energies

MDPI

Article

Blockchain-Based Microgrid for Safe and Reliable Power Generation and Distribution: A Case Study of Saudi Arabia

Mousa Mohammed Khubrani and Shadab Alam *

College of Computer Science & IT, Jazan University, Jazan 45142, Saudi Arabia; mmkhubrani@jazanu.edu.sa
* Correspondence: s4shadab@gmail.com

Abstract: Energy demand is increasing rapidly due to rapid growth and industrialization. It is becoming more and more complex to manage generation and distribution due to the diversification of energy sources to minimize carbon emissions. Smart grids manage reliable power generation and distribution efficiently and cater to a large geographical area and population, but their centralized structure makes them vulnerable. Cybersecurity threats have become a significant concern with these systems' increasing complexity and connectivity. Further transmission losses and its vulnerability to the single point of failure (SPOF) are also major concerns. Microgrids are becoming an alternative to large, centralized smart grids that can be managed locally with fewer user bases and are safe from SPOF. Microgrids cater to small geographical areas and populations that can be easily managed at the local level and utilized for different sources of energy, like renewable energy. A small group of consumers and producers are involved, but microgrids can also be connected with smart grids if required to exchange the excess energy. Still, these are also vulnerable to cybersecurity threats, as in the case of smart grids, and lack trust due to their decentralized nature without any trusted third party. Blockchain (BC) technology can address the trust and cybersecurity challenges in the energy sector. This article proposes a framework for implementing a BC-based microgrid system for managing all the aspects of a microgrid system, including peer-to-peer (P2P) energy trading, Renewable Energy Certificate (REC), and decentralized energy trading, that can be utilized in the case of Saudi Arabia. It can integrate cybersecurity standards and protocols, as well as the utilization of smart contracts, for more secure and reliable energy generation and distribution with transparency.

Keywords: smart grid; microgrid; energy distribution; blockchain; security

Citation: Khubrani, M.M.; Alam, S. Blockchain-Based Microgrid for Safe and Reliable Power Generation and Distribution: A Case Study of Saudi Arabia. *Energies* **2023**, *16*, 5963. https://doi.org/10.3390/en16165963

Academic Editors: Aniruddha Bhattacharjya and Shaohua Wan

Received: 9 July 2023
Revised: 4 August 2023
Accepted: 8 August 2023
Published: 12 August 2023

1. Introduction

The Kingdom of Saudi Arabia (KSA) is a leading oil producer and exporter, with a significant share of its economy and energy sector based on the traditional fossil fuel industry. However, as energy demand continues to grow, there is an urgent need to diversify the sources to improve efficiency and cut carbon emissions. There are various factors, like technological advancements, industrialization, transportation, and the development of smart homes and cities. Energy consumption in Saudi Arabia increased by 33% from 2015 to 2021 [1], and further, it increased at the rate of 4.23% during 2021, as suggested by the General Authority for Statistics (GASTAT) [2]. If these trends continue, an increase of around 45–50% is highly likely due to increasing population and industrial growth. The energy sector produces around 82% of carbon dioxide (CO_2) emissions [3] due to its dependence on fossil fuels for energy. More energy requirements will further increase carbon emissions. There are alternative natural energy resources like solar and wind energy that are abundant and can be used easily in the case of the kingdom. The Kingdom's Vision 2030 has highlighted the ambitious plan to produce 50% of its electrical energy requirements from renewable sources and very actively working to achieve the target [4]. In it, the role of renewable energy has been highlighted, and great emphasis has been given to it. The Ministry of Energy in Saudi Arabia is running a National Renewable

Energy Program (NREP) that is working toward implementing renewable infrastructure development and implementation to slowly lessen the dependency on fossil fuels to fulfill power requirements.

The concept of a community energy system, or micro-grid, is evolving quickly and depends on localized energy generation and distribution [5]. Two aspects are very important and favorable in the case of KSA. The population density is low, and normally, the villages are located far away from each other, so delivery is also a difficult task and costly if we consider centralized renewable energy infrastructure development [6]. Secondly, if the local community is involved, it will fulfill the kingdom's vision and improve the lifestyle of citizens far away from cities.

Microgrid technology can address the issues faced by the energy sector [7]. Microgrid is an independent and decentralized power management system that can operate in parallel with the smart grid (SG) and provide several benefits, such as improved energy efficiency, cost savings, and grid resilience [8]. Various aspects of apprehension and concern in a microgrid or decentralized energy distribution system are reliability of records, predicting and managing the demand, consumption data monitoring, and secure billing to increase trust [9]. Also, the adoption of renewable energy sources is hindered by various challenges, including legal and regulatory barriers, a lack of infrastructure, and technical challenges related to integrating renewable energy sources into the energy grid [10]. Additionally, the energy sector faces grid stability and reliability challenges, as the centralized grid system is vulnerable to cyberattacks and lacks transparency in transactions. Decentralized energy management and secure data transactions have emerged as promising solutions for enhancing the efficiency, reliability, and sustainability of the energy sector [11].

BC technology and smart contracts can manage all these aspects efficiently. In recent years, BC technology has emerged as a formidable technology where the security and reliability of records, immutability, reliable information exchange, and minimization of personal record sharing are required [12]. BC supports a distributed, decentralized system with increased security, immutability, trust, and faster transaction settlement speed. BC can provide a tamper-resistant ledger to support optimal energy management [13]. It has several potential use cases, such as P2P energy trading and optimizing grid operations [14]. With BC, microgrids can be designed to support reliable, secure, and transparent transactions between different stakeholders in the energy system. Furthermore, BC technology can create a secure and decentralized platform for managing and authenticating identities and access controls, helping to prevent unauthorized access or manipulation of critical infrastructure. By providing a secure, decentralized platform for managing and verifying transactions, BC technology has the potential to enhance the security and reliability of energy systems and support the evolution to a more sustainable and robust energy future.

This paper aims to analyze the applicability of BC technology in the microgrid field, also called the community grid, to promote renewable energy and localization of energy generation and distribution. It will help improve the living standards of citizens, provide great scope for entrepreneurship and economic development in the region, and promote healthy and reliable renewable energy in the KSA. It makes a comparative literature analysis of microgrids and BC applications in different countries and identifies potential applications for microgrids and BC in KSA's energy sector, such as integrating renewable energy sources with more efficiency and enhancing grid stability and resilience. Various articles have analyzed the blockchain applications in smart grid but lack several parameters like detailed security analysis and issues in the context of Saudi Arabia. Further, these articles have not considered the concept of microgrid in detail and mainly discussed the aspect of smart grid implementation. The article also discusses the challenges in the adoption of microgrid and BC technologies in KSA's energy sector and proposes a framework for microgrids based on BC applications that can counter security issues and enable the integration of renewable energy. Abbreviations presents the abbreviations and definitions used in the paper.

Further, the article has been organized as follows. Section 2 defines the methodology section that discusses the aspect of related work search, and Section 3 briefly discusses the

identified related works and their analysis. Section 4 reviews the role of smart grids and microgrids in energy management, the challenges of microgrid implementation in Saudi Arabia, and the security challenges. Section 5 provides the details of blockchain application in microgrid and finally present a blockchain-based framework for an energy microgrid in Saudi Arabia. Section 7 briefly summarizes research challenges and aspects of future research, and Section 8 concludes the article.

2. Methodology

This study examines the advantages of utilizing BC and microgrids for safe and sustainable power generation and distribution. Although it is not a systematic literature review, the article followed a structure researcher widely use to address a specific research question, issue, or problem to identify and analyze the related works. The following are important steps conducted during the related work review:

- Identification of problem:
  - Recognize research questions;
- Screening of research article:
  - Identification of related articles
- Inclusion/exclusion based on title and abstract:
  - Removal of duplicate article.

2.1. Recognize the Research Question

The following research questions were drafted for this study:

- How might BC technology help incorporate renewable energy sources into microgrids?
- What are the main potential cybersecurity threats and challenges in microgrids?
- What are the cybersecurity standards and protocols in microgrids?
- Difficulties of implementing BC in SG and applications
- How can BC be integrated into the microgrid framework to guarantee an efficient, reliable, and secure microgrid distribution system that can efficiently predict and manage demand, record consumption data and trust, and make secure billing?

2.2. Identification of Related Articles

An initial step in the research process consisted of using a keyword strategy to search for publications that were relevant to the topic. While looking for research articles, the terms 'BC,' 'smart grid, 'power generation', 'safe power distribution', 'safe power generation', BC, and smart grid' are the keywords that are searched for. It was decided to comprehensively search academic databases, including IEEE, ACM, and Scopus.

2.3. Inclusion/Exclusion Criteria

After determining the questions that needed to be asked about the scope of the research, all of the research articles were reviewed in their entirety so that the essential information could be extracted for the systematic review of this research. Based on a set of criteria for both its inclusion and exclusion in the study, the piece was chosen to be analyzed alongside other works of literature that are considered to be of the utmost significance (see Table 1). The title and abstract of each research paper were examined for the very first time at the beginning of the process. The articles that did not fulfill one or more of the criteria for exclusion were not included in the compilation. Papers were included that reflect "BC and smart grid for safe power generation," "safe and reliable power generation," "BC and smart grid for power generation," "power generation and distribution using BC and smart grid," and "smart grid for power generation and distribution." These phrases all refer to the same thing.

Table 1. Inclusion and Exclusion Criteria.

Selection Criteria	Details
Exclusion	• Articles other than the English language • The title and abstract are not in the scope of the paper • Duplication
Inclusion	• Title and abstract related to BC and smart-grid or microgrid for power generation • Published between 2018 and 2023

Removal of Duplicate Articles

While collecting data, duplicate items are deleted to make the resulting data more accurate. To prevent the duplication and merging of articles is imported into the Mendeley program. This action ultimately results in the elimination of 83 items from the collection.

3. Related Works

This section presents the related work conducted in the domain of this research. Mengelkamp et al. introduce a comprehensive concept and market design for a local energy market where users can directly trade renewable energy inside their community. The market utilizes a private BC to facilitate decentralized trading without intermediaries. It further provides a simulation of the model [15]. Alladi et al. review BC applications in smart grids. It discusses different use cases, BC architecture, block structure, and technologies used. A summary of application areas and technical details is included. Commercial implementations and challenges for integrating BC into smart grids are discussed, along with future research directions [16].

Yahaya et al. present a BC-based system that enables direct P2P energy trading. It incorporates a demurrage mechanism to optimize consumption, minimize price, and incentivize load shifting. Simulation results show significant reductions in electricity costs, and a security analysis ensures the integrity of the energy trading smart contract [17]. A unified BC-based power distribution platform that integrates a bilateral trading mechanism and optimizes energy flows in a microgrid is suggested by Van Leeuwen et al. By constructing an optimal power flow (OPF) issue and combining it with the trading mechanism in a single optimization problem, the platform respects the physical restrictions of the microgrid [18].

Zia et al. summarize recent talks on topologies, distributed ledger technologies, and local energy markets in the context of microgrid transactive energy systems and decentralized power systems. Decentralized transactive energy system topologies and the benefits of decentralized systems over centralized ones are examined. A seven-layer architecture is proposed, and its comparison with the Brooklyn microgrid case study is presented [19]. A secured energy market architecture built on a P2P idea and BC technology is introduced by Kavousi-Fard et al. The suggested model uses a relaxed consensus-innovation (RCI) algorithm for power and price exchange and includes both a microgrid and a smart grid as market players. The communication interfaces are protected from malicious attacks, and uncertainty effects are handled via a stochastic architecture based on the unscented transform (UT). The fault-tolerant system's ability to withstand cyberattacks is assessed using the fault data injection attack (FDIA) model [20].

Du et al. examine the integration of BC technology in the smart grid and its implications for establishing a sustainable supply chain. The authors propose a layered theoretical framework that considers relevant attributes, criteria, and stakeholder relationships to achieve this. They employ a combination of fuzzy-DEMATEL (Decision Making Trial and Evaluation Laboratory) and ISM (Interpretive Structural Modeling) methodologies to analyze and evaluate the sustainable supply chain development system across the entire smart grid value chain under BC technology [21]. The study by Tsao and Thanh focuses on the difficulty of balancing power supply and demand in microgrids with distributed renewable generation units. It suggests using BC technology for peer-to-peer energy trading within

the microgrid, providing members with security and sustainability. The study formulates a sustainable microgrid design problem that considers power flow, renewable generation unit decisions, P2P trading prices, and social constraints to maximize consumer demand satisfaction while balancing economic and environmental objectives [22].

In the context of the developing energy internet, this paper investigates the relationship between British Columbia and the power market. A BC trading framework has been developed to promote multi-agent collaboration and sharing in the energy market. The study models the nodes in market transactions using power system modeling and transaction consensus techniques. A multi-agent collaboration and sharing platform built on the Ethereum private BC is used to demonstrate a sample transaction [23]. The decentralized microgrid model used by Tsao and Vu focuses on the adoption of BC and smart contract technologies by a power distribution company (DC) and an electricity prosumer. Using an evaluation approach, the research assesses the cost-benefit analysis of integrating these technologies for both participants. The study emphasizes the benefits of implementing BC and smart contract technology in microgrid systems [24].

