Article

EPS-Ledger: Blockchain Hyperledger Sawtooth-Enabled Distributed Power Systems Chain of Operation and Control Node Privacy and Security

Abdullah Ayub Khan [1,2], **Asif Ali Laghari** [1,*], **De-Sheng Liu** [3,*], **Aftab Ahmed Shaikh** [1], **Dan-Dan Ma** [3], **Chao-Yang Wang** [3] and **Asif Ali Wagan** [1]

1   Department of Computer Science, Sindh Madressatul Islam University, Karachi 74000, Sindh, Pakistan; abdullah.khan00763@gmail.com (A.A.K.); aftab.shaikh@smiu.edu.pk (A.A.S.); asif.wagan@smiu.edu.pk (A.A.W.)
2   Research Lab of AI and Information Security, Faculty of Computing Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi 75660, Sindh, Pakistan
3   College of Information and Electronic Technology, Jiamusi University, Jiamusi 154007, China; madandan@jmsu.edu.cn (D.-D.M.); wangchaoyang@jmsu.edu.cn (C.-Y.W.)
*   Correspondence: asif.laghari@smiu.edu.pk (A.A.L.); desheng.liu@jmsu.edu.cn (D.-S.L.)

Abstract: A distributed power system operation and control node privacy and security are attractive research questions that deliver electrical energy systems to the participating stakeholders without being physically connected to the grid system. The increased use of renewable energy in the power grid environment creates serious issues, for example, connectivity, transmission, distribution, control, balancing, and monitoring volatility on both sides. This poses extreme challenges to tackle the entire bidirectional power flow throughout the system. To build distributed monitoring and a secure control operation of node transactions in the real-time system that can manage and execute power exchanging and utilizing, balancing, and maintaining energy power failure. This paper proposed a blockchain Hyperledger Sawtooth enabling a novel and secure distributed energy transmission node in the EPS-ledger network architecture with a robust renewable power infiltration. The paper focuses on a cyber-physical power grid control and monitoring system of renewable energy and protects this distributed network transaction on the blockchain and stores a transparent digital ledger of power. The Hyperledger Sawtooth-enabled architecture allows stakeholders to exchange information related to power operations and control monitoring in a private ledger network architecture and investigate the different activities, preserved in the interplanetary file systems. Furthermore, we design, create, and deploy digital contracts of the cyber–physical energy monitoring system, which allows interaction between participating stakeholders and registration and presents the overall working operations of the proposed architecture through a sequence diagram. The proposed solution delivers integrity, confidentiality, transparency, availability, and control access of the distribution of the power system and maintains an immutable operations and control monitoring ledger by secure blockchain technology.

Keywords: blockchain; Hyperledger Sawtooth; smart contract; power systems; chain of operation and control; distributed node privacy and security

1. Introduction

Nowadays, energy crises are emerging as a significant challenge in the supply of power resources to the economy. It has been impacted radically because of localization-based shortages, a restricted fuel supply and demand, over-consumption, nationalization, regulation of energy companies, market failure, shallow infrastructure, and affected by the social and political environment [1]. According to the annual survey of IEA Global Energy Review 2019–2020, the current uncertain situation has an impact on public health, economy,

and, hence, energy; the share of energy exposed to the control measures jumped from 5% to 50% [2], unlike energy use and carbon dioxide emission which have dropped down an average percentage of 25 because of partial and complete lockdowns [2]. The energy data collection for thirty countries until April 2020 showed a two-thirds energy demand decline in the first quarter of the 2020 lockdown by a demand depression of 3.8%. Therefore, global coal, oil, gas, and electricity demands have decreased [3]. The only source that posts growth in demand is renewable energy and power systems. Undoubtedly, these systems requires more installation capacity but a one-time investment along with a priority dispatch.

With the increased use of renewable resources, most of the two energy resources are used, such as solar and wind, which are now in the process of creating large and small productions and a scalability of power generation [4]. Therefore, the requirement is effectively increasing, and the use of advanced control techniques and procedures to work in a microgrid system are makeable. In the last scale of energy production, the operation and control of the system cover the principles involving energy conversion and prominent renewable sources, including the fluid mechanics theory and thermodynamics [5]. However, the challenging aspect is the real-time secure operation and control of distributed power systems at various scales to support a more efficient and reliable electric grid. The current central station power plant controls the electric grid with a single way of power delivery through the distributed generators and, based on this, a distributed operate and control management can handle all the transactions with advanced node communication, and provide robust performance in terms of efficiency and enhanced reliability [6]. The secure monitoring of energy and distributed power system control operations of node transactions are fully protected through a blockchain cyber-physical system. It enables the optimized operation of the system and provides a way to control the node security and preservation along with an improved resilience and more reliability.

The trade of the energy and power grid system shifted from the centralized to the distributed smart power grid system; the development of the current distributed energy business model has encountered critical bottlenecks and implementation challenges [7]. The current multimedia-enabled decentralized cloud management of energy business models is highly relying on third-party services [8]. Thus, this will cause a single point of failure; moreover, it will lead to increased operating costs, potential risk and low node transaction transparency, and a high possibility of data forgery and tampering. The third-part service level may disclose the pattern of user energy generation; on the basis of the data heuristics, where it can easily predict the daily activities of users' power operations and control system management; meanwhile, there is a lack of privacy, protection, and security shown in Figure 1. Furthermore, the market price comparison between traditional and current renewable energy systems will discourage investment in renewables [9]. Therefore, a one-way energy transmission creates disruption because of a complex power management, has more difficulty handling dynamic energy demands, and vulnerability occurs when the power supply runs out. However, the management of distributed two-way directional energy is desirable to improve the system efficiency and stability, and the renewable cost of emission requires full consideration [10].

Blockchain technology has been widely adopted as a decentralized system that provides security and privacy of distributed energy systems control operations of power node transactions [11]. The technology serves various potential advantages in cyber-physical power management and control monitoring development, such as a high node transactions transparency and an easy way to be rid of complex two-way power management, monitoring, and related vulnerabilities [12]. It would also provide the distributed blockchain-aware serverless peer-to-peer (P2P) network with microgrids of renewable energy; blockchain-enabled development can cover several gray areas, including technological, economic, social, and environmental dimensions. Furthermore, there is no additional cost for permanence, and a high level of privacy security pertinent to store energy-related information and control accessibility [13]. For instance, the modular blockchain business models (consortium), including the Hyperledger Sawtooth, act as a permissioned private distributed

