Robust Video Communication using Random Linear Network Coding with Pre-coding and Interleaving. In Proceedings of the 2012 19th IEEE International Conference on Image Processing, Orlando, FL, USA, 30 September–3 October 2012; pp. 2269–2272.
18. Rahman, M.A.; Hossain, M.S.; Loukas, G.; Hassanain, E.; Rahman, S.S.; Alhamid, M.F.; Guizani, M. Blockchain-based Mobile Edge Computing Framework for Secure Therapy Applications. *IEEE Access* **2018**, *6*, 72469–72478. [CrossRef]
19. de Alwis, C.; Arachchi, H.K.; Fernando, A.; Pourazad, M. Content and Network-aware Multicast over Wireless Networks. In Proceedings of the 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Rhodes, Greece, 18–20 August 2014; pp. 122–128.
20. Bhattacharya, P.; Tanwar, S.; Shah, R.; Ladha, A. Mobile Edge Computing-enabled Blockchain Framework—A Survey. In *Proceedings of ICRIC 2019*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 797–809.
21. 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]
22. Strielkowski, W.; Streimikiene, D.; Fomina, A.; Semenova, E. Internet of Energy (IoE) and High-Renewables Electricity System Market Design. *Energies* **2019**, *12*, 4790. [CrossRef]
23. Huang, A.Q.; Crow, M.L.; Heydt, G.T.; Zheng, J.P.; Dale, S.J. The Future Renewable Electric Energy Delivery and Management (FREEDM) System: The Energy Internet. *Proc. IEEE* **2010**, *99*, 133–148. [CrossRef]
24. Khorasany, M.; Dorri, A.; Razzaghi, R.; Jurdak, R. Lightweight Blockchain Framework for Location-aware Peer-to-Peer Energy Trading. *Int. J. Electr. Power Energy Syst.* **2021**, *127*, 106610. [CrossRef]
25. Kabalci, E.; Kabalci, Y. Chapter 1—Introduction to Smart Grid and Internet of Energy Systems. In *From Smart Grid to Internet of Energy*; Kabalci, E., Kabalci, Y., Eds.; Academic Press: Cambridge, MA, USA, 2019; pp. 1–62.
26. Mengelkamp, E.; Gärttner, J.; Rock, K.; Kessler, S.; Orsini, L.; Weinhardt, C. Designing Microgrid Energy Markets: A Case Study: The Brooklyn Microgrid. *Appl. Energy* **2018**, *210*, 870–880. [CrossRef]
27. Ledger, P. Power Ledger White Paper, 2018. Power Ledger Website. Available online: https://www.powerledger.io/company/power-ledger-whitepaper (accessed on 10 July 2021).
28. Wang, J.; Wang, Q.; Zhou, N.; Chi, Y. A Novel Electricity Transaction Mode of Microgrids based on Blockchain and Continuous Double Auction. *Energies* **2017**, *10*, 1971. [CrossRef]
29. Hewa, T.; Gur, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions. In Proceedings of the 2nd 6G Wireless Summit 2020: Gain Edge for the 6G Era (6G SUMMIT), Levi, Finland, 17–20 March 2020.
30. Wang, S.; Taha, A.F.; Wang, J.; Kvaternik, K.; Hahn, A. Energy Crowdsourcing and Peer-to-Peer Energy Trading in Blockchain-enabled Smart Grids. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1612–1623. [CrossRef]
31. Dang, C.; Zhang, J.; Kwong, C.P.; Li, L. Demand Side Load Management for Big Industrial Energy Users under Blockchain-based Peer-to-Peer Electricity Market. *IEEE Trans. Smart Grid* **2019**, *10*, 6426–6435. [CrossRef]
32. Mihaylov, M.; Jurado, S.; Avellana, N.; Van Moffaert, K.; de Abril, I.M.; Nowé, A. NRGcoin: Virtual Currency for Trading of Renewable Energy in Smart Grids. In Proceedings of the 11th International Conference on the European Energy Market (EEM14), Krakow, Poland, 28–30 May 2014; pp. 1–6.
33. JuiceNet. Available online: https://evcharging.enelx.com/products/juicenet-software/juicenet (accessed on 10 July 2021).