Younes et al. explore the application of BC technology in microgrids to improve the efficiency and sustainability of renewable energy systems. It discusses how BC can ensure secure and transparent transactions, record power generation, and facilitate smart contracts for auditing and dispute resolution. The focus is on enhancing the resilience of microgrids through the use of BC and smart contracts [25]. Agung and Handayani suggest the application of BC technology to control transactions in the smart grid. Using smart contracts for execution, the BC network serves as a transaction verifier. The immutability of the BC ensures secure and reliable transaction execution between generators and consumers. Additionally, the transaction history stored on the BC can be used to audit and resolve disputes. The paper introduces an architecture where all entities in the smart grid participate as nodes, with transactions recorded in smart contracts. A mobile application helps users interact with the system [26].

Wu et al. investigate the combined role of microgrids and BC technology in promoting sustainable energy solutions and establishing a green networking ecosystem. It evaluates microgrids' control, communication, and service aspects and explores their potential for coordinating decentralized energy units and integrating with the main grid. The study also examines the role of BC in facilitating decentralized communication enabling cross-border interaction of microgrids and communities. This comprehensive study provides insights into leveraging microgrids and BC for sustainable energy supply chains and offers a foundation for further research and innovation in the field [7]. Dinesha and Balachandra study the broader aspects of inter-microgrid transactions and interoperable communication between microgrids and smart grids but provide a general framework without providing implementation details. Further, it reviews the interoperability and communication between BC-based smart grids and microgrids and their interconnection and energy exchange [27].

Yang et al. demonstrate BC technology's effectiveness in securing energy transactions in microgrids. It proposes a smart contract and PoA-based BC to ensure the microgrid system's security and improve the benefit for the consumers. It highlights the potential of BC technology in securing control systems and optimizing energy trading in microgrids [28]. Meng et al. highlight the importance of BC technology in enabling decentralized transactions in smart grids and its potential for handling various aspects of energy management, including transmission, distribution, consumption, and microgrid management, and interaction with electric vehicles. It provides an overview of BC technology, surveys its applications in the energy sector, and presents the achievements and limitations of BC-based energy transactions [29].

A new BC-based algorithm for P2P energy trading in the Smart Grid is presented by Shukla et al. By offering a reliable and low-latency communication network for energy trading, it tackles the drawbacks of conventional methods, such as network delay. When implemented and assessed with various tools, the proposed algorithm showed secure

trading and decreased network latency [30]. Singh et al. highlighted the Internet of Things (IoT), Artificial Intelligence (AI), and BC as key elements of Industry 4.0 technologies revolutionizing the energy sector. It discusses how they are incorporated into several facets of the energy system, like smart grids, microgrids, electrical devices, and energy markets. The advantages of real-time monitoring, intelligence, and predictive analytics made possible by these technologies are emphasized in the essay.

Additionally, it offers suggestions for applying these technologies, such as the utilization of digital twins and Metaverse, to the energy industry [31]. The difficulties with security and privacy that come with data gathering and energy trading on open networks within smart grids are highlighted by Cao et al. Because BC technology is decentralized, irreversible, and traceable, it is suggested as a remedy for the security, integration, and coordination problems associated with conventional centralized networks. It intends to present and evaluate several BC-based solutions that might improve identity identification, data aggregation, privacy protection, and electricity pricing in smart grids. Additionally, it covers the field's existing difficulties and potential future research directions [32].

This paper provides an overview ofP2P energy trading in the smart grid domain. It discusses the structure and architecture of P2P energy trading, highlighting the role of smart agents and stakeholders involved in the trading process. The paper [33] analyzes various development techniques for P2P energy trading systems and also provides an overview of actual P2P pilot programs. The difficulties and legal issues that must be considered for P2P energy trading to be implemented successfully are underlined. Waseem et al. concentrate particularly on the use of BC in the SG domain. It provides a framework for SG applications leveraging BC technology, covering things like improved metering infrastructure, microgrids, home automation, and electric vehicles. The article explores the privacy and security vulnerabilities that smart grids face in more detail and suggests solutions to reduce these dangers [34]. Table 2 provides a summary of recent related works and their findings.

Table 2. Review of Related Works.

Ref	Year	Theme of the Paper	Technologies and Schemes Used	The Outcome of the Study
[15]	2018	Direct trade of renewable energy within the community without any third party.	Private BC	There is no government or other organization that regulates the market. The market is completely decentralized; direct trading of renewable energy within the community is supported.
[16]	2019	Review of BC implementations and issues in smart grid.	No implementation was provided.	Reviews BC implementations in smart grids with technical details. Further discusses issues and research challenges for BC-based smart grids are discussed.
[17]	2020	Minimizing the billing in local decentralized P2P energy consumption	Private BC with Proof of Work (PoW) Mechanism, Critical Peak Price (CPP), and Real-Time Price (RTP) schemes	Achieving optimal levels of energy use while simultaneously reducing overall power expenses with BC.
[18]	2020	Optimizes energy flows in a microgrid and bilateral trading mechanism	Private BC, Smart Contract	Energy flow optimization and import cost reduction are two key benefits of the proposed methodology.
[19]	2020	BC-based distributed energy transaction system	BC, Smart Contract	Proposes a seven-layer architecture for the microgrid's BC-based distributed energy transaction system.
[20]	2021	secured P2P energy transactions within a microgrid and a smart grid	Relaxed Consensus-Innovation (RCI), BC	It incorporates a microgrid and a smart grid utilizing a Relaxed Consensus-Innovation (RCI) algorithm for power, price exchange, and security against malicious attacks.

Table 2. *Cont.*

Ref	Year	Theme of the Paper	Technologies and Schemes Used	The Outcome of the Study
[21]	2021	Supply chain management and sustainable development in Smart grid	ISM and fuzzy decision-making, BC	Examines the integration of BC technology in the smart grid and its implications for establishing a sustainable supply chain. To achieve this, the authors propose a layered theoretical framework.
[22]	2021	P2P energy trading in the microgrid	fuzzy multi-objective programming model, genetic algorithm, BC	Encourage P2P energy trading without any centralized authority
[23]	2021	P2P energy transactions and security of transactions	Multi-agent system, Private BC, smart contract	Reviews the role of BC in a distributed trading platform and propose a framework for transparent transactional activities
[24]	2021	Profit maximization in microgrid	BC and Smart contract based framework	It reviews the role of BC and smart contract technology in microgrid systems for maximizing profits for the prosumer.
[25]	2021	Review the research on BC application in microgrids and the reliability of transactions	Review article	It explores the application of BC in microgrids for the efficiency and sustainability of renewable energy systems.
[26]	2022	Transaction management	Smart contract	Proposes a BC framework to record and manage transactions in a smart grid with smart contracts.
[7]	2022	Microgrid and smart grid integration	Identity Management, BC	It examines the role of BC in facilitating decentralized communication, enabling cross-border networking, and supporting the incorporation of microgrids and energy communities.
[27]	2022	Interoperability and communication between BC-based smart grids	Framework without implementation	It discusses the broader aspects of inter-microgrid transactions and interoperable communication between microgrids and smart grids but provides a general framework without implementation details.
[28]	2022	Security of the distributed control systems and energy trading in microgrids	Proof-of-Authority (PoA) BC, Smart contract	It discusses the role of BC in securing microgrid systems and how to maximize the benefits for the users.
[29]	2022	Review of BC-based P2P energy trading	Review article	Highlights the importance of BC technology in enabling decentralized transactions in smart grids
[30]	2022	P2P Energy Trading	Fog Computing, IoT, BC	Proposes a novel algorithm for P2P energy trading in the Smart Grid.
[31]	2022	Review the role of Industry 4.0 enabling technologies in Smart grids and energy distribution.	Review article focusing on Machine learning (ML), BC, and IoT in the Energy sector.	Highlights the role of Industry 4.0 technologies in transforming the energy system, focusing on IoT, AI, and BC
[32]	2023	Review of different BC-enabled technologies for managing security and transaction of smart grids.	Review article	Compare different BC-based technologies that can enhance security and adjust electricity pricing in smart grids.

Table 2. *Cont.*

Ref	Year	Theme of the Paper	Technologies and Schemes Used	The Outcome of the Study
[33]	2023	P2P energy trading	Game Theory, BC, smart contracts	The paper reviews different methodologies used to develop P2P energy exchange frameworks.
[34]	2023	Review of different domains of applications	Review article	It discusses the various domains of smart grid applications and the role of BC. Further, it highlights the security concerns for each use case and solution.
Our Study	2023	Overall aspects of Microgrid transaction, security, and its integration with Smart Grid	Provide a detailed framework and algorithm for implementation	Provide step-by-step transaction processing algorithms and interconnection of different entities and all possible aspects of microgrid working like P2P transaction, billing, Identity and access management, and renewable energy tracking.

Overall, the articles reviewed show that BC technology has enormous potential for the energy sector, particularly in microgrid and smart grid applications. Many of the articles provide case studies and propose new systems that leverage BC technology to enhance energy efficiency, reduce costs, and increase renewable energy integration. However, the limitations of existing works in comparison to other works are mostly focused on the lack of real-world testing, the limited analysis of technical challenges, and a need for more comprehensive cybersecurity and privacy protocols. Additionally, there is a need for further research on the integration of BC technology with other energy management technologies to provide more comprehensive solutions. The research articles related to BC and smart grids for safe and reliable power generation and distribution provide valuable insights into the applications, benefits, and challenges of using BC technology in the energy sector. However, several limitations exist in the current research. First, most of the studies are based on theoretical models and simulations, and there are limited real-world implementations. Second, the studies primarily focus on microgrid applications, and there is a lack of research on how BC can be integrated into larger-scale smart grid systems. Third, some studies do not consider specific countries' legal and regulatory frameworks, which may vary significantly and can impact the implementation of BC-based solutions. Fourth, there is a need for more research on the interoperability of different BC platforms and protocols. Fifth, most of the studies do not provide a detailed analysis of the cybersecurity risks associated with the adoption of BC in energy systems. Sixth, the energy industry is highly regulated, and there is a need to comply with existing standards and protocols. Seventh, the scalability of BC-based solutions remains a challenge, and there is a need for more research on how to improve the scalability of these solutions.

4. Smart Grid, Microgrid, and Energy Management

Smart grids are advanced electricity networks that use digital communications technology to monitor and manage the flow of electricity in real-time. Microgrids are small-scale power grids that can operate independently or in conjunction with the main grid. energy management involves optimizing the use of energy resources to reduce waste and improve efficiency. By integrating these technologies and practices, we can create a more sustainable and resilient energy system that meets the needs of communities and businesses while minimizing environmental impact [35]. This section further reviews these interrelated concepts and their roles and challenges in energy management.

4.1. Smart Grid

A smart grid is an advanced electricity grid that uses digital communication technologies and advanced sensors to enable real-time monitoring and control of energy generation and consumption [36]. Smart grids can enable more efficient and optimized energy management, reduce energy losses, and enhance grid resilience [37]. Smart grids can offer

several advantages over traditional, centralized energy grids. For example, they can enable real-time monitoring and control of energy generation and consumption, enabling more efficient and optimized energy management. They can also reduce energy losses by enabling more efficient energy distribution and storage. Additionally, smart grids can enhance grid resilience by providing backup power during outages or emergencies [38].

Smart grid technologies include advanced sensors, smart meters, energy storage systems, and IoT devices. These technologies can enable real-time monitoring and control of energy systems, enabling more efficient and optimized energy management. Smart grid technologies can also enable more efficient energy distribution and storage, reducing energy losses and enhancing grid resilience [39]. Figure 1 provides a general structure of the smart grid framework.

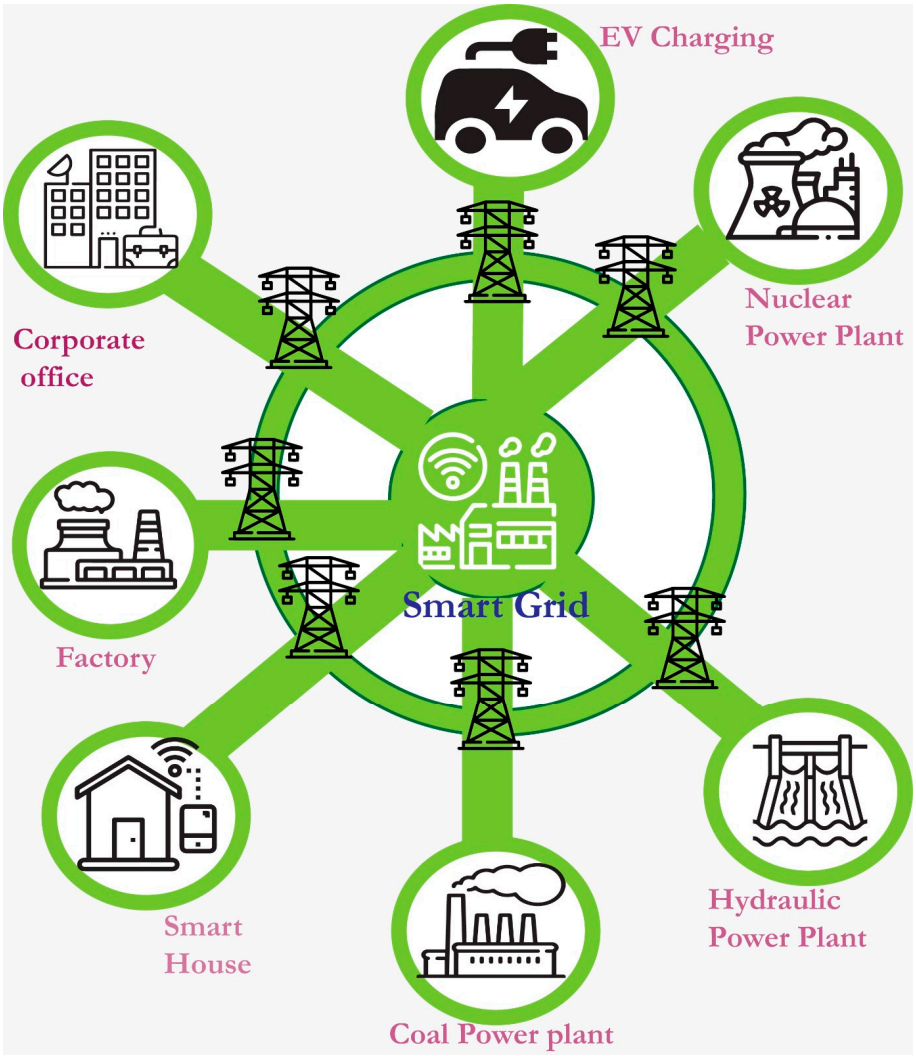

Figure 1. General structure of smart grid framework.