network architecture. The Hyperledger Sawtooth-based customized (programable) smart contracts guaranteed by blockchain, automate rule-based transactions execution and security. It also allows to design and create a seamless hash encryption, which supports the general-purpose programming language for maintaining a trustable private network and pluggable consensus protocols effectively and efficiently. Through the experiment, the hash-encrypted power node transaction is formed in chronological order and it achieves various benefits in the domain of distributed energy management and control, such as reducing the peak load, increasing economic savings, market trading efficiency, and avoiding third-part administrative barriers and authenticity.
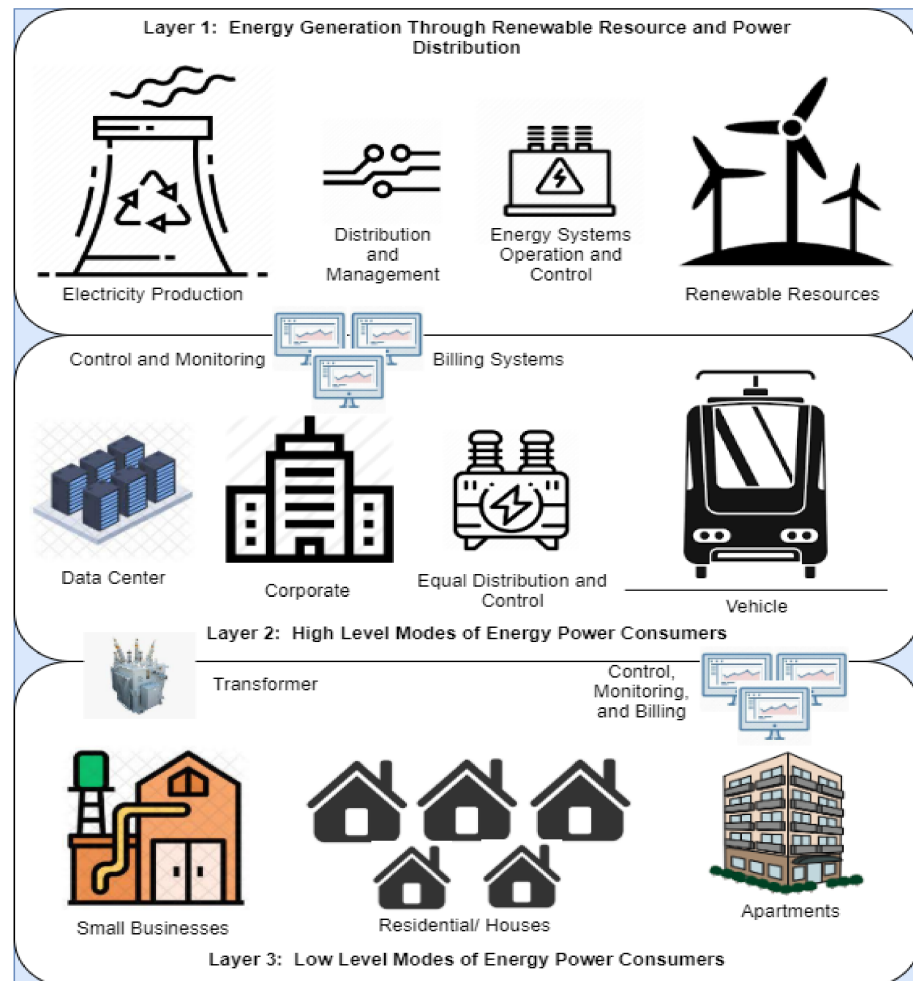

Figure 1. Traditional unsecure centralized energy power grid systems operation and control monitoring.

This study addresses the blockchain Hyperledger Sawtooth-enabled energy and power control operations systems, an emerging distributed computing technology that acts in distinct energy, power, and grid systems operation and controls management. A new way of blockchain–cyber-physical systems for monitoring distributed power operations and bidirectional energy controls and management is introduced. The blockchain-enabled secure node transactions of a power system provides immutable data entry, reliability, transparency, and establishes a trustworthiness environment between participating stakeholders and discards other vendor-related services or any third-party provider connectivity. This proposed architecture can easily track all the operations and actions of renewable energy and power systems and their control management; the main contributions of this study are as follows:

- We introduce the combination of blockchain and cyber-physical technology in the energy system, which provides transactions of power node security, data immutability, integrity, transparency, and a distributed control access and distributed monitoring. It resists the unauthorized access of system operation and control, connects stakeholders in a permissioned private network, and exchanges and transfers energy-related information in a secure transmission channel.
- In addition, we propose a novel and secure blockchain Hyperledger Sawtooth-aware serverless distributed network architecture for renewable energy and power systems chain of operations and control management to replace the current centralized system that impacts an improved performance, transparency, security, and complete provenance.
- We explain the importance of the P2P network of microgrids in renewable energy and analyze the developed blockchain-enabled security and create smart contracts (such as register(), AddNode(), and UpdateTransaction()) for secure communication and distributed monitoring.
- Finally, the consensus policy and event transitions and execution are discussed, and we highlight critical implementation challenges and limitations in the proposed EPS-ledger, along with the open research areas and future developments.

The rest of this paper is organized as follows: Section 2 discusses the related work of energy, power and grid systems operations and control, distributed node transaction privacy, and security with a blockchain Hyperledger-enabled private permissioned network architecture. Section 3 describes the existing power systems control operations and distributed monitoring, and the use of newly blockchain distributed technology-based secure cyber monitoring of the real-time environment and calculates its radical impact on the energy system. Section 4 presents the proposed the architecture of the blockchain Hyperledger Sawtooth-enabled distributed power system chain of operation and control and allows the accessibility of this system through DAPP. The next section focuses on the chain code implementation, including the consensus algorithm and protocols, the verification policy, SH-256 hash encryption, and the core system of power node transactions. Moreover, we briefly discuss the system implementation challenges and explain the working mechanism of the cyber-physical secure control monitoring transaction in the private network through a sequence diagram and compare this with other state-of-the-art models. Finally, we conclude our research paper in Section 6.

2. Literature Review

A proper supply of energy resources is one of the prime objectives of renewable energy and power management and monitoring [14]. The characteristics of the renewable energy and power systems control operations and blockchain technology are consistent. In this scenario, blockchain technology was applied to the energy system, a decentralized energy trading and control operations monitoring platform was design and maintained according to the blockchain Hyperledger-customized consensus policies and power node transactions execution verification protocols. Automated and efficient monitoring is guaranteed by the proper design and implementation of digital contracts [15]. The registered stakeholders in the permissioned private network were allowed to query transaction data in the gazette structure, where blockchain ensured the complete data transparency of the system. Moreover, blockchain technology is more feasible because of the distributed nature and decentralized platform for renewable energy systems. The data in the system were protected by a hash-encrypted SH-256 algorithm and preserved by a distributed data storage (file structure) such as interplanetary file systems (IPFS) [16]. Presently, several research methods have been proposed related to renewable energy systems, distributed operation and control, monitoring, and blockchain technology separately. We highlighted a few works of the literature and discussed (Table 1) the proposed architectural open challenges and the implementation issues are as follows:

Table 1. Blockchain Hyperledger-enabled renewable energy and power systems-related literatures.

Paper Title	Proposed Methodology	Challenges/Limitations	References
How to improve the competitiveness of distributed energy resources in China with blockchain technology	J. Hou et al. presented the current status of distributed energy resources in China first, and then used Michael Porter's force strategy to analyze the competitiveness of distributed energy resources.	• Weaknesses, opportunities, and threats of distributed blockchain-enabled energy resources are listed • Improved consensus policy and recommendation • Issues in billing and settlement	[17]
Distributed energy systems as common goods: Socio-political acceptance of renewables in intelligent microgrids	Maarten Wolsink investigated the distributed energy resources and their impact on social political acceptance, and further managed private commodity delivery in the public grid and monitoring through the P2P application.	• High diffusion of distributed energy system • Self-governing • Common pool resources theory (Ostrom's theory) • Public ledger	[18]
Distributed Energy Resources and the Application of AI, IoT, and Blockchain in Smart Grids	N. M Kumar et al. explained the modern power infrastructure based on the smart grid, the two-way flow of electricity and data between peers within the distributed electric energy power system using blockchain, IoT, and artificial intelligence (fuzzy logic).	• An additional cost of the electronics component • Permissionless distributed ledger architecture • Replacing fossil fuel conventional grid • Improved traceability	[19]
Blockchain as Key Enabling Technology for Future Electric Energy Exchange: A Vision	A. Baggio et al. proposed a blockchain enabling technology for designing and supporting grid infrastructure, a framework that addresses a decentralized energy grid platform hosted through direct participation of the coordination procedures.	• Control connectivity board for smart inventor • Platform interoperability • Regulatory compliance • Required characteristics	[20]
Ethereum Blockchain-Based Peer-To-Peer Energy Trading Platform	A. Iskakova et al. focused on the blockchain ethereum-enabled application for the energy industry, addressing the potential challenges and limitations of distributed energy resources and reliable transactive energy management (P2P).	• Integration of transactive management and multilevel agent • Public ledger network • Ethereum smart contract through operation and control, monitoring and energy trading	[21]
Smart contract for distributed energy trading in virtual power plants based on blockchain	J. Lu et al. proposed a blockchain-enabled distributed architecture for virtual power plants and energy internet for real-time electricity prices and monitoring. In addition, the analysis of the supply and demand information was conducted in real time, so that bidirectional selection could be carried out, and this distributed energy was connected to the grid.	• Whisper protocol used in the P2P • Proof-of-Stake (coinage) • SHA-3 • Permissionless network	[22]
Blockchain for energy sharing and trading in distributed prosumer communities	I. Petri et al. demonstrated how blockchains can be utilized and support the formation of energy systems. Design and implement a blockchain-enabled framework and smart contract that manages energy node transactions and energy-related information exchanges in a community of prosumers; moreover, to provide a more secure energy trading environment between producers and consumers.	• Ethereum model • Public ledger • Permissionless network (P2P)	[23]