34. Greeneum. Available online: https://www.greeneum.net/ (accessed on 10 July 2021).
35. Share & Charge. Available online: https://shareandcharge.com/ (accessed on 9 July 2021).
36. Jouliette. Available online: https://www.jouliette.net/ (accessed on 8 July 2021).
37. Zhuang, P.; Zamir, T.; Liang, H. Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Trans. Ind. Inform.* **2020**, *17*, 3–19. [CrossRef]
38. Sabounchi, M.; Wei, J. Towards Resilient Networked Micrograids: Blockchain-enabled Peer-to-Peer Electricity Trading Mechanism. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017; pp. 1–5.
39. *Cryptography and Network Security: Principles and Practice*, 7th ed.; Stallings, W., Ed.; Pearson Education Limited: London, UK, 2017; p. 766.
40. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [CrossRef]
41. Shafi, Q.; Basit, A. DDoS Botnet Prevention using Blockchain in Software Defined Internet of Things. In Proceedings of the 2019 16th international Bhurban conference on applied sciences and technology (IBCAST), Islamabad, Pakistan, 8–12 January 2019; pp. 624–628.
42. Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Ylianttila, M. AI and 6G Security: Opportunities and Challenges. In Proceedings of the 2021 Joint European Conference on Networks and Communications (EuCNC) & 6G, Porto, Portugal, 8–11 June 2021.
43. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Ylianttila, M. 6G Security Challenges and Potential Solutions. In Proceedings of the 2021 Joint European Conference on Networks and Communications (EuCNC) & 6G, Porto, Portugal, 8–11 June 2021.
44. Ahl, A.; Yarime, M.; Goto, M.; Chopra, S.S.; Kumar, N.M.; Tanaka, K.; Sagawa, D. Exploring Blockchain for the Energy Transition: Opportunities and Challenges based on a Case Study in Japan. *Renew. Sustain. Energy Rev.* **2020**, *117*, 109488. [CrossRef]
45. 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]
46. Micciancio, D.; Regev, O. Lattice-based Cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 147–191.
47. Overbeck, R.; Sendrier, N. Code-based Cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 95–145.
48. Kiktenko, E.O.; Pozhar, N.O.; Anufriev, M.N.; Trushechkin, A.S.; Yunusov, R.R.; Kurochkin, Y.V.; Lvovsky, A.; Fedorov, A.K. Quantum-secured Blockchain. *Quantum Sci. Technol.* **2018**, *3*, 035004. [CrossRef]
49. Yu, Y.; Guo, Y.; Min, W.; Zeng, F. Trusted Transactions in Micro-grid based on Blockchain. *Energies* **2019**, *12*, 1952. [CrossRef]
50. Casino, F.; Dasaklis, T.K.; Patsakis, C. A Systematic Literature Review of Blockchain-based Applications: Current Status, Classification and Open Issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
51. 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]
52. 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.* **2016**, *15*, 840–852. [CrossRef]
53. Laszka, A.; Dubey, A.; Walker, M.; Schmidt, D. Providing Privacy, Safety, and Security in IoT-based Transactive Energy Systems using Distributed Ledgers. In Proceedings of the Seventh International Conference on the Internet of Things, Linz, Austria, 22–25 October 2017; pp. 1–8.
54. Kvaternik, K.; Laszka, A.; Walker, M.; Schmidt, D.; Sturm, M.; Dubey, A. Privacy-preserving Platform for Transactive Energy Systems. *arXiv* **2017**, arXiv:1709.09597.
55. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A Blockchain-based Smart Grid: Towards Sustainable Local Energy Markets. *Comput. Sci. Res. Dev.* **2018**, *33*, 207–214. [CrossRef]
56. Mwasilu, F.; Justo, J.J.; Kim, E.K.; Do, T.D.; Jung, J.W. Electric Vehicles and Smart Grid Interaction: A Review on Vehicle to Grid and Renewable Energy Sources Integration. *Renew. Sustain. Energy Rev.* **2014**, *34*, 501–516. [CrossRef]
57. Hussain, S.; Nadeem, F.; Aftab, M.A.; Ali, I.; Ustun, T.S. The Emerging Energy Internet: Architecture, Benefits, Challenges, and Future Prospects. *Electronics* **2019**, *8*, 1037. [CrossRef]
58. Noor, S.; Yang, W.; Guo, M.; van Dam, K.H.; Wang, X. Energy Demand Side Management within Micro-grid Networks enhanced by Blockchain. *Appl. Energy* **2018**, *228*, 1385–1398. [CrossRef]
59. Gao, J.; Asamoah, K.O.; Sifah, E.B.; Smahi, A.; Xia, Q.; Xia, H.; Zhang, X.; Dong, G. GridMonitoring: Secured Sovereign Blockchain based Monitoring on Smart Grid. *IEEE Access* **2018**, *6*, 9917–9925. [CrossRef]
60. Hewa, T.; Bracken, A.; Ylianttila, M.; Liyanage, M. Blockchain-based Automated Certificate Revocation for 5G IoT. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–7.