4.2. Microgrid

Microgrids can run independently or concurrently with the main grid in a decentralized manner. They provide enhanced energy efficiency, cost savings, and grid resilience, among other advantages. Different energy sources, including conventional fossil fuels, renewable energy, and energy storage devices, can power microgrids. Microgrids can also be tailored to satisfy particular energy requirements, such as those of distant or industrial locations. [40].

Microgrids can offer several advantages over traditional, centralized energy grids. For example, they can improve energy efficiency by minimizing losses during transmission and distribution. They can also reduce energy costs by enabling local energy generation and consumption, reducing reliance on expensive centralized power plants [41].

However, microgrids also face interoperability, data management, and regulatory challenges. To enable seamless energy management, microgrids must integrate with the existing energy grid and other microgrids, which requires interoperability standards and protocols. Data management is also important, as microgrids produce a lot of data that must be safely and effectively managed [42]. Additionally, microgrid regulations are still evolving, and clear regulations are needed to promote investment and innovation in the sector.

Smart grids and microgrids are two distinct approaches to electricity distribution that differ in several important ways. Smart grids are large-scale, centralized systems that use advanced digital technologies to optimize the flow of electricity across the grid. They incorporate sensors, meters, and other monitoring devices to collect real-time data on energy demand, generation, and transmission, which is used to make decisions about allocating resources and managing power flows [35]. In contrast, microgrids are smaller, decentralized systems that operate independently of the main grid. They can be used to provide power to specific locations, such as remote communities or military bases, and often incorporate renewable energy sources like solar or wind power. Unlike smart grids, which are designed to optimize the performance of the entire grid, microgrids are focused on providing reliable and sustainable power to specific localities, even in the event of disruptions to the main grid.

4.3. Microgrid and Energy Management

Microgrids can be customized to meet specific energy needs, such as those of industrial or remote areas. Additionally, microgrids can be powered by various energy sources [43]. Microgrids improve energy efficiency by minimizing energy losses during transmission and distribution. Microgrids can also reduce energy costs by enabling local energy generation and consumption, reducing reliance on expensive centralized power plants. Different technologies, including energy storage systems, smart grid technologies, and IoT devices, can support energy management in microgrids. Energy storage systems provide more effective energy management by storing extra energy produced by renewable energy sources and releasing it during times of high demand. Real-time monitoring and control of energy production and consumption are made possible by smart grid technology, enabling improved and more effective energy management. IoT gadgets can allow for remote control and monitoring of energy systems, allowing for more effective energy management and upkeep [44].

However, energy management in microgrids also faces interoperability, data management, and regulation challenges. To enable seamless energy management, microgrids must integrate with the existing energy grid and other microgrids, which requires interoperability standards and protocols. Data management is also important, as microgrids generate a large amount of data that needs to be managed securely and efficiently. Additionally, microgrid regulations are still evolving, and clear regulations are needed to promote investment and innovation in the sector.

4.4. Benefits of Microgrid for Energy Management

Microgrids offer several benefits for energy management, including improved energy efficiency, cost savings, and grid resilience. Microgrids can be modified to fulfill particular energy requirements, such as those of distant or industrial areas [45].

4.4.1. Improved Energy Efficiency

It improves energy efficiency by minimizing energy losses during transmission and distribution. Microgrids can generate and use energy locally, reducing inefficient long-distance transmission and distribution that result in energy losses.

4.4.2. Cost Savings

Microgrids can also offer cost savings by enabling local energy generation and consumption and reducing reliance on expensive centralized power plants. Additionally, microgrids can use a combination of energy sources, such as traditional fossil fuels and renewable energy, as per availability for cost reduction and efficiency.

4.4.3. Grid Resilience

Microgrids are designed to run autonomously or in parallel with the main grid, reducing reliance on the main grid and supporting overall grid resilience.

4.4.4. Customized Energy Solutions

Microgrids can be customized to meet specific energy needs, such as those of industrial or remote areas. This customization can enable more efficient energy management and cost savings by using the most appropriate energy sources for specific energy needs.

4.5. Challenges to Microgrid Implementation in Saudi Arabia

Various challenges hinder the adoption of microgrid and BC technologies in KSA's energy sector. Legal and regulatory challenges include the lack of clear regulations for microgrids and BC, which can create uncertainty and hinder investment in these technologies. Additionally, adopting new technologies can be slow due to public perception and adoption, as consumers may be hesitant to adopt new technologies due to a lack of awareness or understanding [46].

Technical challenges also hinder the adoption of microgrid and BC technologies. As KSA has a centralized grid system, implementing microgrids requires significant investment and technical expertise, which may limit the adoption of this technology. Additionally, interoperability is a challenge for microgrids, as they need to integrate with the existing energy grid and other microgrids to enable seamless energy management.

Data security is also challenging for microgrid and BC technologies, requiring secure and reliable data transactions to ensure the system's integrity. The vulnerability of traditional centralized energy grids to cyberattacks has been a concern in KSA, and adopting decentralized energy management systems can increase the need for secure data transactions.

In conclusion, the adoption of microgrid and BC technologies in KSA's energy sector faces legal and regulatory barriers, public perception and adoption challenges, technical challenges related to interoperability and data security, and challenges related to integrating renewable energy sources into the grid. Addressing these challenges will require a coordinated effort between stakeholders, including the government, energy companies, and technology providers, to promote investment, innovation, and collaboration in the sector.

The implementation of microgrid technology in KSA faces various challenges related to technical, economic, and regulatory issues. These challenges include:

4.5.1. Lack of Technical Expertise

Implementing microgrid technology requires significant investment and technical expertise. KSA's current power grid is centralized, which means that the development of microgrid technology requires a significant change in the power generation and distribution infrastructure. This lack of expertise and infrastructure can limit the adoption of microgrid technology in KSA.

4.5.2. Interoperability Issues

Interoperability is a significant challenge for microgrid technology, as microgrids need to be able to integrate with the existing energy grid and other microgrids. Interoperability standards and protocols are needed to ensure seamless energy management and integration.

4.5.3. Cost and Economic Feasibility

The cost of microgrid technology can be high, and its economic feasibility needs to be evaluated. Microgrid technology costs depend on various factors, such as energy sources, energy storage systems, and control systems. The economic feasibility of microgrid technology needs to be evaluated for each specific application, considering the local energy market, energy prices, and the potential for revenue generation.

4.5.4. Regulatory Barriers

The adoption of microgrid technology can be hindered by regulatory barriers, including licensing, permitting, and regulatory requirements. Clear regulations and policies are needed to promote investment and innovation in the microgrid sector.

4.5.5. Public Perception and Adoption

Adopting new technologies can be slow due to public perception and adoption. Consumers may hesitate to adopt new technologies due to insufficient awareness or understanding.

4.5.6. Harsh Environmental Conditions

Saudi Arabia experiences extreme temperatures, sandstorms, and other harsh environmental conditions that can affect the performance and efficiency of smart grids and, mainly, transmission lines.

4.5.7. Long Distance between Inhabited Locations

Saudi Arabia is sparsely populated, and long gaps between two villages or cities cause the transmission line to be transmitted for a long time, which may result in transmission loss. Maintaining them in harsh weather is also tricky. It will also result in a revenue loss.

4.5.8. Cybersecurity Concerns

Adopting decentralized energy management systems, including microgrid technology, can increase the need for secure data transactions. The vulnerability of traditional centralized energy grids to cyberattacks has been a concern in KSA, and adopting microgrid technology can increase this vulnerability [47].

Smart microgrids collect, transmit, and process data to govern system functioning. Cyber system data flow must be efficient, reliable, and timely for physical processes to function [48]. Cyberattacks on smart microgrid data flow compromise availability, integrity, and confidentiality [49].

4.5.9. Type of Cybersecurity Attack on Smart Grids and Microgrids

There are several types of possible cyber threats to smart grid and microgrid infrastructure. The most prominent ones have been given below, and some examples of these attacks in the recent past have been summarized in Table 3.

- Distributed denial of service (DDoS) attacks: In the context of smart grids and microgrids, DDoS attacks can cause disruptions to the communication and control systems used to manage the flow of electricity. This can result in power outages or other system failures [50].
- Malware attacks: Malware attacks on smart grids and microgrids can compromise the systems used to monitor and control the flow of electricity, leading to system failures or disruptions. Malware can also be used to steal sensitive data or credentials, which can be used to carry out further attacks [51].

- Ransomware attacks: Ransomware attacks on smart grids and microgrids can result in system failures or disruptions, which can have serious consequences for public safety and the economy. In some cases, attackers may demand ransom payments in exchange for the decryption key needed to restore systems [52].
- Social engineering attacks: Social engineering attacks on smart grids and microgrids can be used to gain unauthorized access to critical systems or steal sensitive data. This can result in system failures or disruptions and compromise the security of the entire energy grid [53].
- Insider threats: Insider threats in the context of smart grids and microgrids can involve trusted employees or contractors who intentionally or unintentionally compromise security. It can include stealing data or credentials, introducing malware code, or failing to follow security protocols [54,55].
- Physical attacks: Physical attacks on smart grids and microgrids can involve vandalizing or damaging critical infrastructure, such as power lines, transformers, or substations. It can cause significant disruptions to the flow of electricity and pose a serious threat to public safety.
- Supply chain attacks: Supply chain attacks on smart grids and microgrids can involve exploiting vulnerabilities in third-party software or hardware used in the system. This can result in unauthorized access to critical systems, theft of sensitive data, or system failures or disruptions.
- Advanced persistent threat (APT) attacks: APT attacks on smart grids and microgrids involve using sophisticated techniques to gain persistent access to the network and steal sensitive data or cause system failures or disruptions. APT attacks can be difficult to detect and prevent, resulting in long-term damage to the energy grid.
- Credential stuffing attacks: Credential stuffing attacks on smart grids and microgrids involve using stolen login credentials to gain unauthorized access to critical systems. It can result in system failures or disruptions and compromise the security of the entire energy grid.
- Zero-day attacks: Zero-day attacks on smart grids and microgrids involve exploiting previously unknown vulnerabilities in software or hardware. This can result in unauthorized access to critical systems, theft of sensitive data, or system failures or disruptions. Zero-day attacks can be difficult to detect and prevent and can cause significant damage to the energy grid [56].

Table 3. Examples of cybersecurity attacks on smart grids and microgrids.

Example	Country	Year	Type of Attack	Details
Ukraine power outage [57]	Ukraine	2015	DDoS	In December 2015, a group of attackers used a DDoS attack to overload the servers of three Ukrainian power distribution companies, causing a widespread power outage that left over 225,000 customers without electricity for several hours.
Dragonfly 2.0 [58]	Global	2013	APT	Dragonfly 2.0 is a malware campaign that has been targeting energy grids and other critical infrastructure around the world since 2013. The attackers behind the campaign have been using various techniques to gain access to energy grid control systems, including spear-phishing and watering hole attacks.
City of Johannesburg ransomware [59]	South Africa	2019	Ransomware	In 2019, the City of Johannesburg in South Africa suffered a ransomware attack that affected its power grid, causing widespread power outages across the city. The attackers demanded a ransom of 4 Bitcoin, which the city refused to pay.
Target breach [60]	United States	2013	Social Engineering	In 2013, attackers gained access to the systems of the US retailer Target by using a phishing attack to steal login credentials from an HVAC contractor. The attackers were able to take the credit card data of over 40 million clients.