Table 1. *Cont.*

Paper Title	Proposed Methodology	Challenges/Limitations	References
Blockchain-Integrated Virtual Power Plant Demonstration	A. Mnatsakanyan et al. proposed a blockchain-enabled mechanism that handles energy transactions with a virtual power plant on a distributed ledger along with complete data transparency. Moreover, they developed the management of grid digitalized and enabled new distributed applications in power systems.	• Increase the security cost by smart grid • Risk of controlling the aggregated distributed energy resources • Ethereum-based architecture • Public network	[24]

The blockchain Hyperledger is an open-source community that focuses on the development of a suite of stable architectures, programming libraries, frameworks, tools, and security patches for small and large business deployments [25,26]. For our solution, we chose a Hyperledger Sawtooth platform. This technology offers a flexible modular framework that separates the core system of power systems from the distributed application domain [27]; this Hyperledger provides benefits for building, deploying, and running a distributed solution for the cyber-physical power systems' chain of operation and control monitoring [28,29]. Sawtooth implements secure node transaction-based updates to the shared power control state between stakeholders in the private permissioned network by a consensus algorithm [30]. It segregates power system core ledgers from the application domain environment; thereby, the Sawtooth-enabled distributed applications of power systems are simply developed to keep the record safe and secure [31–33]. Sawtooth demonstrates the complete periphery of the system; this system operates the power, run, and host without interfering with the core distributed EPS-ledger. This core power system logic was required for the secure cyber-physical control monitoring shown in Figure 2. Furthermore, we designed and ran as a smart contract virtual machine based on a self-governing mechanism, created transactional rules, consensus policy, defined permissioned network authentication, and notified and executed digital contracts between various stakeholders in the chain-like chronological order.
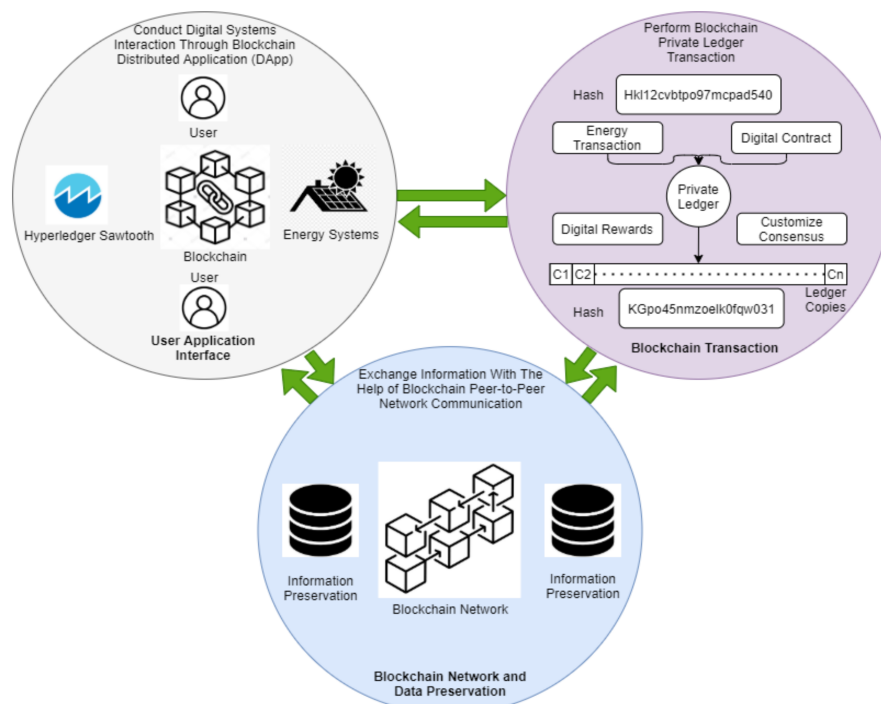

Figure 2. Blockchain Hyperledger Sawtooth-enabled secure EPS-ledger distributed node transaction.

3. The Existing Power Systems Control Operations and Monitoring with Blockchain-Cyber-Physical System

The current power systems have transformed from centralized to distributed; the main objective was to maintain a continuous power supply with a high-quality acceptance to consumers of the systems [25,33]. Therefore, the system was set to be the equilibrium when the supply and generation of power were in the balance condition as shown in Figure 3. Modern energy power systems are complex structures and spread in a large geographical area. Due to an increasing demand and industrial growth, a new trend in this technology emerged that needs to be considered while operating and planning, such as active power and reactive power control, power transfer, voltage stability, controlled frequency and load balancing, quality, and auto-electric generation. Moreover, multimachine systems, a competitive environment, reliability, billing, and settlement monitoring, are crucial aspects of the operation and control of the power system [26,32,33]. However, this system becomes unstable if it is subjected to faults. To determine the stability and security of the system, we had to study and analyze the state of the system. Recently, the current energy systems faced most of the faults; the unsymmetric faults of power systems are the main issue, including ground line, double line, and line-to-ground faults [27,31].
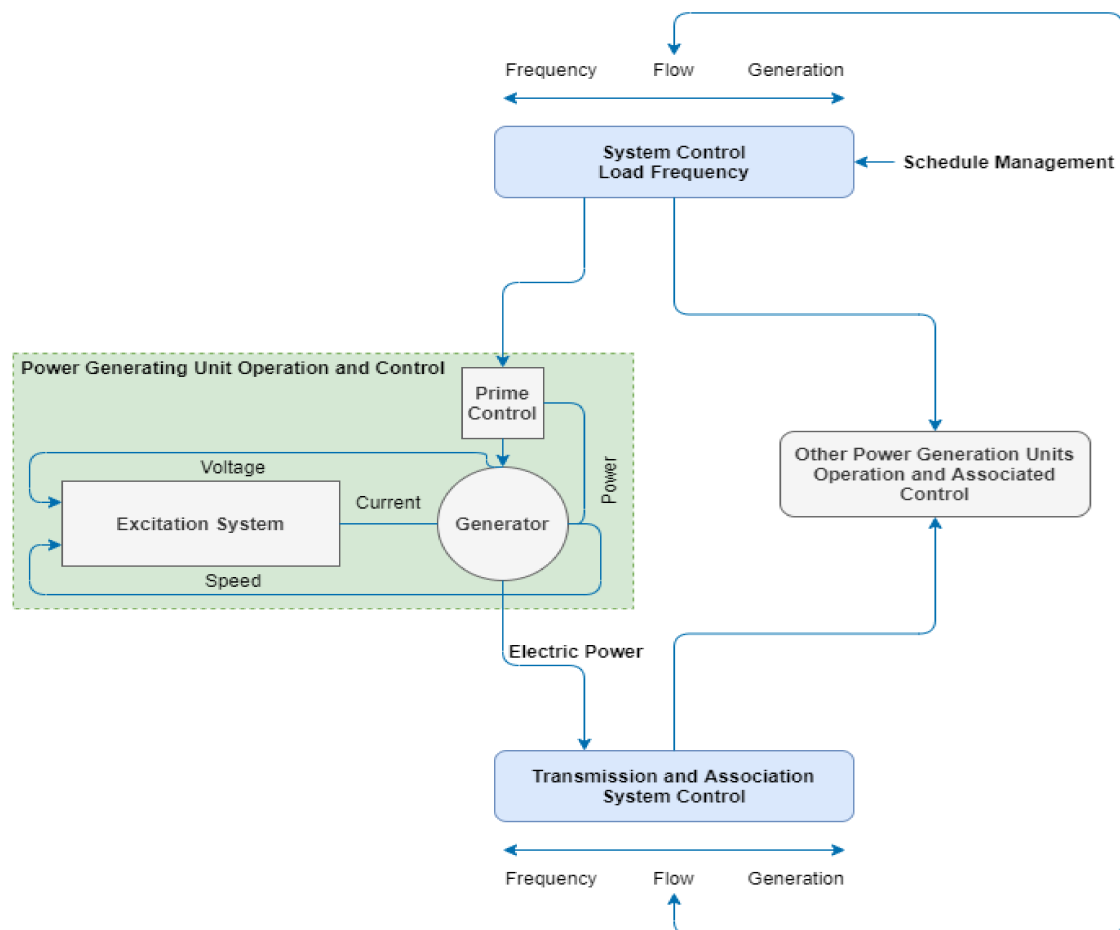

Figure 3. Presented is the working of current renewable power grid systems operation and control monitoring.