61. 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]
62. Guan, Z.; Si, G.; Zhang, X.; Wu, L.; Guizani, N.; Du, X.; Ma, Y. Privacy-preserving and Efficient Aggregation based on Blockchain for Power Grid Communications in Smart Communities. *IEEE Commun. Mag.* **2018**, *56*, 82–88. [CrossRef]
63. 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]

64. Malik, H.; Manzoor, A.; Ylianttila, M.; Liyanage, M. Performance Analysis of Blockchain based Smart Grids with Ethereum and Hyperledger Implementations. In Proceedings of the 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, 16–19 December 2019; pp. 1–5.
65. Dahlquist, O.; Hagström, L. Scaling Blockchain for the Energy Sector. Student Thesis, Uppsala University, Uppsala, Sweden, July 2017.
66. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. Available online: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (accessed on 10 July 2021).
67. Abdella, J.; Shuaib, K. Peer to Peer Distributed Energy Trading in Smart Grids: A Survey. *Energies* **2018**, *11*, 1560. [CrossRef]
68. Zolanvari, M.; Teixeira, M.A.; Gupta, L.; Khan, K.M.; Jain, R. Machine Learning-based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 6822–6834. [CrossRef]
69. Zhou, Z.; Wang, B.; Dong, M.; Ota, K. Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *50*, 43–57. [CrossRef]
70. Qiu, S.; Liu, Q.; Zhou, S.; Wu, C. Review of Artificial Intelligence Adversarial Attack and Defense Technologies. *Appl. Sci.* **2019**, *9*, 909. [CrossRef]
71. Manzoor, A.; Braeken, A.; Kanhere, S.S.; Ylianttila, M.; Liyanage, M. Proxy Re-encryption enabled Secure and Anonymous IoT Data Sharing Platform based on Blockchain. *J. Netw. Comput. Appl.* **2021**, *176*, 102917. [CrossRef]
72. Yrjölä, S. How could Blockchain Transform 6G towards Open Ecosystemic Business Models? In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 7–11 June 2020; pp. 1–6.
73. 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]
74. Pop, C.; Antal, M.; Cioara, T.; Anghel, I.; Sera, D.; Salomie, I.; Raveduto, G.; Ziu, D.; Croce, V.; Bertoncini, M. Blockchain-based Scalable and Tamper-evident Solution for Registering Energy Data. *Sensors* **2019**, *19*, 3033. [CrossRef]
75. Lotfi, M.; Monteiro, C.; Shafie-khah, M.; Catalão, J.P. Transition toward Blockchain-based Electricity Trading Markets. In *Blockchain-Based Smart Grids*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 43–59.