Table 3. *Cont.*

Example	Country	Year	Type of Attack	Details
Metcalf substation attack [61]	United States	2013	Physical Attack	In 2013, attackers fired over 100 rounds of ammunition at the Metcalf substation in California, damaging transformers and other equipment. While the attack did not cause a power outage, it highlighted the vulnerability of physical infrastructure to attack.
Colonial Pipeline attack [62]	United States	2021	Ransomware	The Colonial Pipeline, which provides over half of the petroleum for the US East Coast, experienced a ransomware attack in May 2021, forcing it to cease operations. Colonial Pipeline eventually paid the $4.4 million Bitcoin ransom requested by the attackers, a group going under the name of DarkSide.
SolarWinds hack [63]	Global	2020	Supply Chain Attack	The SolarWinds Orion software (version 2019.4 through 2020.2.1 HF1) was found to have been compromised in December 2020 as a result of a sophisticated supply chain attack that affected numerous US government organizations and commercial businesses. The attackers thought to be a state-sponsored gang from Russia, could access private information and systems thanks to the infected software.
Tesla's AWS servers were hacked for cryptocurrency mining [64]	United States	2018	Credential Stuffing	In 2018, attackers were able to compromise Tesla's AWS servers using credential stuffing, which involves using stolen login credentials from one site to gain access to another. The attackers used the compromised servers to mine cryptocurrency, which can be a lucrative source of revenue.
Sandworm Team attack [65]	Global	2019	Insider Threat	In 2019, the investigative journalism site Bellingcat published a report on the GRU's Sandworm Team. This Russian state-sponsored hacking group has been linked to multiple attacks on energy grids and other critical infrastructure. The report alleged that the group includes insiders who have helped to facilitate their attacks.
Accellion FTA attacks [66]	Global	2021	Supply Chain Attack	In early 2021, attackers began exploiting vulnerabilities in the Accellion File Transfer Appliance (FTA), a popular file-sharing tool many organizations use. The attackers were able to steal sensitive data from numerous companies, including energy companies like Royal Dutch Shell and the Australian energy company Powercor.
Enel ransomware attack [67]	Italy	2020	Ransomware	In 2020, energy giant Enel was targeted by a snake and Netwalker ransomware.
Natanz nuclear facility attack [68]	Iran	2021	Insider Threat	In 2021, a cyberattack targeted Iran's Natanz nuclear facility, causing significant damage to its centrifuge assembly plant. The attack was allegedly carried out by insiders who were able to gain access to the facility's control systems and cause the damage.

5. BC Enabled Micro Grid

BC is a decentralized, secure, and transparent system for recording transactions. BC technology enables the creation of a digital ledger of transactions that can be shared among a network of participants without the need for a central authority or intermediary. BC technology uses cryptographic techniques to ensure data integrity, confidentiality, and availability. Figure 2 below provides a sample transaction flow for any BC transaction.

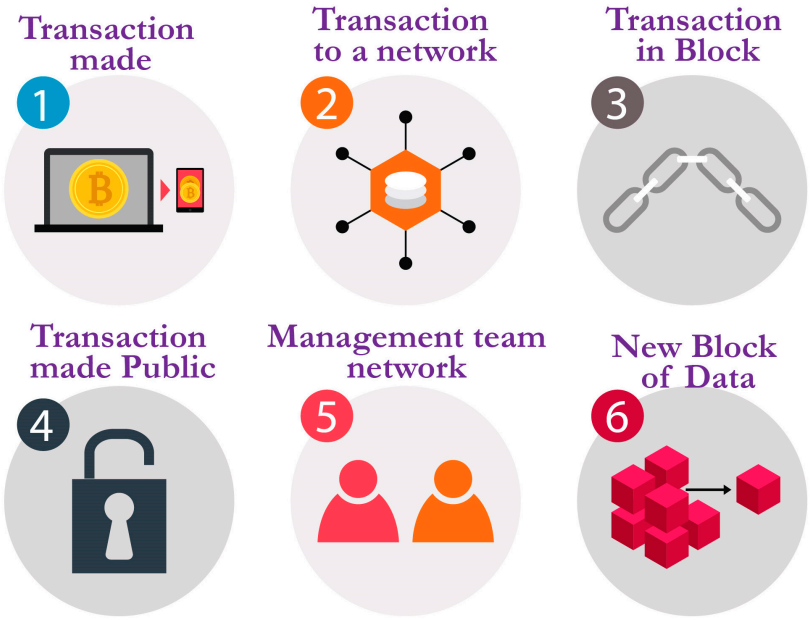

Figure 2. Sample BC transaction.

BC is classified three categories: public, private, and hybrid. In addition to the main types of BC, different consensus algorithms are used to validate BC transactions, such as PoW and proof of stake (PoS).

In conclusion, BC technology is a decentralized, secure, and transparent system for recording transactions. There are three main types of BC: public, private, and hybrid, each with advantages and use cases. Adopting BC technology requires a coordinated effort between stakeholders, including the government, energy companies, and technology providers, to promote investment, innovation, and collaboration in the sector.

5.1. BC Technology in the Energy Sector

By facilitating safe and transparent data transfers between energy producers, customers, and grid operators, BC technology has the potential to revolutionize the energy management industry. The advantages of BC for energy management include the following:

5.1.1. Decentralization

BC technology enables decentralized energy management solutions by eliminating the necessity for a centralized organization or middleman. Using decentralized energy management systems can improve energy management effectiveness and lessen reliance on centralized energy infrastructure. BC technology can lessen the possibility of energy monopolies by doing away with the need for a central authority and enhancing competition. Decentralized energy management systems can also aid in lowering the possibility of blackouts and improving energy security because energy can be produced and managed locally.

5.1.2. Security

BC technology enables secure and transparent data transactions between energy producers, consumers, and grid operators. BC-based energy trading platforms, demand response programs, and decentralized energy management systems can provide higher levels of security than traditional systems. With BC technology, all energy transactions are securely recorded and validated, reducing the risk of fraud and errors. Additionally, BC technology can enable greater control over access to energy data, reducing the risk of unauthorized access or misuse [69].

5.1.3. Transparency

BC technology enables transparent data transactions between energy producers, consumers, and grid operators. BC-based energy trading platforms, demand response programs, and decentralized energy management systems can provide greater transparency in energy transactions, promoting trust and accountability. All energy transactions are publicly recorded and validated with BC technology, enabling greater transparency and accountability in the energy management sector.

5.1.4. Efficiency

BC technology enhances energy management by lowering transaction costs and promoting renewable energy. The ability to purchase energy directly from suppliers through BC's demand response programs and energy trading systems lowers transaction costs while promoting renewable energy. BC technology enables real-time monitoring and control of the energy system, reducing energy waste and increasing efficiency.

5.1.5. Innovation

BC technology makes P2P energy trade and decentralized energy management systems possible, which can foster innovation in energy management. Demand response initiatives and BC energy trading platforms can support creative energy management while reducing reliance on the energy grid. Developing energy storage and renewable energy technologies can benefit from BC technology.

5.2. Potential BC Applications for Energy Management in Saudi Arabia

KSA is one of the world's largest oil-producing countries and has traditionally relied heavily on fossil fuels for its energy needs. However, in recent years, KSA has recognized the need to diversify its energy sources and promote greater efficiency and sustainability in energy management. BC technology has emerged as a promising solution for achieving these goals, enabling secure and transparent data transactions between energy producers, consumers, and grid operators. In this section, we will explore the potential applications of BC technology in KSA's energy sector, including energy trading, demand response, decentralized energy management, smart contracts, and environmental concerns.

5.2.1. Energy Trading

P2P energy trading can be made possible in the energy sector of KSA using BC technology. Energy trading platforms headquartered in BC can encourage the use of renewable energy sources and lessen reliance on centralized energy networks by letting customers buy energy directly from renewable energy providers. BC-based energy trading platforms can also facilitate more effective energy management by lowering transaction costs and enabling real-time monitoring and control of energy facilities.

5.2.2. Demand Response

Demand response programs can be made possible by BC technology in the energy industry in KSA. Demand response solutions allow energy users to use less energy during periods of high demand, preventing blackouts and lowering reliance on fossil fuels. The energy sector in KSA may encourage more efficiency and creativity in energy management by adopting BC technology to securely and transparently manage demand response programs.

5.2.3. Decentralized Energy Management

Decentralized energy management systems can be made possible using BC technology in the KSA energy industry. Systems for decentralized energy management remove the need for a central authority or middleman, enabling more effective energy management. Decentralized energy management systems based in BC can encourage the use of renewable

energy sources and lessen reliance on centralized energy systems by allowing energy producers and customers to actively participate in energy management actively.

5.2.4. Environmental Concerns

BC technology can promote greater transparency and accountability in KSA's energy sector by enabling more effective monitoring and management of environmental concerns. By using BC technology to securely and transparently record energy consumption and emissions data, KSA's energy sector can promote greater environmental awareness and sustainability.

By fostering higher efficiency, creativity, and sustainability in energy management, BC technology has the potential to completely change the energy landscape in KSA completely. Energy businesses, the government, and technology providers must work together in a coordinated effort to encourage investment, innovation, and cooperation in the industry if BC technology is to be adopted in KSA's energy sector.

5.3. Case Studies of BC Applications in Energy Management

Blockchain technology has been utilized in energy management for a while for different tasks. A summary of case studies of BC applications in other countries for energy management has been presented in Table 4.

Table 4. Case studies of BC applications in energy management.

Company/Project	Country	Application	Year
Power Ledger [70]	Australia	BC-based energy trading platform enabling P2P trading between renewable energy producers and consumers	2016
TenneT [71]	Germany	Equigy, a BC-based platform enabling energy producers to participate in demand response programs and provide power to the grid thru peak demand times	2020
Brooklyn Microgrid [72]	United States	BC-based energy trading platform enabling consumers to purchase energy directly from local renewable energy producers	2017
TEPCO [73]	Japan	Energy Web Chain, a BC-based platform enabling secure and transparent data transactions between energy producers, consumers, and grid operators	2019
Energie Wasser Bern [74]	Switzerland	BC-based energy trading platform enabling P2P trading between renewable energy producers and consumers	2017
Wien Energie [75]	Austria	Local energy marketplace enabling P2P energy trading	2018
Electron [76]	United Kingdom	National database for renewable energy certificates using BC technology to ensure authenticity and traceability	2018
Thai Digital Energy Development (TDED) [77]	Thailand	A BC-based platform for tracking renewable energy certificates and ensuring compliance with renewable energy targets	2019
KEPCO [78]	South Korea	P2P energy trading platform enabling consumers to trade energy directly with each other	2019
Acciona [79]	Spain	A BC-based platform for tracking the production and consumption of renewable energy	2020
Vattenfall [80]	Sweden	A BC-based platform for tracking the origin of renewable energy	2021
SP Group [81]	Singapore	A BC-based platform for P2P energy trading	2018
Enexis [82]	Netherlands	A BC-based platform for managing energy data	2019
Électricité de France (EDF) [83]	France	A BC-based platform for managing the supply chain of renewable energy certificates	2018
Xpansiv [84]	United States	A BC-based platform for tracking and trading energy commodities	2018

Numerous nations worldwide are implementing BC-based energy management systems to encourage renewable energy and enable more effective energy management. These case studies demonstrate how BC technology can reform the energy industry by facilitating safe and transparent data exchanges between grid operators, energy providers, and consumers. Adopting BC technology requires a coordinated effort between stakeholders, including the government, energy companies, and technology providers, to promote investment, innovation, and collaboration in the sector.

5.4. Role of BC in Supporting Standards and Protocols for Cybersecurity in Smart Grids and Microgrids

Adopting BC technology in KSA's energy sector presents opportunities and challenges. BC technology can improve the efficiency of KSA's energy sector by reducing transaction costs, promoting transparency, and enabling real-time monitoring and control of energy systems. Furthermore, BC technology can help promote the adoption of renewable energy sources in KSA and enhance the cybersecurity of energy management systems. However, there are challenges to the adoption of BC technology in KSA's energy sector. Technical challenges, such as a lack of expertise and investment in new infrastructure, can pose a challenge for energy companies and government agencies. Additionally, regulatory challenges around data privacy, security, and ownership issues must be addressed. The lack of interoperability between different BC platforms and energy systems also presents a challenge to the adoption of BC technology in KSA's energy sector. To overcome these challenges, KSA's energy sector stakeholders must collaborate to develop innovative solutions and promote more significant investment and innovation. Different agencies have defined a set of protocols and standards that must be followed to overcome cybersecurity threats in smart grids and microgrids. These standards are being followed in different regions based on their requirements. A summary of these Standard/Protocol have been given in Table 5 and further elaborates on how BC can help support these standard/protocol. It can be beneficial for the KSA to develop some standard protocols or adopt any of these and integrate them with BC applications.

Table 5. Role of BC in supporting standards and protocols for cybersecurity in smart grids and microgrids.

Standard/Protocol	Details of Standard/Protocol	Role of BC
NISTIR 7628 [85]	NIST publication provides guidelines for securing smart grid systems. It covers several areas related to cybersecurity, including access control, network security, and incident response.	BC can provide secure and immutable logging of events and transactions, making tracking and tracing potential security breaches easier. It can also enable secure data sharing among stakeholders in the energy sector.
NERC CIP [86]	This set of cybersecurity standards applies to the bulk power system in North America. The NERC CIP standards cover several areas related to power system security, including cybersecurity awareness, physical security, and incident response.	BC can provide secure and decentralized identity management, making controlling access to critical systems and information easier. It can also enable secure and transparent communication among stakeholders in the energy sector.
IEC 62351 [87]	This set of standards developed by the International Electrotechnical Commission (IEC) provides a framework for the secure communication and operation of power systems. It covers several areas related to power system security, including authentication and encryption, data integrity, and access control.	BC can provide secure and decentralized key management, making it easier to manage and protect cryptographic keys used for authentication and encryption. It can also enable secure and transparent communication among stakeholders in the energy sector.

Table 5. *Cont.*

Standard/Protocol	Details of Standard/Protocol	Role of BC
ISO/IEC 27001/27002 [88]	These complementary standards provide a framework for information security management systems (ISMS). They cover several areas related to information security, including risk assessment, access control, incident response, and security management.	BC can provide secure and immutable logging of events and transactions, making tracking and tracing potential security breaches easier. It can also enable secure and transparent information sharing among stakeholders in the energy sector.
GB/T 22239 [89]	This set of cybersecurity standards developed by the Chinese National Standardization Technical Committee for Information Security guides the secure design, implementation, and operation of information systems and networks.	BC can provide secure and decentralized identity management, making controlling access to critical systems and information easier. It can also enable secure and transparent communication among stakeholders in the energy sector.
SP 800-82 [90]	This publication by NIST provides guidelines for the secure design, implementation, and operation of industrial control systems (ICS). It covers several areas related to ICS security, including risk management, access control, network security, and system security.	BC can provide secure and immutable logging of events and transactions, making tracking and tracing potential security breaches easier. It can also enable secure and transparent information sharing among stakeholders in the energy sector.