3.1. Energy Systems and Blockchain Hyperledger Sawtooth-Enabled Cyber-Physical Systems

Cyber–physical systems are a setup that controls and monitors elements of different scientific and engineering disciplines such as cybernetics, distributed control, sensor networks, embedded devices, and engineering systems and control theory [28,32]. In energy systems, the optimal integration of physical and digital components of power system operation and control maximizes the synergy between the two. Therefore, achieving signif-

icant benefits in energy systems such as cost, performance, overall power management, secure monitoring, and life-cycle sustainability [29,33]. The cyber-physical systems-enabled energy systems, hardware, and software have been performing seamless integration towards achieving well-defined tasks. These tasks are highly automated and distributed in nature (multi-agents); this trustworthiness process of collecting energy-related data in primary condition guarantees the electric power systems safe and reliable operation. Whereas cyber-physical systems collaborate with the sensors and networks embedded with an EPS-ledger to monitor and control the physical environment; we also used feedback loops that allow systems to self-activate, for example, computing, communication, and control [30,31]. Additionally, blockchain technology provides operational and control node transaction security, validates transactions, and ensures data immutability. Moreover, consensus algorithms, distributed data preservation, storage, and secure protocol, which are used to provide robustness such as performance and reliability, also eliminate the risk associated with the current energy systems operations and control monitoring.

3.2. Business Rules

It is an application program usually known as business logic and policy decision making that defines a set of assets and the transaction instructions for modifying these assets. Business rules are created and executed by peer-to-peer nodes to authenticate, facilitate, and enforce them by reading defined rules, to preserve and change other energy-related state information, and share them with participating stakeholders in the Sawtooth-permissioned network [34]. The Sawtooth business core design allows the programmable distributed application to choose the predefined transaction rules, consensus algorithms, customization, and permissions that support the proper implementation of business rules. When the condition is meet, the business rule triggers and executes; accordingly, as a result, the transaction execution in a set of assets is submitted to the permissioned network and last appended to the ledgers on all peer-to-peer nodes [35].

Presently, the power system is one of the open applicational areas where business rules are being deployed and implemented to deal with challenges, such as power management, electronic data handling, exchanging information, cyber-physical systems-enabled monitoring, and a smart and intelligent programmable controlled operation. Moreover, accessing, storing, and preserving energy-related sensitive information are serious issues in renewable energy systems. One of the main features of using these business rules in the renewable distributed energy system is the support of digital signature approvals between the participating stakeholders to execute transactions based on the agreed conditions [36]. The infrastructural cost is also reduced by using business rules, as it replaces other third-party vendor-based solutions in exchanging various transactions.

3.2.1. Peer-to-Peer (P2P) Connectivity

In a peer-to-peer network, the blockchain Hyperledger Sawtooth network has a single or multichannel peer connectivity; the main objective is to update the ledger and consist of transactional logs and states in it. Multi-channel peering in a blockchain can automatically synchronize [37]. We adopted multichannel peer connectivity for distributed power system monitoring which has two roles, either endorsed to commit or vice versa, but not both. A transaction request is submitted to the Sawtooth Engineer where it validates the ledger network with the P2P policies and enforces it to create policies for distributed energy systems.

3.2.2. Permissioning Requirements (Validated Authority)

This service manages Sawtooth requirements for permissions, including both the on-chain wide network permission and local validator configuration [32]. In the local configuration, a validated engineer can limit who is allowed to submit a request for transactions and batches directly, whereas the on-chain configuration can set up the whole network and enforce consistent permissioning rules. The validators on the Sawtooth-

permissioned network reject the redundant nodes from peers, which ensures that only known nodes can join the network [32,34]. The Sawtooth components for permission requirements that make the distributed systems more secure are as follows:

- Batch;
- Transaction and transaction processor;
- Consensus;
- Validator;
- Node;
- Client;
- Authorization procedure;
- State subscriber;
- Policy.

Moreover, we chose the blockchain Hyperledger Sawtooth platform because it provides:

- Data privacy, integrity, and confidentiality;
- Efficient processing;
- Sawtooth business rules functionality;
- Secure request submission, validation, and node transaction.

In this scenario, the involved stakeholders of renewable energy systems, distributed power operation and control, secure node transaction, and monitoring were as follows:

1. Renewable energy project developers;
2. Electric utility management;
3. Environment and Nature Land Authority;
4. Economic and Social Development Authority;
5. Other interest groups;
6. Residents and business owners;
7. Non-government organizations.

4. Proposed Blockchain Hyperledger Sawtooth-Enabled Architecture for Distribution Power Systems

In this section, we proposed a blockchain Hyperledger Sawtooth-enabled novel and secured an architecture for distributed renewable energy and power systems chain of control operations of node transactions and distributed monitoring. Figure 4 presents the EPS-ledger blockchain Hyperledger Sawtooth architecture that enabled the renewable energy systems operation, control, and management of power in the secure monitoring context, including the multimachine system, competitive environment, billing, settlement, and reliability. This architecture demonstrated the proper scenario of renewable power monitoring between various node transactions' integrity and the secure preservation in the distributed ledger; moreover, it maintained a consensus policy for update transactions and encrypted using hash SH-256 and stored these transaction updates in an IPFS distributed storage. The participating stakeholders (*register()* contract) directly accessed the IPFS storage and checked the power management details, submitted approval for the transaction, applied for the request for cyber-physical operation and controlled the monitoring and billing settlement through the distributed application (DApp). A Sawtooth engineer tackled the request of all participating stakeholders related to access records. In this regard, the engineer also handled a set of logs in the distributed storage structure and managed the energy-related data redundancy and validation challenges. Whereas the objective of the IPFS storage structure is to provide a secure preservation of renewable distributed power systems control node transaction records, it also allows for the setup of timely update transaction reporting, documenting, and exchange data among participating stakeholders.
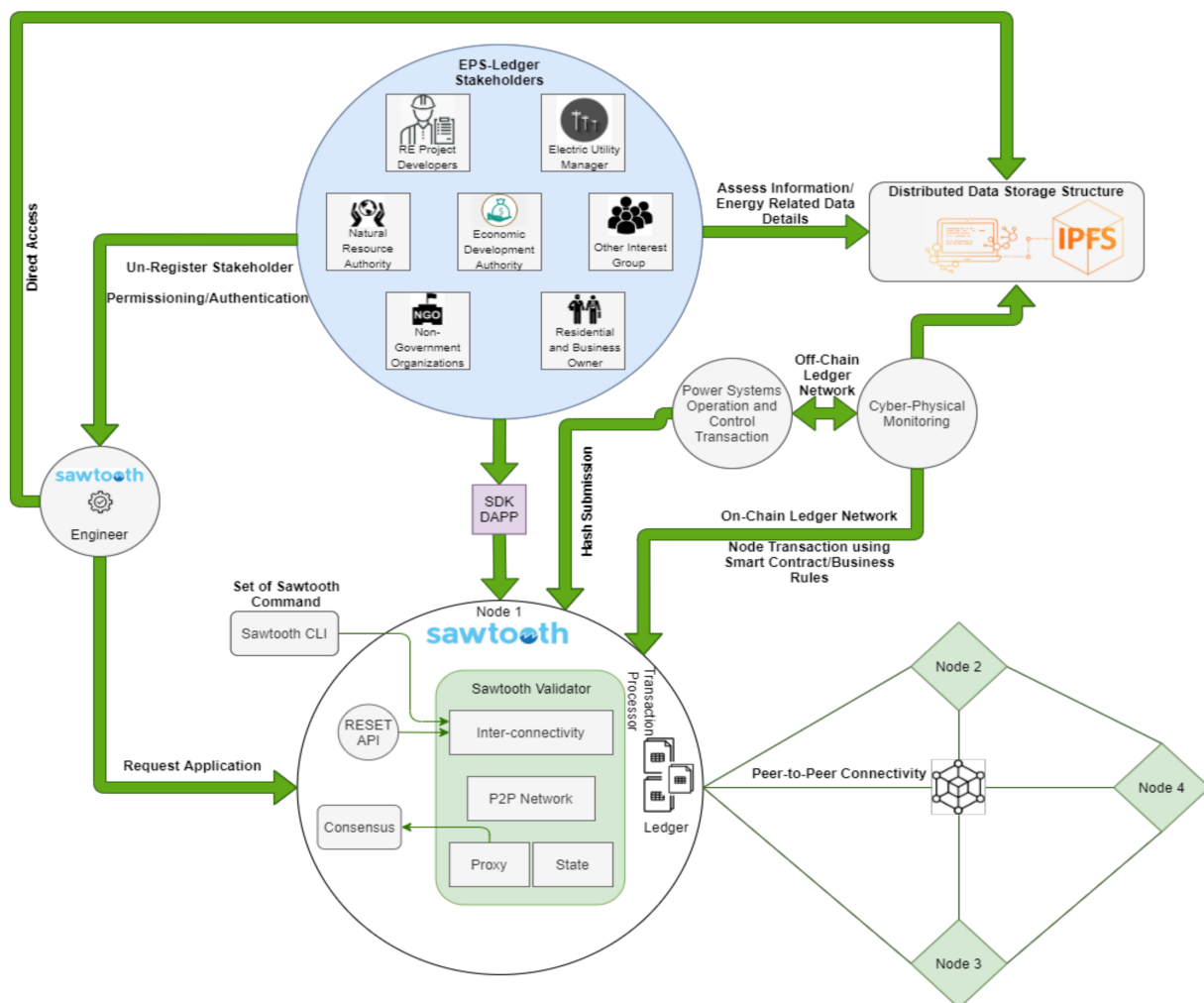
Figure 4. The proposed blockchain Hyperledger Sawtooth enables novel and secure architecture for distributed power systems control node transaction.