76. Arrieta, A.B.; Díaz-Rodríguez, N.; Del Ser, J.; Bennetot, A.; Tabik, S.; Barbado, A.; García, S.; Gil-López, S.; Molina, D.; Benjamins, R.; et al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Inf. Fusion* **2020**, *58*, 82–115. [CrossRef]
77. Fan, M.; Zhang, X. Consortium Blockchain based Data Aggregation and Regulation Mechanism for Smart Grid. *IEEE Access* **2019**, *7*, 35929–35940. [CrossRef]
78. Zhang, X.; Fan, M. Blockchain-based Secure Equipment Diagnosis Mechanism of Smart Grid. *IEEE Access* **2018**, *6*, 66165–66177. [CrossRef]
79. Antonopoulos, I.; Robu, V.; Couraud, B.; Kirli, D.; Norbu, S.; Kiprakis, A.; Flynn, D.; Elizondo-Gonzalez, S.; Wattam, S. Artificial Intelligence and Machine Learning Approaches to Energy Demand-Side Response: A Systematic Review. *Renew. Sustain. Energy Rev.* **2020**, *130*, 109899. [CrossRef]
80. Ferrag, M.A.; Maglaras, L. DeepCoin: A Novel Deep Learning and Blockchain-based Energy Exchange Framework for Smart Grids. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1285–1297. [CrossRef]
81. Feng, L.; Zhao, Y.; Guo, S.; Qiu, X.; Li, W.; Yu, P. Blockchain-based Asynchronous Federated Learning for Internet of Things. *IEEE Trans. Comput.* **2021**. [CrossRef]
82. Feng, L.; Yang, Z.; Guo, S.; Qiu, X.; Li, W.; Yu, P. Two-Layered Blockchain Architecture for Federated Learning over Mobile Edge Network. *IEEE Netw.* **2021**. [CrossRef]
83. Drungilas, V.; Vaičiukynas, E.; Jurgelaitis, M.; Butkienė, R.; Čeponienė, L. Towards Blockchain-Based Federated Machine Learning: Smart Contract for Model Inference. *Appl. Sci.* **2021**, *11*, 1010. [CrossRef]
84. Explainable AI—How Humans Can Trust AI. Available online: https://www.ericsson.com/en/reports-and-papers/white-papers/explainable-ai--how-humans-can-trust-ai (accessed on 23 June 2021)
85. Jiao, J. Application and Prospect of Artificial Intelligence in Smart Grid. In *IOP Conference Series: Earth and Environmental Science*; IOP Publishing: Bristol, UK, 2020; Volume 510, p. 022012.
86. Hewa, T.; Hu, Y.; Liyanage, M.; Kanhare, S.; Ylianttila, M. Survey on Blockchain based Smart Contracts: Technical Aspects and Future Research. *IEEE Access* **2021**, 87643–87662 [CrossRef]
87. Baggio, A.; Grimaccia, F. Blockchain as Key Enabling Technology for Future Electric Energy Exchange: A Vision. *IEEE Access* **2020**, *8*, 205250–205271. [CrossRef]
88. Hameed, B.; Khan, M.M.; Noman, A.; Ahmad, M.J.; Talib, M.R.; Ashfaq, F.; Usman, H.; Yousaf, M. A Review of Blockchain based Educational Projects. *Framework* **2019**, *28*, 30. [CrossRef]
89. Delmolino, K.; Arnett, M.; Kosba, A.; Miller, A.; Shi, E. Step by Step towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 79–94.
90. Münsing, E.; Mather, J.; Moura, S. Blockchains for Decentralized Optimization of Energy Resources in Microgrid Networks. In Proceedings of the 2017 IEEE Conference on Control Technology and Applications (CCTA), Maui, HI, USA, 27–30 August 2017; pp. 2164–2171.

91. Prosume Decentralising Power White Paper. 2017. Available online: https://fdocuments.net/document/white-paper-prosume-white-paper-the-future-is-prosumers-a-individual-consumers.html (accessed on 9 July 2021).
92. 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.* **2017**, *14*, 3690–3700. [CrossRef]
93. 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]
94. Manzoor, A.; Liyanage, M.; Braeke, A.; Kanhere, S.S.; Ylianttila, M. Blockchain based Proxy re-encryption Scheme for Secure IoT Data Sharing. In Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea, 14–17 May 2019; pp. 99–103.
95. Ahl, A.; Yarime, M.; Chopra, S.; Nallapaneni, M.K.; Tanaka, K.; Sagawa, D. Exploring blockchain and new ways forward in the energy sector: A case study in Japan. In Proceedings of the 2019 Applied Energy Symposium, Boston, MA, USA, 22–24 May 2019.
96. Hafeez, G.; Alimgeer, K.S.; Khan, I. Electric Load Forecasting based on Deep Learning and Optimized by Heuristic Algorithm in Smart Grid. *Appl. Energy* **2020**, *269*, 114915. [CrossRef]
97. Burger, C.; Kuhlmann, A.; Richard, P.; Weinmann, J. Blockchain in the Energy Transition. A Survey among Decision-makers in the German Energy Industry. *DENA Ger. Energy Agency* **2016**.
98. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
99. Hu, Y.; Manzoor, A.; Ekparinya, P.; Liyanage, M.; Thilakarathna, K.; Jourjon, G.; Seneviratne, A. A Delay-tolerant Payment Scheme based on the Ethereum Blockchain. *IEEE Access* **2019**, *7*, 33159–33172. [CrossRef]