Overall, BC can play a valuable role in enhancing the security and reliability of smart grids and microgrids by providing secure and decentralized identity management, key management, and logging of events and transactions. It can also enable secure and transparent communication and sharing of information among stakeholders in the energy sector.

6. BC-Based Framework for an Energy Microgrid in Saudi Arabia

A BC-based framework for an energy microgrid in Saudi Arabia has been presented in Figure 3. There are several aspects to its functioning. These are the detailed representations of the BC-based framework for a microgrid system, which includes the following components and steps:

- Energy Tracking and Trading Platform
    - Receive energy data from IoT sensors installed in the microgrid/community grid;
    - Convert energy data into digital format and timestamp it;
    - Store the energy data on a decentralized BC network;
    - Verify the energy data using a consensus mechanism;
    - Facilitate energy trading between energy producers and consumers based on smart contracts;
    - Execute energy transactions using cryptocurrencies or digital tokens;
    - Update energy data on the BC ledger and generate receipts for energy transactions.
- Renewable Energy Certificate (REC) Tracking System
    - Receive information about renewable energy production from energy producers;
    - Verify the authenticity of the information using a consensus mechanism;
    - Issue digital certificates for the amount of renewable energy produced;
    - Store the digital certificates on a decentralized BC network;
    - Facilitate the trading of digital certificates between energy producers and consumers based on smart contracts;
    - Execute certificate transactions using cryptocurrencies or digital tokens;
    - Update certificate data on the BC ledger and generate receipts for certificate transactions.
- Energy Management System (EMS)

- Monitor energy demand and supply in the microgrid/community grid using IoT sensors;
- Collect energy data and process it using analytics tools;
- Use predictive analytics to forecast energy demand and supply;
- Optimize energy use and distribution using automated algorithms;
- Communicate with the energy tracking and trading platform to facilitate energy transactions.

- Decentralized Energy Marketplace
  - Provide a decentralized platform for energy trading;
  - Facilitate P2P energy trading using smart contracts;
  - Enable producers to sell excess energy to other microgrid/community grid consumers;
  - Provide transparency and traceability for the energy transactions using BC technology;
  - Ensure the security and privacy of energy data and transactions.
- Identity and Access Management System
  - Authenticate and authorize energy producers and consumers using digital identities;
  - Store digital identities on a decentralized BC network;
  - Provide role-based access control to energy data and transactions;
  - Ensure the privacy and security of digital identities using encryption and cryptographic techniques.
- Analytics and Reporting Platform
  - Collect and process energy data from the energy tracking and trading platform and EMS;
  - Generate reports and dashboards for energy usage, supply, and demand;
  - Provide real-time insights into energy consumption patterns and trends;
  - Facilitate decision-making for energy management and planning;
  - Ensure data accuracy and integrity using BC-based data storage and verification mechanisms.

Overall, a BC-based framework for a microgrid or community grid system could enable greater transparency, efficiency, and security in energy trading and management while promoting the integration of renewable energy and decreasing reliance on centralized energy systems.

These components would work together to create a BC-based framework for a microgrid or community grid system that supports efficient and secure energy exchange.

Algorithm A1 (refer to Appendix A) provides a pseudo code of energy tracking and trading function. This function in Algorithm A1 will track energy production, consumption, and trading. It continuously monitors the system's energy producers, consumers, and traders to track their energy production, consumption, and trading activities. Based on the collected energy data, it creates energy transactions and updates the energy prices for trading. The function runs in an infinite loop to ensure real-time energy tracking and trading within the microgrid system. It will do this by first checking if the lists of producers, consumers, and traders are empty. If they are not, it will then iterate through each list and call the getEnergyProduced(), getEnergyConsumed(), and getEnergyTraded() functions, respectively. These functions will return the amount of energy produced, consumed, or traded by the corresponding entity. If the amount of energy exceeds 0, the function will add a new energy transaction to the energyTransactions list.

Once the function has added all energy transactions to the list, it will call the getEnergyPrice() function for each transaction. This function will return the price of the energy in the transaction. The function will then add the price to the energyPrices list.

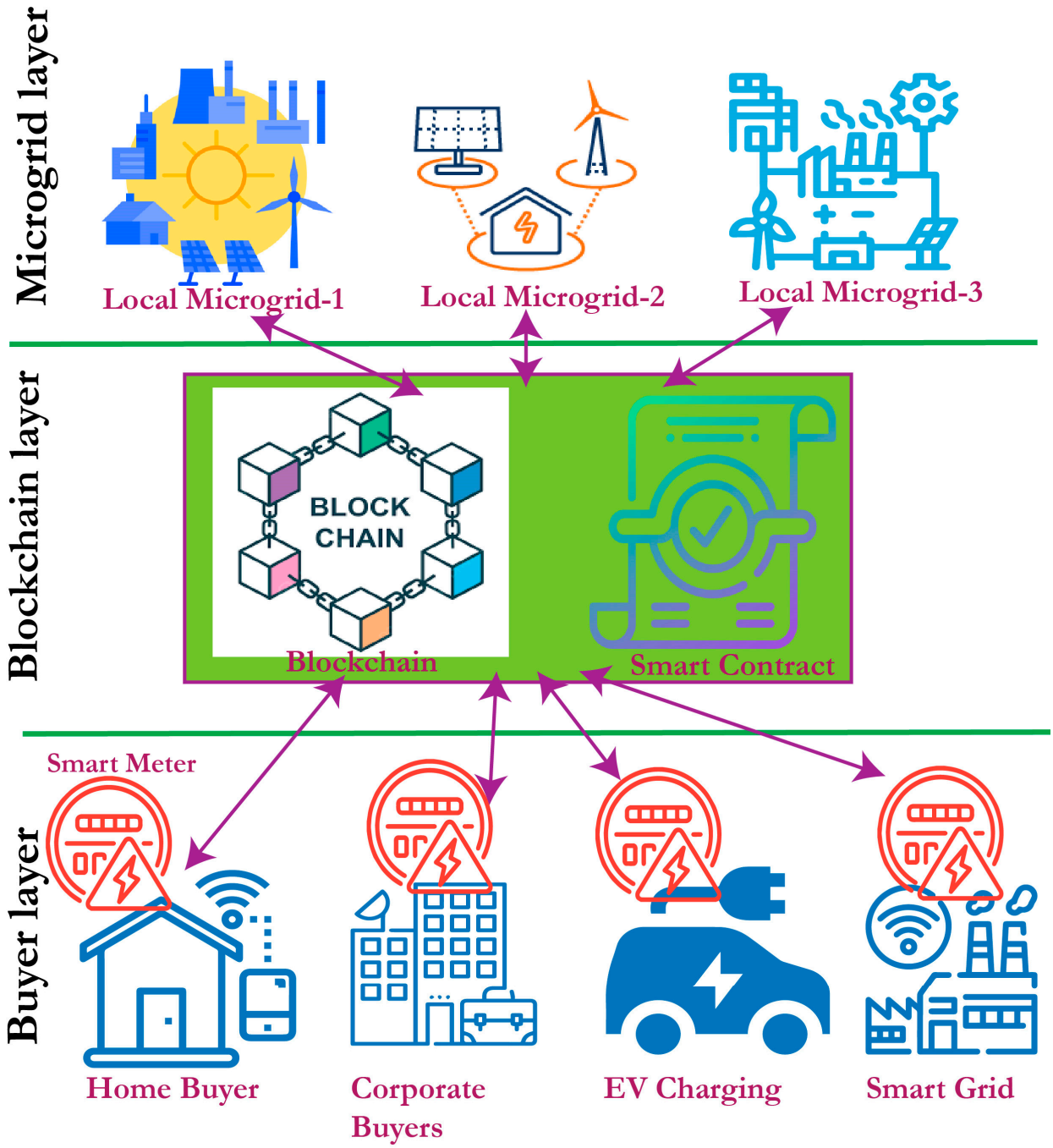

Figure 3. BC-based Framework for an Energy Microgrid.

Algorithm A2 (refer to Appendix B) provides a pseudo code of renewable energy certificate (REC) tracking function. This function in Algorithm A2 will track the issuance of a renewable energy certificate (REC). It monitors the system's renewable energy certificates (RECs) to track their issuance and updates. Based on the collected REC data, it creates REC transactions to record the issuance of RECs on the blockchain ledger. The function runs in an infinite loop to ensure real-time tracking of renewable energy certificates within the microgrid system. It will do this by first checking if the list of RECs is empty. If it is not, it will then iterate through the list and call the getRecIssued() function for each REC. This function will return the number of RECs issued for the corresponding REC. If the number of RECs exceeds 0, the function will add a new REC transaction to the recTransactions list.

Algorithm A3 (refer to Appendix C) provides a pseudo code for the Energy Management System (EMS) component in the proposed blockchain-based microgrid framework. The EMS continuously monitors energy demand and supply using IoT sensors and processes the collected data using analytics tools. It forecasts energy demand and supply using predictive analytics and optimizes energy distribution using automated algorithms. The EMS then communicates with the energy tracking and trading platform to facilitate energy transactions based on the optimized energy distribution. The function runs in an infinite loop to ensure real-time monitoring and management of energy within the microgrid system.

The pseudocode in Algorithm A4 (refer to Appendix D) represents the decentralized energy marketplace component in the proposed blockchain-based microgrid framework. The smart contract EnergyTradingContract enables energy trading between sellers and buyers based on the specified energy amount and price. Before executing the transaction, it performs necessary validations, such as checking energy availability and the buyer's available funds. The function initiateEnergyTrading is used to initiate peer-to-peer (P2P) energy trading by calling the initiateEnergyTransaction function in the smart contract. The respective functions carry out the transfer of energy tokens or cryptocurrencies and the update of the energy transaction on the blockchain ledger.

The pseudocode in Algorithm A5 (refer to Appendix E) reflects the identity and access management system part of a BC-based microgrid system for a microgrid in Saudi Arabia. It includes functions for authenticating and authorizing identities, storing digital identities on the blockchain, providing role-based access control, ensuring privacy and security, and storing access logs on the blockchain for auditing purposes. These functions collectively manage users' digital identities in the microgrid system and control their access to various functionalities and data based on their roles and permissions.

This pseudocode in Algorithm A6 (refer to Appendix F) provides a basic framework for an analytics and reporting platform in an energy management system. The collectAndProcessEnergyData() function collects energy data from the energy tracking and trading platform and EMS and then processes the data. The generateReportsAndDashboards() function generates reports and dashboards based on the processed data, and the provideRealTimeInsights() function provides real-time insights from the processed data. It then processes the collected data to generate useful information, which is used to create reports, dashboards, and real-time insights. The platform operates in a loop, ensuring continuous data collection and processing at regular intervals. The actual implementation of the functions would depend on the specific requirements and data processing needs of the energy microgrid system.

The BC-based Framework for an energy microgrid consists of three interconnected layers that facilitate seamless interactions and enable efficient energy management and trading. In Layer 1, microgrids play a vital role in generating energy. Algorithm A1, the energy tracking and trading function, enables energy producers to record their energy production data collected from IoT sensors within the microgrids. This data is then timestamped and stored on the blockchain in Layer 2. In Layer 2, Algorithm A4, the decentralized energy marketplace, creates a decentralized platform for energy trading. Producers can sell their excess energy to other microgrid consumers through smart contracts, and energy transactions are executed using cryptocurrencies or digital tokens.