Through the experiment of the EPS-ledger architecture, there was an on-chain network that connected the cyber-physical control monitor system (embedded sensor network) and Sawtooth node transactions using digital contracts—ensuring operation validity, state, consensus proxy, interconnectivity, and peering between other connected hash-encrypted nodes. The off-chain connection maintained two-way communication between the cyber-physical control system and renewable power operation monitoring, analysis, active validation, and system integrity and secure node preservation. However, RESET API was used to reset nodes if it had data on them, which was not needed for the transaction process. The Sawtooth state represented the transfer API in the internet service deployment that was used to retrieve control objects. Moreover, the transaction processor (transaction ledger) investigated each record of power-related data, and Sawtooth CLI supported a set of customized commands (according to business rules) to interact with Sawtooth services. In addition, the design consensus protocol (transaction execution policy)—implemented as a separate process, a trusted execution that provides proof-of-work solutions efficiently—is shown in Figure 5. This proposed architecture provided a robust performance and supported the distributed power control, node transaction security, and ensured operation integrity, confidentiality, and distributed renewable energy systems monitoring protection.
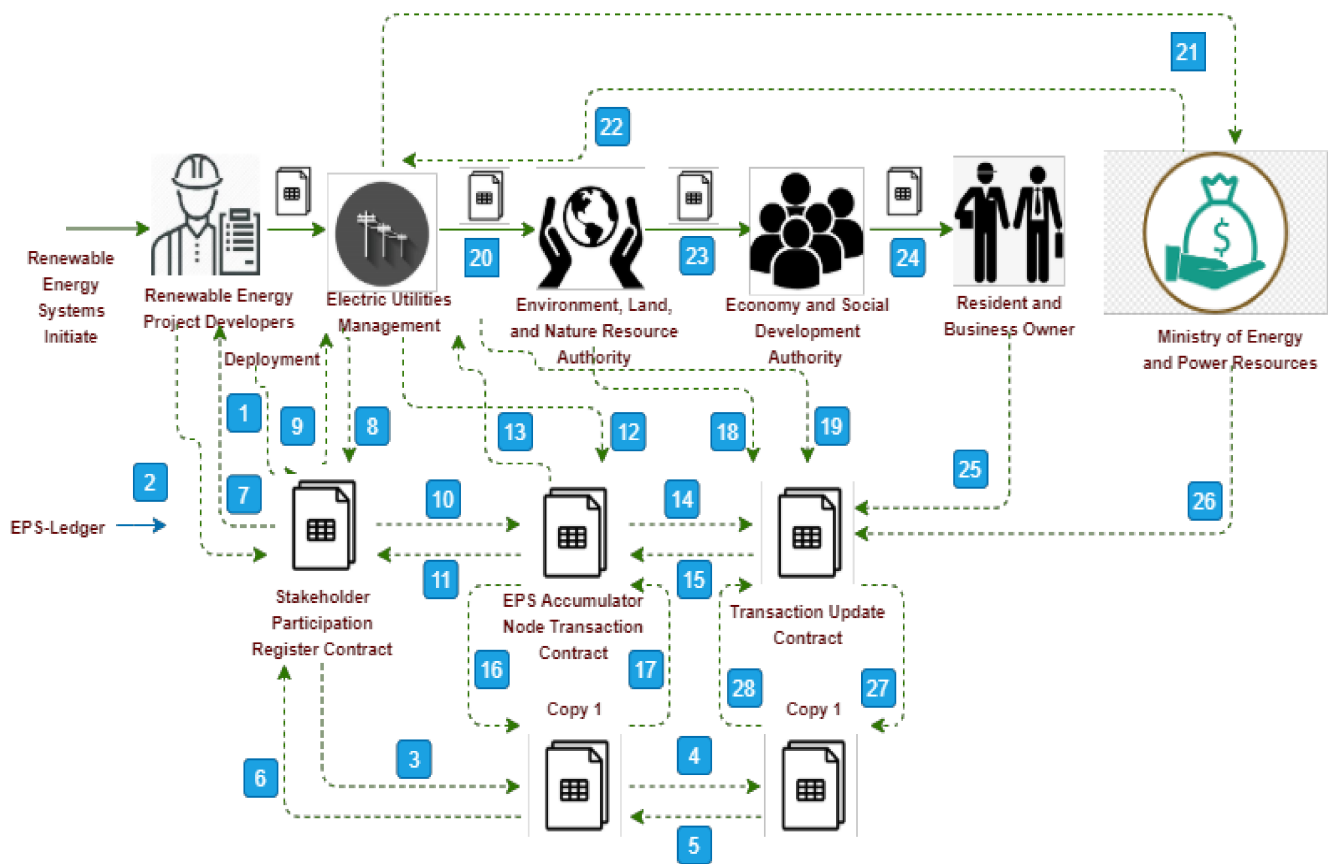
Figure 5. Event-based power node transaction execution process of the proposed blockchain Hyperledger Sawtooth-enabled distributed EPS-ledger.

4.1. Implementation of Business Rules

In this context, we designed and implemented Hyperledger Sawtooth-enabled business rules (digital contracts); there were three crucial contracts that were used for creating a distributed power system, control operations of power node transactions and execution, update, and distributed control monitoring:

- Registration contract (register() contract);
- Operation and control accumulator contract (addNode() contract);
- Transaction update contract (updateTransaction() contract).

The participating stakeholder registration contract (register()) was initiated and deployed between the Sawtooth Engineer and Renewable Energy and Power Resource ministry to authorize new participants of energy systems along with the power node operation enrolment. The register() was created to add and execute energy-related data, validated by the SE, and record participating stakeholders' transactions according to the Sawtooth predefined consensus policy tuned by the SE. Additionally, this contract also recorded more information related to participating stakeholders: stakeholderTitle, primaryStakeholders, secondaryStakeholders, names, timestamps, and other active registration steps. Once the stakeholder was registered in the distributed network ledger (register() contract), the system initiated the operation accumulator transaction contract (addNode() contract) as demonstrated in Algorithm 1.