Additionally, Algorithm A2, the REC tracking function, ensures the tracking and trading of renewable energy certificates on the blockchain, further enhancing the sustainability aspect of the system. Layer 3 involves consumers and producers interacting with the energy tracking and trading platform (Algorithm A1) to initiate energy transactions. Algorithm A5, the identity and access management function, ensures that all participants are authenticated and authorized to engage in energy trading, adding a layer of security to the system. The energy management system (Algorithm A3) continuously monitors energy demand and supply, optimizing energy distribution and communication with the energy tracking and trading platform to facilitate transactions. Algorithm A6, the analytics and

reporting platform, processes energy data and generates valuable insights for decision-making and planning. These interactions between the layers create a comprehensive and robust framework that fosters transparency, security, and efficiency in energy management and trading within the microgrid system. A simplified implementation has been made using the Python programming language for the above functions, and a sample of five transactions have been made using the system. The sample five transactions have been shown in Figure 4. Further, for the simulation purpose, we have considered five users that have been shown as User 0 to User 4. The transactions have been used to update the total amount of transactions and total due amount based on the variable energy rate. Each user amount is updated regularly for a period. This period can be daily, weekly, or monthly, depending on the account settlement. A sample report for five users has been presented in Figure 5.

```
Transaction 1:
Seller: User 0
Buyer: User 1
Energy Amount: 100 kWh
Price Rate: 2
Transaction Time: 10:03:10

Transaction 2:
Seller: User 2
Buyer: User 3
Energy Amount: 200 kWh
Price Rate: 3
Transaction Time: 10:03:11

Transaction 3:
Seller: User 4
Buyer: User 5
Energy Amount: 300 kWh
Price Rate: 4
Transaction Time: 10:03:12

Transaction 4:
Seller: User 1
Buyer: User 2
Energy Amount: 400 kWh
Price Rate: 5
Transaction Time: 10:03:13

Transaction 5:
Seller: User 3
Buyer: User 4
Energy Amount: 500 kWh
Price Rate: 1
Transaction Time: 10:03:14
```

Figure 4. Sample Transactions.

```
------------------
User: User 0
Sold Energy Amount: 100 kWh
Purchased Energy Amount: 0 kWh
Total Sold Energy Price: Energy Amount * Price Rate = 100*2 = 200
Total Purchased Energy Price: 0 SAR
Total Amount Due: 200 SAR

------------------
User: User 1
Sold Energy Amount: 100 kWh
Purchased Energy Amount: 400 kWh
Total Sold Energy Price: Energy Amount * Price Rate = 100*5 = 500
Total Purchased Energy Price: Energy Amount * Price Rate = 400*5 = 2000
Total Amount Due: -1500 SAR

------------------
User: User 2
Sold Energy Amount: 200 kWh
Purchased Energy Amount: 0 kWh
Total Sold Energy Price: Energy Amount * Price Rate = 200*3 = 600
Total Purchased Energy Price: 0 SAR
Total Amount Due: 600 SAR

------------------
User: User 3
Sold Energy Amount: 500 kWh
Purchased Energy Amount: 200 kWh
Total Sold Energy Price: Energy Amount * Price Rate = 500*1 = 500
Total Purchased Energy Price: Energy Amount * Price Rate = 200*3 = 600
Total Amount Due: -100 SAR

------------------
User: User 4
Sold Energy Amount: 0 kWh
Purchased Energy Amount: 300 kWh
Total Sold Energy Price: 0 SAR
Total Purchased Energy Price: Energy Amount * Price Rate = 300*4 = 1200
Total Amount Due: -1200 SAR
```

Figure 5. Sample User Financial Transactions.

Security Analysis of the Proposed Framework

This section presents a theoretical security analysis of the proposed framework, highlighting its robustness and transparency.

- Immutability and Data Integrity: Using a blockchain ensures immutability and data integrity. Once data is recorded on the blockchain, it cannot be altered or tampered with, providing high trust and preventing unauthorized modifications. For example, the Cryptographic Hash Function (e.g., SHA-256) is used for immutability and data integrity.
- Consensus Mechanism: The consensus mechanism used in the blockchain ensures the agreement and validity of transactions among participating nodes. This mechanism helps prevent attacks such as double-spending and ensures the system's integrity. Proof-of-Work or Byzantine Fault Tolerance (BFT) algorithms ensure blockchain data.
- Encryption and Privacy: Encryption techniques are applied to protect sensitive data, including digital identities, energy transactions, and personal information. It helps to ensure privacy and confidentiality, making it difficult for unauthorized parties to access or manipulate data. Elliptic Curve Cryptography (ECC) with Homomorphic Encryption will provide a secure and reliable environment for security and privacy.
- Authentication and Access Control: The Identity and Access Management System implements strong authentication mechanisms and role-based access control. It ensures that only authorized users with the appropriate roles can access specific functionalities and data, reducing the risk of unauthorized access. The Elliptic Curve Digital Signature Algorithm (ECDSA) with Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) is used for strong Authentication and Access Control.
- Secure Communication: Secure communication protocols are employed to protect data transmission within the microgrid system. It prevents eavesdropping and unauthorized interception of sensitive information. Transport Layer Security (TLS) or Secure Socket Layer (SSL) protocols can be used for secure communication.

- Resilient Infrastructure: The microgrid system is designed with redundancy and fault tolerance mechanisms, ensuring the availability and reliability of energy supply. This resilience helps mitigate the impact of potential attacks or failures and maintains uninterrupted energy distribution.
- Auditing and Monitoring: The framework includes auditing and monitoring mechanisms to promptly detect and respond to security incidents. Logs of access events, transactions, and system activities are stored on the blockchain, enabling traceability and accountability. Real-time monitoring tools and anomaly detection algorithms can be implemented to identify potential security threats.
- Regulatory Compliance: The framework ensures compliance with relevant regulations and standards related to data protection, privacy, and energy trading. By leveraging blockchain technology, the system provides transparent and auditable records that can aid in regulatory compliance.
- Threat Mitigation: Using blockchain technology reduces the risk of centralized attacks as the distributed nature of the network makes it more difficult for malicious actors to compromise the system. Additionally, integrating cryptographic techniques and secure protocols helps mitigate various security threats.

The proposed framework can counter the cyber security concerns that will help counter the known threats and provide a secure and reliable system for power generation and distribution in KSA.

7. Research Challenges and Future Work

There are some research challenges and future research scope that need to be considered for further research:

- Scalability: Scaling BC technology to handle large transactions and data in a microgrid context is a significant challenge. Developing solutions to improve the scalability of BC networks while maintaining security and efficiency is crucial [91].
- Interoperability: Microgrids involve stakeholders, including energy producers, consumers, grid operators, and regulatory bodies. Ensuring interoperability between BC platforms and legacy systems is essential for seamless integration and data exchange [92].
- Protocol Design and Optimization: Continued research is needed to design and optimize BC protocols tailored to smart grid and microgrid applications. It includes developing consensus algorithms, smart contract frameworks, and data management techniques that address the unique requirements of the power generation and distribution domain [34].
- Integration with Emerging Technologies: Exploring the integration of BC with other emerging technologies, such as the IoT, AI, and edge computing, can unlock new possibilities for microgrid applications. Investigating how these technologies can complement each other and enhance the safety and reliability of power systems is an area for future work [93].
- Regulatory and Policy Considerations: As BC technology evolves, addressing legal, regulatory, and policy challenges becomes paramount. Research on developing frameworks, standards, and guidelines that promote the adoption of BC in the energy sector while addressing concerns regarding privacy, security, and governance is necessary.
- Safe and reliable power generation and distribution can be further realized and optimized by addressing these research challenges and future work in these areas.

8. Conclusions

This article has reviewed the state of the art to get the current standards in the domain and reviewed the security threats to energy generation and distribution infrastructure. Case studies from different countries have been presented, and the possible international standards for cybersecurity have been reviewed. This article examines in detail the role of BC in securing energy infrastructures and their respective advantages and limitations.

Based on these reviews and analyses, it can be concluded that adopting BC and microgrid technologies in KSA's energy sector presents significant opportunities for improving energy efficiency, promoting renewable energy adoption, and enhancing cybersecurity. However, adopting these technologies also presents substantial challenges, including technical, regulatory, and legal challenges and a lack of interoperability between different BC platforms and energy systems. It also highlights the specific needs of the energy sector in KSA and the required technological developments to ensure compliance with existing regulations and promote the adoption of BC and microgrid technologies in KSA's energy sector. Finally, this article proposes a BC-based framework for integrating all the aspects of a microgrid system, including peer-to-peer (P2P) energy trading, renewable energy certificates (REC) to support renewable energy utilization, identity, and access management, and decentralized energy trading that can be utilized in Saudi Arabia. It includes the integration of cybersecurity standards and protocols, as well as the utilization of smart contracts. A theoretical security analysis has been conducted that highlights its robustness and security. The proposed framework can ensure the cybersecurity of microgrids and pave the way for more secure and durable energy in the future with high reliability and transparency.

Future work in this area could involve the development of pilot projects and testbeds to demonstrate the feasibility and effectiveness of BC and microgrid technologies in KSA's energy sector. Additionally, the research could focus on developing new applications and use cases for BC and microgrid technologies in energy management, such as integrating electric vehicle charging infrastructure and using BC-based tokens to incentivize renewable energy adoption. By recognizing these limitations and challenges, stakeholders can proactively mitigate risks and foster a conducive environment for BC and microgrid technologies to flourish. Furthermore, engaging and educating stakeholders, including energy consumers and producers, is crucial for the widespread adoption of BC and microgrid solutions. Raising awareness about the benefits and functionalities of these technologies will help build trust and foster greater acceptance among all participants.

Author Contributions: Conceptualization, S.A. and M.M.K.; formal analysis, S.A. and M.M.K.; investigation, S.A. and M.M.K.; project administration, M.M.K.; resources, M.M.K.; visualization, M.M.K.; writing—original draft, S.A. and M.M.K.; writing—review and editing, S.A. and M.M.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Deanship of Scientific Research, Jazan University, Jazan, Saudi Arabia, under grant no W43-071.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviation

Abbreviation	Definition
SPOF	Single Point Of Failure
BC	Blockchain
P2P	Peer-To-Peer
REC	Renewable Energy Certificate
KSA	Kingdom of Saudi Arabia
GASTAT	General Authority for Statistics, KSA
CO_2	Carbon Dioxide
NREP	National Renewable Energy Program, KSA
SG	Smart Grid
IoT	Intenet of Things
AI	Artificial Intelligence
PoW	Proof of Work
PoA	Proof-of-Authority
PoS	pProof Of Stake

DDoS	Distributed Denial of Service
APT	Advanced Persistent Threat
REC	Renewable Energy Certificate
EMS	Energy Management System
SHA	Secure Hash Algorithm
BFT	Byzantine Fault Tolerance
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
MFA	Multi-factor Authentication
RBAC	Role-Based Access Control
TLS	Transport Layer Security
SSL	Secure Socket Layer

Appendix A

Algorithm A1: Pseudo Code of Energy Tracking and Trading Function

```
Input:
energyProducers: A collection of energy producers in the system.
energyConsumers: A collection of energy consumers in the system.
energyTraders: A collection of energy traders in the system.
energyPrices: A collection of energy prices.
Output:
energyTransactions: A list of energy transactions.
FUNCTION energyTrackingAndTrading()
    WHILE TRUE
        IF energyProducers IS NOT EMPTY
            FOR EACH producer IN energyProducers
                DECLARE energyProduced AS INTEGER
                energyProduced = getEnergyProduced(producer)
                IF energyProduced > 0
                    energyTransactions.append(createEnergyTransaction(producer,
energyProduced))
                END IF
        IF energyConsumers IS NOT EMPTY
            FOR EACH consumer IN energyConsumers
                DECLARE energyConsumed AS INTEGER
                energyConsumed = getEnergyConsumed(consumer)
                IF energyConsumed > 0
                    energyTransactions.append(createEnergyTransaction(consumer,
energyConsumed))
        END IF
        IF energyTraders IS NOT EMPTY
            FOR EACH trader IN energyTraders
                DECLARE energyTraded AS INTEGER
                energyTraded = getEnergyTraded(trader)
                IF energyTraded > 0
                    energyTransactions.append(createEnergyTransaction(trader, energyTraded))
        END IF
        IF energyPrices IS NOT EMPTY
            FOR EACH transaction IN energyTransactions
                DECLARE price AS INTEGER
                price = getEnergyPrice(transaction)
                energyPrices.append(price)
        END IF
        WAIT UNTIL NEXT INTERVAL
    END WHILE
END FUNCTION
```

Appendix B

Algorithm A2: Pseudo Code of Renewable Energy Certificate (REC) Tracking Function

```
FUNCTION recTracking()
    WHILE TRUE
        IF recs IS NOT EMPTY
            FOR EACH rec IN recs
                DECLARE recIssued AS INTEGER
                recIssued = getRecIssued(rec)
                IF recIssued > 0
                    recTransactions.append(createRecTransaction(rec, recIssued))
        END IF
            WAIT UNTIL NEXT INTERVAL
        END WHILE
END FUNCTION
```

Appendix C

Algorithm A3: Pseudo Code of Energy Management System (EMS)

```
# Energy Management System (EMS)
# Function to monitor energy demand and supply using IoT sensors
function monitorEnergyDemandAndSupply():
    while True:
        energyDemand = getEnergyDemandFromSensors()
        energySupply = getEnergySupplyFromSensors()
        # Process energy data using analytics tools
processedData = processEnergyData(energyDemand, energySupply)
        # Use predictive analytics to forecast energy demand and supply
        forecastedDemand = forecastEnergyDemand(processedData)
        forecastedSupply = forecastEnergySupply(processedData)
        # Optimize energy use and distribution using automated algorithms
        optimizedDistribution = optimizeEnergyDistribution(forecastedDemand,
forecastedSupply)
        # Communicate with the Energy Tracking and Trading Platform
        communicateWithTrackingAndTradingPlatform(optimizedDistribution)
        # Wait until the next monitoring interval
        waitUntilNextInterval()
# Function to get energy demand from IoT sensors
function getEnergyDemandFromSensors():
function getEnergySupplyFromSensors():
function processEnergyData(energyDemand, energySupply):
function forecastEnergyDemand(processedData):
function forecastEnergySupply(processedData):
function optimizeEnergyDistribution(forecastedDemand, forecastedSupply):
function communicateWithTrackingAndTradingPlatform(optimizedDistribution):
function waitUntilNextInterval():
function main():
    monitorEnergyDemandAndSupply()
```

Appendix D

Algorithm A4: Pseudo Code for Decentralized Energy Marketplace

```
# Smart contract for energy trading
contract EnergyTradingContract:
    function initiateEnergyTransaction(seller, buyer, energyAmount, price):
        # Perform necessary validations and checks
        if validateTransaction(seller, buyer, energyAmount, price):
            # Transfer energy tokens or cryptocurrencies
            transferTokens(seller, buyer, energyAmount, price)
            # Update energy transaction on the blockchain ledger
            updateEnergyTransaction(seller, buyer, energyAmount, price)
        else:
            handleTransactionError()
# Function to initiate P2P energy trading
function initiateEnergyTrading(seller, buyer, energyAmount, price):
    energyContract = EnergyTradingContract()
    energyContract.initiateEnergyTransaction(seller, buyer, energyAmount, price)
# Function to handle energy token or cryptocurrency transfer
function transferTokens(seller, buyer, energyAmount, price):
    # Transfer energy tokens or cryptocurrencies from buyer to seller
    transferEnergyTokens(buyer, seller, energyAmount)
    # Transfer payment from buyer to seller
    transferPayment(buyer, seller, price)
# Function to update energy transaction on the blockchain ledger
function updateEnergyTransaction(seller, buyer, energyAmount, price):
    # Create a new energy transaction record on the blockchain
    createEnergyTransactionRecord(seller, buyer, energyAmount, price)
# Function to validate energy transaction
function validateTransaction(seller, buyer, energyAmount, price):
    # Perform necessary validations, such as energy availability, price calculations, etc.
    if isEnergyAvailable(seller, energyAmount) and isPriceValid(buyer, price):
        return True
    else:
        return False
# Function to check energy availability
function isEnergyAvailable(seller, energyAmount):
    # Check if the seller has the required amount of energy available
    if seller.energySupply >= energyAmount:
        return True
    else:
        return False
# Function to validate price
function isPriceValid(buyer, price):
    if buyer.availableFunds >= price:
        return True
    else:
        return False
```

Appendix E

Algorithm A5: Pseudo Code for Identity and Access Management Function

```
function AuthenticateAndAuthorize(identity, role):
    authenticity = VerifyIdentity(identity)
    if authenticity is true:
        assignedRole = DetermineRole(identity)
        authorizedPermissions = RetrievePermissionsFromBlockchain(assignedRole)
        GrantAccess(authorizedPermissions)
    else:
        DenyAccess()
function StoreDigitalIdentity(identity):
    uniqueIdentifier = GenerateUniqueIdentifier()
    encryptedIdentity = EncryptIdentity(identity)
    transaction = CreateTransaction(encryptedIdentity)
    includedInBlock = ReachConsensus(transaction)
    if includedInBlock is true:
        AssignUniqueIdentifier(uniqueIdentifier)
    else:
        HandleTransactionFailure()
function ProvideRoleBasedAccessControl(identity, data):
    assignedRole = RetrieveRoleFromBlockchain(identity)
    authorizedPermissions = RetrievePermissionsFromBlockchain(assignedRole)
    if ValidateAccessRequest(authorizedPermissions, data):
        GrantAccess()
    else:
        DenyAccess()
function EnsurePrivacyAndSecurity(identity):
    encryptedIdentity = EncryptIdentity(identity)
    secureTransmission = ProtectTransmission(encryptedIdentity)
    strongAuthentication = ImplementAuthentication(encryptedIdentity)
    UpdateSecurityMeasures()
    StoreLogsOnBlockchain()
```

Appendix F

Algorithm A6: Pseudo Code for Analytics and Reporting Platform

```
function collectAndProcessEnergyData():
    while True:
        energyData = collectEnergyData()
        processedData = processEnergyData(energyData)
        generateReportsAndDashboards(processedData)
        provideRealTimeInsights(processedData)
        waitUntilNextInterval()
function collectEnergyData():
function processEnergyData(energyData):
function generateReportsAndDashboards(processedData):
function provideRealTimeInsights(processedData):
function waitUntilNextInterval():
    collectAndProcessEnergyData()
```

References

1. Hassan, Q.; Al-Hitmi, M.; Tabar, V.S.; Sameen, A.Z.; Salman, H.M.; Jaszczur, M. Middle East Energy Consumption and Potential Renewable Sources: An Overview. *Clean. Eng. Technol.* **2023**, *12*, 100599. [CrossRef]
2. General Authority for Statistics (GASTAT) Electric Energy Statistics 2021. Available online: https://www.stats.gov.sa/sites/default/files/Electric_Energy_Statistics_2021_En.pdf (accessed on 1 August 2023).

3. Kahouli, B.; Hamdi, B.; Nafla, A.; Chabaane, N. Investigating the Relationship between ICT, Green Energy, Total Factor Productivity, and Ecological Footprint: Empirical Evidence from Saudi Arabia. *Energy Strateg. Rev.* **2022**, *42*, 100871. [CrossRef]
4. Almulhim, A.I. Understanding Public Awareness and Attitudes toward Renewable Energy Resources in Saudi Arabia. *Renew. Energy* **2022**, *192*, 572–582. [CrossRef]
5. Sharma, S.; Sood, Y.R.; Sharma, N.K.; Bajaj, M.; Zawbaa, H.M.; Turky, R.A.; Kamel, S. Modeling and Sensitivity Analysis of Grid-Connected Hybrid Green Microgrid System. *Ain Shams Eng. J.* **2022**, *13*, 101679. [CrossRef]
6. Come Zebra, E.I.; van der Windt, H.J.; Nhumaio, G.; Faaij, A.P.C. A Review of Hybrid Renewable Energy Systems in Mini-Grids for off-Grid Electrification in Developing Countries. *Renew. Sustain. Energy Rev.* **2021**, *144*, 111036. [CrossRef]
7. Wu, Y.; Wu, Y.; Cimen, H.; Vasquez, J.C.; Guerrero, J.M. Towards Collective Energy Community: Potential Roles of Microgrid and Blockchain to Go beyond P2P Energy Trading. *Appl. Energy* **2022**, *314*, 119003. [CrossRef]
8. Panda, S.; Mohanty, S.; Rout, P.K.; Sahu, B.K. A Conceptual Review on Transformation of Micro-grid to Virtual Power Plant: Issues, Modeling, Solutions, and Future Prospects. *Int. J. Energy Res.* **2022**, *46*, 7021–7054. [CrossRef]
9. Hirsch, A.; Parag, Y.; Guerrero, J. Microgrids: A Review of Technologies, Key Drivers, and Outstanding Issues. *Renew. Sustain. Energy Rev.* **2018**, *90*, 402–411. [CrossRef]
10. Al-Shetwi, A.Q. Sustainable Development of Renewable Energy Integrated Power Sector: Trends, Environmental Impacts, and Recent Challenges. *Sci. Total Environ.* **2022**, *822*, 153645. [CrossRef]
11. Ghiasi, M.; Niknam, T.; Wang, Z.; Mehrandezh, M.; Dehghani, M.; Ghadimi, N. A Comprehensive Review of Cyber-Attacks and Defense Mechanisms for Improving Security in Smart Grid Energy Systems: Past, Present and Future. *Electr. Power Syst. Res.* **2023**, *215*, 108975. [CrossRef]
12. Alam, S.; Shuaib, M.; Khan, W.Z.; Garg, S.; Kaddoum, G.; Hossain, M.S.; Zikria, Y. Bin Blockchain-Based Initiatives: Current State and Challenges. *Comput. Netw.* **2021**, *198*, 108395. [CrossRef]
13. Alam, S. Security Concerns in Smart Agriculture and Blockchain-Based Solution. In Proceedings of the 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON), Raigarh, India, 8–10 February 2023; pp. 1–6.
14. Guo, Y.; Wan, Z.; Cheng, X. When Blockchain Meets Smart Grids: A Comprehensive Survey. *High-Confid. Comput.* **2022**, *2*, 100059. [CrossRef]
15. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A Blockchain-Based Smart Grid: Towards Sustainable Local Energy Markets. *Comput. Sci. Dev.* **2018**, *33*, 207–214. [CrossRef]
16. 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] [PubMed]
17. Yahaya, A.S.; Javaid, N.; Alzahrani, F.A.; Rehman, A.; Ullah, I.; Shahid, A.; Shafiq, M. Blockchain Based Sustainable Local Energy Trading Considering Home Energy Management and Demurrage Mechanism. *Sustainability* **2020**, *12*, 3385. [CrossRef]
18. van Leeuwen, G.; AlSkaif, T.; Gibescu, M.; van Sark, W. An Integrated Blockchain-Based Energy Management Platform with Bilateral Trading for Microgrid Communities. *Appl. Energy* **2020**, *263*, 114613. [CrossRef]
19. Zia, M.F.; Benbouzid, M.; Elbouchikhi, E.; Muyeen, S.M.; Techato, K.; Guerrero, J.M. Microgrid Transactive Energy: Review, Architectures, Distributed Ledger Technologies, and Market Analysis. *IEEE Access* **2020**, *8*, 19410–19432. [CrossRef]
20. Kavousi-Fard, A.; Almutairi, A.; Al-Sumaiti, A.; Farughian, A.; Alyami, S. An Effective Secured Peer-to-Peer Energy Market Based on Blockchain Architecture for the Interconnected Microgrid and Smart Grid. *Int. J. Electr. Power Energy Syst.* **2021**, *132*, 107171. [CrossRef]
21. Du, X.; Qi, Y.; Chen, B.; Shan, B.; Liu, X. The Integration of Blockchain Technology and Smart Grid: Framework and Application. *Math. Probl. Eng.* **2021**, *2021*, 9956385. [CrossRef]
22. Tsao, Y.-C.; Thanh, V.-V. Toward Sustainable Microgrids with Blockchain Technology-Based Peer-to-Peer Energy Trading Mechanism: A Fuzzy Meta-Heuristic Approach. *Renew. Sustain. Energy Rev.* **2021**, *136*, 110452. [CrossRef]
23. Wang, X.; Liu, P.; Ji, Z. Trading Platform for Cooperation and Sharing Based on Blockchain within Multi-Agent Energy Internet. *Glob. Energy Interconnect.* **2021**, *4*, 384–393. [CrossRef]
24. Tsao, Y.-C.; Vu, T.-L. A Decentralized Microgrid Considering Blockchain Adoption and Credit Risk. *J. Oper. Res. Soc.* **2022**, *73*, 2116–2128. [CrossRef]
25. Younes, Z.; Alhamrouni, I.; Mekhilef, S.; Khan, M.R.B. Blockchain Applications and Challenges in Smart Grid. In Proceedings of the 2021 IEEE Conference on Energy Conversion (CENCON), Virtual, 25 October 2021; pp. 208–213.
26. Agung, A.A.G.; Handayani, R. Blockchain for Smart Grid. *J. King Saud Univ. Inf. Sci.* **2022**, *34*, 666–675. [CrossRef]
27. Dinesha, D.L.; Balachandra, P. Conceptualization of Blockchain Enabled Interconnected Smart Microgrids. *Renew. Sustain. Energy Rev.* **2022**, *168*, 112848. [CrossRef]
28. Yang, J.; Dai, J.; Gooi, H.B.; Nguyen, H.D.; Wang, P. Hierarchical Blockchain Design for Distributed Control and Energy Trading Within Microgrids. *IEEE Trans. Smart Grid* **2022**, *13*, 3133–3144. [CrossRef]
29. Meng, Q.; Berntzen, L.; Vesin, B.; Johannessen, M.R.; Oprea, S.; Bara, A. *Blockchain Applications in Smart Grid A Review and a Case Study BT Information Systems*; Themistocleous, M., Papadaki, M., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 130–149.