Algorithm 1: Registration of Participating Stakeholders (register()), (registration of the participating stakeholders and validate their roles).

Input: EPS-Ledger-Sawtooth Engineer Initiate System

　　　　　tx.main(),

　　　　　renewable_energy_participanets (participationStakeholders), stakeholder title

　　　　　(stakeholderTitle), primary stakeholders, secondary stakeholders

　　　　　primaryStakeholders, name

　　　　　secondaryStakeholders, name

　　　　　name, current timestamp(execute),

　　　　　renewable energy system accumulator contract address (acAddress), stakeholder register

　　　　　stakeholderRegister, counter(stakeholderCounter)

　　　　　stakeholderRegister is responsible to authorization or set of authorization to maintain register ad-

dresses in the contract;

if　　　　tx.main() is true,

　　　　　then

　　　　　if　　　　participationStakeholders is not in the contract

　　　　　　　then

　　　　　　　changes state of the contract and add new details

　　　　　　　record participationStakeholders, stakeholderTitle, primaryStakeholders, secondaryStake-

holders, name

　　　　　　　execute,

　　　　　　　and

　　　　　　　acAddress;

　　　　　　　counter calculates the StakeholderCounter and store;

　　　　　else

　　　　　　　backtracking and state error generation

　　　　　　　end;

else

　　　　　backtracking and state error generation

　　　　　end;

The power control operations accumulator contract (addNode() contract) was deployed and the initiation of the system automatically when an event occurred was added to the contract (addNode()). This contract stored renewable power operations, control, and monitoring related information, even the related transactions recorded, and updated the accumulator contract. The addNode() was created to add a new node and execute updated information; additionally, this contract could store more relevant data such as the accumulator ID (accID), access (accNodeTransaction), timestamp, and the current operation and control information. Once the accumulator was added to the ledger network (addNode() contract), the system initiated the transaction update contract (updateTransaction() contract) as shown in Algorithm 2.

Algorithm 2: addNode() Contract, The distributed power systems chain of operation and control accumulator contract (addNode()).

Input: EPS-Transaction-Sawtooth Engineer Initiate System Addresses

         tx.main(),

         accumulator ID (accID), accumulator node transaction

         access (accNodeTransaction), current operation and control

         timestamp(execute),

         transaction of energy power operational record update contract (add Transaction Update Contract (TUC))

         EPS-Ledger Sawtooth Engineer (SE), EPS accumulator count (acCount)

         SE is a set of all authorized addresses of the energy **Sawtooth Engineer**

if   tx.main() is SE

     then

     if   accumulator node has not existed

         then

         change state of acCount, add new node transaction record;

         accID, accNodeTransaction, current operational and control, tx.main(),

         add on TUC to the blockchain distributed ledger;

         acCount is increment by a unit;

     else

         backtracking and state error generation

         end;

else

     backtracking and state error generation

     end;

The transaction update contract (updateTransaction()) is deployed and it initiated the update when new power accumulator-related information was added to the accumulator contract (addNode()). This contract shared the updated information among the participating stakeholders using permissioned authority and mentioned policy accordingly. The updated transaction record was based on the power operation and control management-related data and responded to the add-in registration contract and node accumulator contract. The updateTransaction() was created to add updated transactions and execute the update history of new power-related operation and control information in the TUC contract. Furthermore, this contract stored additional records such as assign, timestamp, curTransaction, preTransaction, and calTransaction in the respective business rules mentioned in Algorithm 3.

Algorithm 3: updateTransaction() Contract, EPS-ledger transaction update contract (updateTransaction()).

Input: EPS-Transaction-Sawtooth Engineer Initiate System Addresses

   tx.main(),

   accumulator ID (accID), accumulator node transaction

   access (accNodeTransaction), current operation and control

   timestamp(execute),

   transaction of energy power operational record update contract (add Transaction Update Contract (TUC))

   EPS-Ledger Sawtooth Engineer (SE), EPS accumulator count (acCount)

   SE is a set of all authorized addresses of the energy **Sawtooth Engineer**

if   tx.main() is SE

  then

   if   accumulator node has not existed

    then

    change state of acCount, add new node transaction record;

    accID, accNodeTransaction, current operational and control, tx.main(),

    add on TUC to the blockchain distributed ledger;

    acCount is increment by a unit;

   else

    backtracking and state error generation

    end;

else

  backtracking and state error generation

  end;

4.2. Simulations and Results Discussion

Applying the simulation of the proposed EPS-ledger architecture for distributed energy and power systems chain of control nodes, we tested different blockchain distributed power nodes by evaluating the transaction batches, cost per transaction, and cost per hash (SH-256) and automated the transaction execution and verification with the help of the created smart contracts shown in Table 2. This architecture was tested with different purposes where parameters are a permissioned private network and P2P connectivity, active participating stakeholders and exchanging information policy, the number of power distributed nodes of control operations, and the set of power system distributed types were varied. The three business conditions (rules) were tested through the distributed architecture, participation registration (register()), secure accumulator transaction (addNode()), and update transaction (updateTransaction()), shown in Figures 6–8, according to the customized design EPS-ledger consensus policies and sawtooth protocol. The Sawtooth validator was responsible for managing the overall transaction from validation to the transaction processor and peers of different nodes in the chain. In addition, it ensured the privacy and protection of the transaction and the relation between the cost of node transaction along with the security cost per node (hash encryption), shown in Figures 9–11.

Table 2. Calculated hashes of the encrypted nodes and the relation between cost of node transaction.

Energy Type	No. of Nodes	Encrypted Hash	Transaction Cost	Batch
Renewable (Wind, Water, Solar, **etc.)**	Node 1	000000a87cb5eafdcca6a8cde0fb0dcc1400c5ab27447a6aa82c1c0cbf0fbcaf64c0b	1	0
	Node 2	000000a87cb5eafdcca6a8cde0fb0dcc1400c5ab27447a6aa82c128440f169a04216b7	3	0
	Node 3	000000a87cb5eafdcca6a8cde0fb0dcc1400c5ab27447a6aa82c1918142591ba4e8a7	8	1
	Node 4	000000a87cb5eafdcca6a8cde0fb0dcc1400c5ab27447a6aa82c12840f169a04216b7	13	1

Figure 6. Web-based blockchain Sawtooth-enabled renewable energy and power chain of node interface.

Figure 7. Sawtooth validator initiate system validation (register()).
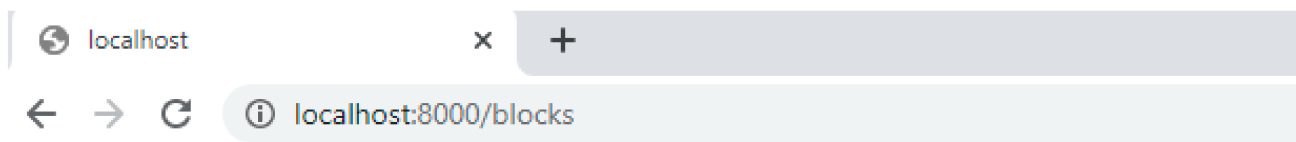
Figure 8. Web-based blockchain Sawtooth-enabled renewable energy and power chain of node interface.

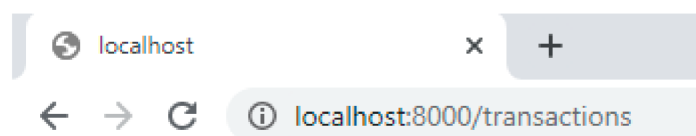**Figure 9.** Batch wise hash-encrypted node transactions (addNode()).

Figure 10. Run local host: 8000 for adding updated transaction in the distributed power chain of control node.

```
▼ 1:
    ▼ address:    "000000a87cb5eafdcca6a8c983c585ac3c40d9b1eb2ec8ac9f31ff82a3537ff0dbce7e"
    ▼ data:       "CiwKIXNhd3Rvb3RoLmNvbnNlbnN1cy5hbGdvcml0aG0ubmFtFtZRIHRGV2bW9kZQ=="
▼ 2:
    ▼ address:    "000000a87cb5eafdcca6a8cde0fb0dec1400c5ab274474a6aa82c12840f169a04216b7"
    ▼ data:       "CmwKJnNhd3Rvb3RoLnNldHRpbmdzLnZvdGGUuYXV0aG9yaXplZF9rZXlzEkIwMjA3TllZGYwMzBjZGViYzg3NWI5MmI3Zjg5ODDY3ZDYyNGM1YWE0YWZhNWFhNMyMzFmY2U0Z"
▼ 3:
    ▼ address:    "8ac6aec2879b0209cfa70c3f464ab38177341707edac6b2bc58e974141d2fd46b1d44a"
      data:       "aGVsbG8gd29ybGQ="
▼ head:           "c8d5f9675a1a0dd67f6f61cd88fb86c2031ee62286ac3e7ed4bd5b5e134b47487395266535a09c83fe34c11a220b12d45b385a446897dc2a5fe7de574eef5ef0"
▼ link:           "http://localhost:8008
                  /state?head=c8d5f9675a1a0dd67f6f61cd88fb86c2031ee62286ac3e7ed4bd5b5e134b47487395266535a09c83fe34c11a220b12d45b385a446897dc2a5fe7de574e
                  start=000000a87cb5eafdcca6a8c983c585ac3c40d9b1eb2ec8ac9f31ff5ca4f3850ccc331a&limit=100"
▼ paging:
    limit:        null
    start:        null
```

Figure 11. Hash-encrypted power-related data stored and exchange details among the participating stakeholders and connected in the chain-like structure (updateTransaction()).

The proposed chain of control node transactions presented the individual transaction verification that required less amount of time to validate, as shown in Figures 12 and 13. With the number of power operation transactions having increased, the execution cost exceeded exponentially, maintaining the performance of the blockchain distributed node transaction by applying the experiment using Hyperledger, whereas Hyperledger Sawtooth validator completed the energy-based transaction verification and validation as the minimum time cost effectively. The simulation-based experimental results showed that the performance (in terms of efficiency and security) of this proposed architecture were more efficient than the other public permissionless state-of-the-art non-blockchain-based unsecure models. Figure 12 presents that compared with the blockchain-based secure transaction model for distributed renewable energy in the industrial Internet of Things using a Bitcoin transaction algorithm, which executes the transaction verification and validation process with security [38]. J. Hou et al. presented an architecture that decreases the energy-related transaction verification cost and design consensus, but cannot consider the wallet-freezing problem. Undoubtedly, it is a secure architecture for energy-related distributed transaction verification and validation, but less efficient along with consuming a wider scope of data cost and privacy and computational power, as shown in Figures 12 and 13.
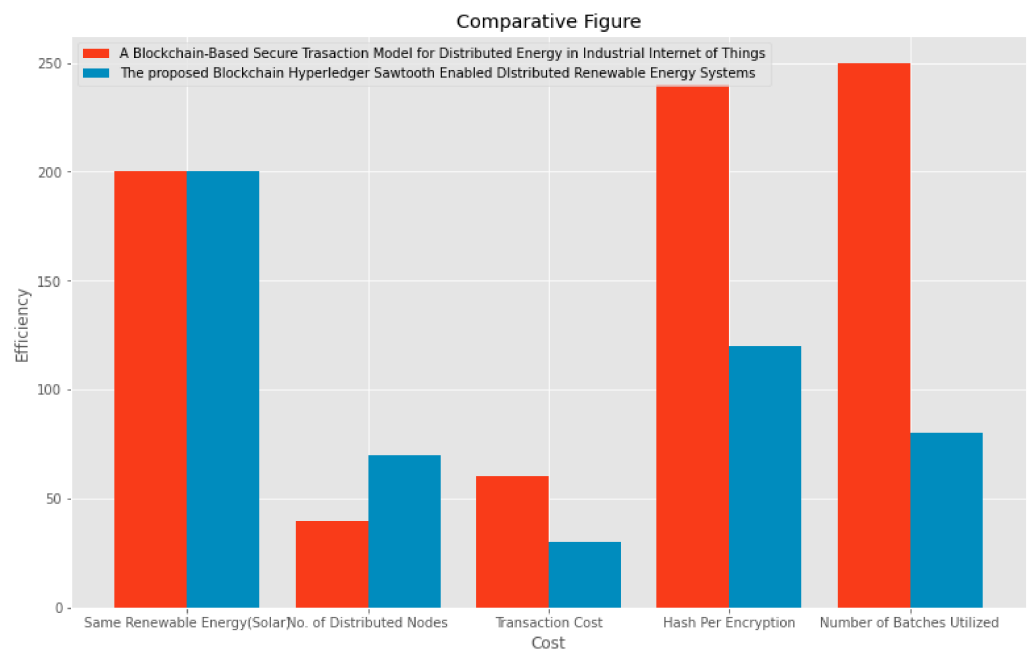
Figure 12. Comparison of the proposed architecture with other state-of-the-art methods.
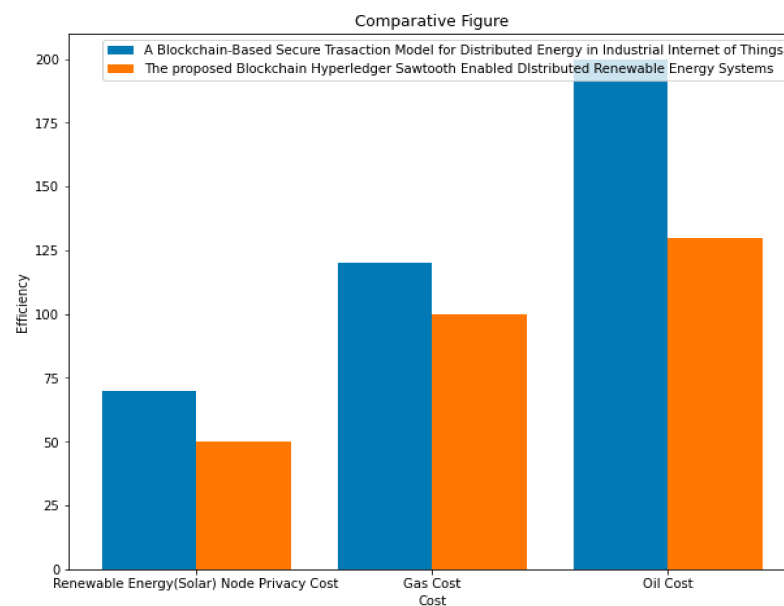

Figure 13. Comparison of the proposed EPS-Ledger with other State-of-the-Art Methods 3(a).