30. Shukla, S.; Thakur, S.; Hussain, S.; Breslin, J.G. *A Blockchain-Enabled Fog Computing Model for Peer-To-Peer Energy Trading in Smart Grid BT Blockchain and Applications*; Prieto, J., Partida, A., Leitão, P., Pinto, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 14–23.
31. Singh, R.; Akram, S.V.; Gehlot, A.; Buddhi, D.; Priyadarshi, N.; Twala, B. Energy System 4.0: Digitalization of the Energy Sector with Inclination towards Sustainability. *Sensors* **2022**, *22*, 6619. [CrossRef] [PubMed]
32. Cao, Y.-N.; Wang, Y.; Ding, Y.; Guo, Z.; Wu, Q.; Liang, H. Blockchain-Empowered Security and Privacy Protection Technologies for Smart Grid. *Comput. Stand. Interfaces* **2023**, *85*, 103708. [CrossRef]
33. Suthar, S.; Cherukuri, S.H.C.; Pindoriya, N.M. Peer-to-Peer Energy Trading in Smart Grid: Frameworks, Implementation Methodologies, and Demonstration Projects. *Electr. Power Syst. Res.* **2023**, *214*, 108907. [CrossRef]
34. Waseem, M.; Adnan Khan, M.; Goudarzi, A.; Fahad, S.; Sajjad, I.A.; Siano, P. Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenges. *Energies* **2023**, *16*, 820. [CrossRef]
35. Yoldaş, Y.; Önen, A.; Muyeen, S.M.; Vasilakos, A.V.; Alan, I. Enhancing Smart Grid with Microgrids: Challenges and Opportunities. *Renew. Sustain. Energy Rev.* **2017**, *72*, 205–214. [CrossRef]
36. Shuaib, M.; Bhatia, S.; Alam, S.; Masih, R.K.; Alqahtani, N.; Basheer, S.; Alam, M.S. An Optimized, Dynamic, and Efficient Load-Balancing Framework for Resource Management in the Internet of Things (IoT) Environment. *Electronics* **2023**, *12*, 1104. [CrossRef]
37. Baimel, D.; Tapuchi, S.; Baimel, N. Smart Grid Communication Technologies-Overview, Research Challenges and Opportunities. In Proceedings of the 2016 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), Capri, Italy, 22–24 June 2016; pp. 116–120.
38. Taha, M.Q. Advantages and Recent Advances of Smart Energy Grid. *Bull. Electr. Eng. Inform.* **2020**, *9*, 1739–1746. [CrossRef]
39. Jaradat, M.; Jarrah, M.; Bousselham, A.; Jararweh, Y.; Al-Ayyoub, M. The Internet of Energy: Smart Sensor Networks and Big Data Management for Smart Grid. *Procedia Comput. Sci.* **2015**, *56*, 592–597. [CrossRef]
40. Guerrero, J.M.; Chandorkar, M.; Lee, T.-L.; Loh, P.C. Advanced Control Architectures for Intelligent Microgrids—Part I: Decentralized and Hierarchical Control. *IEEE Trans. Ind. Electron.* **2012**, *60*, 1254–1262. [CrossRef]
41. Platt, G.; Berry, A.; Cornforth, D. What Role for Microgrids? In *Smart Grid*; Elsevier: Amsterdam, The Netherlands, 2012; pp. 185–207.
42. Chaudhary, G.; Lamb, J.J.; Burheim, O.S.; Austbø, B. Review of Energy Storage and Energy Management System Control Strategies in Microgrids. *Energies* **2021**, *14*, 4929. [CrossRef]
43. Shayeghi, H.; Shahryari, E.; Moradzadeh, M.; Siano, P. A Survey on Microgrid Energy Management Considering Flexible Energy Sources. *Energies* **2019**, *12*, 2156. [CrossRef]
44. Dey, B.; Misra, S.; Marquez, F.P.G. Microgrid System Energy Management with Demand Response Program for Clean and Economical Operation. *Appl. Energy* **2023**, *334*, 120717. [CrossRef]
45. Arefifar, S.A.; Ordonez, M.; Mohamed, Y.A.-R.I. Energy Management in Multi-Microgrid Systems—Development and Assessment. *IEEE Trans. Power Syst.* **2016**, *32*, 910–922. [CrossRef]
46. Shafiullah, M.; Refat, A.M.; Haque, M.E.; Chowdhury, D.M.H.; Hossain, M.S.; Alharbi, A.G.; Alam, M.S.; Ali, A.; Hossain, S. Review of Recent Developments in Microgrid Energy Management Strategies. *Sustainability* **2022**, *14*, 14794. [CrossRef]
47. Liu, Y.; Ning, P.; Reiter, M.K. False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 1–33. [CrossRef]
48. Alam, S.; Mohammad, O.K.J.; Alfurhood, B.S.; Saxena Kuldeep, K.; Anand, M.; Mahaveerakannan, R.; Savitha, V. Effective Sound Detection System in Commercial Car Vehicles Using Msp430 Launchpad Development. *Multimed. Tools Appl.* **2023**. [CrossRef]
49. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Reza Ahrabi, R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2020**, *14*, 27. [CrossRef]
50. Sui, T.; Mo, Y.; Marelli, D.; Sun, X.; Fu, M. The Vulnerability of Cyber-Physical System Under Stealthy Attacks. *IEEE Trans. Automat. Contr.* **2021**, *66*, 637–650. [CrossRef]
51. Pinto, S.J.; Siano, P.; Parente, M. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies* **2023**, *16*, 1651. [CrossRef]
52. Mohammadi, Z.; Pinto, S.J.; Panda, G.; Thokchom, S. A Survey of Cyber Security in Smart Microgrid. In *Sustainable Energy and Technological Advancements: Proceedings of ISSETA 2021*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 687–698.
53. Mazhar, T.; Irfan, H.M.; Khan, S.; Haq, I.; Ullah, I.; Iqbal, M.; Hamam, H. Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods. *Futur. Internet* **2023**, *15*, 83. [CrossRef]
54. Hasan, M.K.; Habib, A.K.M.A.; Shukur, Z.; Ibrahim, F.; Islam, S.; Razzaque, M.A. Review on Cyber-Physical and Cyber-Security System in Smart Grid: Standards, Protocols, Constraints, and Recommendations. *J. Netw. Comput. Appl.* **2023**, *209*, 103540. [CrossRef]
55. Alam, S.; Bhatia, S.; Shuaib, M.; Khubrani, M.M.; Alfayez, F.; Malibari, A.A.; Ahmad, S. An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring. *Sustainability* **2023**, *15*, 5660. [CrossRef]
56. Takiddin, A.; Rath, S.; Ismail, M.; Sahoo, S. Data-Driven Detection of Stealth Cyber-Attacks in DC Microgrids. *IEEE Syst. J.* **2022**, *16*, 6097–6106. [CrossRef]

57. Whitehead, D.E.; Owens, K.; Gammel, D.; Smith, J. Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies. In Proceedings of the 2017 70th Annual Conference for Protective Relay Engineers (CPRE), College Station, TX, USA, 3–6 April 2017; pp. 1–8.
58. Kshetri, N.; Voas, J. Hacking Power Grids: A Current Problem. *Computer* **2017**, *50*, 91–95. [CrossRef]
59. Pieterse, H. The Cyber Threat Landscape in South Africa: A 10-Year Review. *Afr. J. Inf. Commun.* **2021**, *28*, 1–21. [CrossRef]
60. Hemsley, K.; Fisher, R. A History of Cyber Incidents and Threats Involving Industrial Control Systems. In Proceedings of the Critical Infrastructure Protection XII: 12th IFIP WG 11.10 International Conference, ICCIP 2018, Arlington, VA, USA, 12–14 March 2018; Revised Selected Papers 12. Springer: Berlin/Heidelberg, Germany, 2018; pp. 215–242.
61. Smith, R. US Risks National Blackout from Small-Scale Attack. *Wall Str. J.* **2014**, *12*. Available online: https://maxenergysystems.com/pdf/March-12-2014-U.S-Risks-National-Blackout-From-Small-Scale-Attack.pdf (accessed on 1 August 2023).
62. Hobbs, A. The Colonial Pipeline Hack: Exposing Vulnerabilities in Us Cybersecurity. In *SAGE Business Cases*; SAGE Publications: Thousand Oaks, CA, USA, 2021; ISBN 1529789761.
63. Alkhadra, R.; Abuzaid, J.; AlShammari, M.; Mohammad, N. Solar Winds Hack: In-Depth Analysis and Countermeasures. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, Kharagpur, India, 6–8 July 2021; pp. 1–7.
64. Bose, D.B.; Rahman, A.; Shamim, S.I. 'Under-Reported' Security Defects in Kubernetes Manifests. In Proceedings of the 2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS), Virtual, 16 May 2022; pp. 9–12.
65. Johns, S. Sandworms and Computer Worms: An Assessment of American Critical Infrastructure Cyber Vulnerabilities and the Russian Federation's Growing Offensive Capabilities. Bachelor's Thesis, University of Mississippi, University, MS, USA, 2022.
66. Kiesel, K.; Deep, T.; Flaherty, A.; Bhunia, S. Analyzing Multi-Vector Ransomware Attack on Accellion File Transfer Appliance Server. In Proceedings of the 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech), Bol and Split, Croatia, 5–8 July 2022; pp. 1–6.
67. Zheng, T.; Liu, M.; Puthal, D.; Yi, P.; Wu, Y.; He, X. Smart Grid: Cyber Attacks, Critical Defense Approaches, and Digital Twin. *arXiv* **2022**, arXiv:2205.11783.
68. Baram, G. A Sliding Scale of Secrecy: Toward a Better Understanding of the Role of Publicity in Offensive Cyber Operations. *J. Cyber Policy* **2023**, *7*, 275–293. [CrossRef]
69. Khubrani, M.M.; Alam, S. A Detailed Review of Blockchain-Based Applications for Protection against Pandemic like COVID-19. *TELKOMNIKA Telecommun. Comput. Electron. Control* **2021**, *19*, 1185–1196. [CrossRef]
70. Kim, G.; Park, J.; Ryou, J. A Study on Utilization of Blockchain for Electricity Trading in Microgrid. In Proceedings of the 2018 IEEE International Conference on Big Data and Smart Computing (BigComp), Shanghai, China, 15–17 January 2018; pp. 743–746.
71. Jansen, M.; Duffy, C.; Green, T.C.; Staffell, I. Island in the Sea: The Prospects and Impacts of an Offshore Wind Power Hub in the North Sea. *Adv. Appl. Energy* **2022**, *6*, 100090. [CrossRef]
72. Orsini, L.; Kessler, S.; Wei, J.; Field, H. How the Brooklyn Microgrid and TransActive Grid Are Paving the Way to Next-Gen Energy Markets. In *The Energy Internet*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 223–239.
73. Umayam, M.L. Possibilities of Blockchain Technology for Nuclear Security. In *Blockchain for International Security: The Potential of Distributed Ledger Technology for Nonproliferation and Export Controls*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 55–73.
74. da Conceição, N. Blockchain for EV Management. Ph.D. Thesis, Haute Ecole de Gestion & Tourisme, Sierre, Switzerland, 2019.
75. Akagi, J. *Citizen Participation for Solar Energy Development in the EU–Case Study from Vienna, Austria*; Institute for Global Environmental Strategies: Fukuoka, Japan, 2023.
76. Livingston, D.; Sivaram, V.; Freeman, M.; Fiege, M. Applying Blockchain Technology to Electric Power Systems. 2018. Available online: http://www.jstor.org/stable/resrep21340 (accessed on 1 August 2023).
77. Nasrat, L.; Zedan, M.; Ali, A.-A.; Shabib, G. Review on Energy Trading of Community-Based Projects around the World. In Proceedings of the 2022 23rd International Middle East Power Systems Conference (MEPCON), Cairo, Egypt, 13–15 December 2022; pp. 1–8.
78. Li, D.; Bae, J.-H.; Rishi, M. A Preference Analysis for a Peer-to-Peer (P2P) Electricity Trading Platform in South Korea. *Energies* **2022**, *15*, 7973. [CrossRef]
79. Yap, K.Y.; Chin, H.H.; Klemeš, J.J. Blockchain Technology for Distributed Generation: A Review of Current Development, Challenges and Future Prospect. *Renew. Sustain. Energy Rev.* **2023**, *175*, 113170. [CrossRef]
80. Basova, A. V Blockchain as a Platform to Digitally Transform the Electricity Sector. In Proceedings of the IOP Conference Series: Earth and Environmental Science; IOP Publishing: Bristol, UK, 2022; Volume 990, p. 12056.
81. Li, P.; Ng, J.; Lu, Y. Accelerating the Adoption of Renewable Energy Certificate: Insights from a Survey of Corporate Renewable Procurement in Singapore. *Renew. Energy* **2022**, *199*, 1272–1282. [CrossRef]
82. Dukovska, I.; Slootweg, J.G.; Paterakis, N.G. Decentralized Coordination of a Community of Electricity Prosumers via Distributed MILP. *IEEE Trans. Power Syst.* **2021**, *36*, 5578–5589. [CrossRef]
83. Brousmichc, K.-L.; Anoaica, A.; Dib, O.; Abdellatif, T.; Deleuze, G. Blockchain Energy Market Place Evaluation: An Agent-Based Approach. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 321–327.

84. Saraji, S. Blockchain and Sustainable Energy. In *Sustainable Oil and Gas Using Blockchain*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 121–143.
85. Harvey, M.; Long, D.; Reinhard, K. Visualizing Nistir 7628, Guidelines for Smart Grid Cyber Security. In Proceedings of the 2014 Power and Energy Conference at Illinois (PECI), IEEE, Champaign, IL, USA, 28 February–1 March 2014; pp. 1–8.
86. Christensen, D.; Martin, M.; Gantumur, E.; Mendrick, B. Risk Assessment at the Edge: Applying NERC CIP to Aggregated Grid-Edge Resources. *Electr. J.* **2019**, *32*, 50–57. [CrossRef]
87. Uslar, M.; Specht, M.; Dänekas, C.; Trefke, J.; Rohjans, S.; González, J.M.; Rosinger, C.; Bleiker, R.; Rosinger, C.; Uslar, M. Smart Grid Security: Iec 62351 and Other Relevant Standards. In *Standardization in Smart Grids: Introduction to IT-Related Methodologies, Architectures and Standards*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 129–146.
88. Leszczyna, R.; Leszczyna, R. Cybersecurity Standards Applicable to the Electricity Sector. In *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 59–86.
89. Guo, Y.; Wang, J. New Cybersecurity Standards for IACS of the Nuclear Power Industry in China. In Proceedings of the 7th GI/ACM I4.0 Workshop on Industrial Automation and Control Systems, Virtually, 28 September 2022.
90. Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2. May 2015. Available online: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf (accessed on 4 August 2023).
91. Wang, F.; Yan, Z.; Luan, Y.; Zhang, H. Blockchain Adoption and Security Management of Large Scale Industrial Renewable-Based Systems: Knowledge-Based Approach. *J. Innov. Knowl.* **2023**, *8*, 100328. [CrossRef]
92. Choobineh, M.; Arabnya, A.; Sohrabi, B.; Khodaei, A.; Paaso, A. Blockchain Technology in Energy Systems: A State-of-the-art Review. *IET Blockchain* **2023**, *3*, 35–59. [CrossRef]
93. Moudgil, V.; Hewage, K.; Hussain, S.A.; Sadiq, R. Integration of IoT in Building Energy Infrastructure: A Critical Review on Challenges and Solutions. *Renew. Sustain. Energy Rev.* **2023**, *174*, 113121. [CrossRef]