5. The Proposed Hyperledger Sawtooth-Enabled Modular Operations Presented through Sequence Diagram

Figure 14 presents the blockchain Hyperledger Sawtooth-enabled EPS-ledger renewable energy identification, registration, validation, and verification process. The initial process was executed between the residential and business owner and the Ministry of Energy and Power Resource, once the consensus reached the point of record registration, in which both the participating stakeholders interacted and signed with the level of encryption. After that, the residential and business owners received the updated ledger from the ministry; then, the business rule updated the information using *updateTransaction()* and stored in the distributed IPFS storage shown in Figure 14.
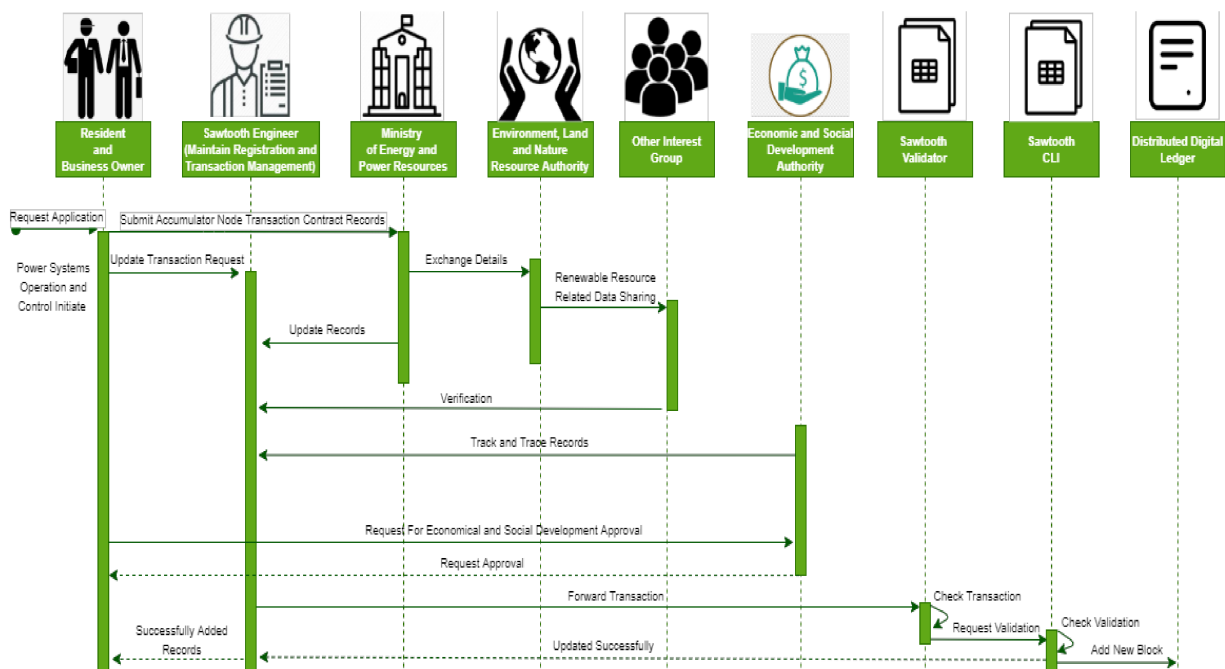
Figure 14. The working of blockchain Hyperledger Sawtooth-enabled EPS-ledger registration, validation, and verification process through sequence diagram.

5.1. Working Operations of the Proposed EPS-Ledger

The implementation of renewable energy and power systems chain of control operations of node transaction executed TUC (updateTransaction()), where the economic and social development authority tracked and traced each aspect before taking any development and financial decision, whereas the Sawtooth Engineer maintained registration and power transaction management and produced complete statistical information related to power system monitoring. Additionally, the Sawtooth engineer collected and analyzed individual records of residential and business owners, environment and nature authorities, other interest groups, and social development authorities, including the meta-record, timestamp record, and other affiliation information and stored them in a secure distributed EPS-ledger.

5.2. EPS-Ledger Implementation Challenges and Limitations

The transition of blockchain Hyperledger technology from advertising to reality poses critical challenges and adaptability issues, most probably in the context of renewable energy systems, where the data exchange, transfer, storage, and interoperability of the power systems chain of operation and control-related transactions and their provenance is the main concern area that needs to provide a solution by using the blockchain Hyperledger-enabled solution [39]. Following are the critical implementation challenges discussed in detail:

5.2.1. Regulatory Compliance

One of the implementation issues was regulatory compliance; the federal authority of energy and power management policy maker needs to consider and design, as well as develop, the instruction and policy guideline of power systems. Whereas the node transactions regarding the blockchain Hyperledger implication of power system control operations, such as the distributed preservation, operational data exchange, access of the node, and records on the ledger, and when does the access change, with distinct rights on the distributed ledge network [40]. The renewable energy sector needs to collaborate and facilitate the running of regulatory frameworks such as the USER commission for

security and the development of modern blockchain evolution of an energy system and power systems chain of operation and control ecosystem to formulate new administrative policies [34].

5.2.2. Platform Interoperability

A mass adaptation of business platforms across multiple enterprises is needed to provide an efficient and effective business solution to end-users using different platforms such as blockchain-enabled platforms and legacy systems [39]. The current legacy of power system operation and control solutions is a lack of interoperable solutions. These discontinuities and weak implementations may raise adaptability issues and scalability difficulties. Recently, several Hyperledger technologies have worked on system interoperability; they try to cope with these issues and provide efficient solutions to connect to ensure maximum scalability and adaptability to enable intercommunication between the renewable energy sectors [41].

5.2.3. Security Cost and Data Privacy

The distributed ledger network of energy and power systems, chain stakeholders and control monitoring-related core electronic data records and access to this sensitive information on the blockchain platform are a serious privacy challenge, as most renewable energy consumers do not want to share their personal information and confidential data with their competitors [34,40]. The current blockchain Hyperledger technology copes with this security challenge and provides more privacy and protection of stakeholders' details and other related information and ensures the solution will increase the system security and reduce the cost of data privacy [42,43].

5.2.4. Data Standardization and Scope

This is significant for the renewable industries to cater which type of energy-related data will be stored on the distributed secure preservation and how it will be stored using the blockchain ledger (off-chain and on-chain) [39]. For the renewable energy supply system, most of the power systems chain of operation and control-related data and monitoring information are private and sensitive; therefore, it must be verified and double-checked to be stored against the on-chain hash-encrypted evidence [43,44]. However, data standardization is one of the significant aspects, and the size of the data will be stored in a private ledger is one of the challenging factors. Storing a large amount of data and duplication will lead to an additional impact on the cost of node transactions. In addition, this will affect the performance in terms of efficiency. Renewable industries have to maintain standardized data on the distributed ledger network to achieve a better enterprise performance and meet their needs, such as adequately defining the size, format, and type of data preserved on the blockchain distributed ledger [44,45].

6. Conclusions

This paper addressed the security and privacy issues in the current distributed renewable energy systems and multichannel power control operations and monitoring management. We identified the distributed node privacy solution and highlighted the implementation challenges involved in the current system, using blockchain Hyperledger Sawtooth-enabled cyber-physical monitoring of renewable energy and secure node transactions execution solutions, including the multimachine system, competitive environment, billing, settlement, and reliability. The EPS-ledger is a private network-based permissioned architecture designed and implemented between participating stakeholders for operation and control node monitoring and to maintain the integrity and transparency of energy-related records preservation. In addition, this proposed Hyperledger Sawtooth-enabled architecture provides robust security and novelty, ensuring the maintenance of decentralized power-related data records stored in a distributed ledger that is completely immutable, protected, easy to exchange, transfer, track, and trace through the hash-encrypted and com-

bination of business rules. It also protects node transaction and data secrecy, timestamping, unanimous, and programmable private network-based permissioned interfaces. The ES-ledger solution is a proper package that is completely distributed in nature; moreover, we ran a process-like non-repudiation with provenance and traceable by agile courage without any conflict in the distributed power systems chain-of-operation and control secure node transactions.

Author Contributions: A.A.K. writing the original draft and preparation, A.A.L., D.-S.L. and A.A.S. have reviewed, rewrote, performed part of the literature survey, and edited, D.-D.M., C.-Y.W. and A.A.W. have investigated, designed the architecture, and explored the software tools. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors did not have any conflict of interest.

References

1. Poudyal, R.; Loskot, P.; Nepal, R.; Parajuli, R.; Khadka, S.K. Mitigating the current energy crisis in Nepal with renewable energy sources. *Renew. Sustain. Energy Rev.* **2019**, *116*, 109388. [CrossRef]
2. Newell, R.G.; Raimi, D. *Global Energy Outlook Comparison Methods: 2020 Update*; Resources for the Future: Washington, DC, USA, 2020.
3. Vedik, B.; Kumar, R.; Deshmukh, R.; Verma, S.; Shiva, C.K. Renewable Energy-Based Load Frequency Stabilization of Interconnected Power Systems Using Quasi-Oppositional Dragonfly Algorithm. *J. Control. Electr. Syst.* **2021**, *32*, 227–243. [CrossRef]
4. Weschenfelder, F.; Leite, G.D.N.P.; da Costa, A.C.A.; de Castro Vilela, O.; Ribeiro, C.M.; Ochoa, A.A.V.; Araujo, A.M. A review on the complementarity between grid-connected solar and wind power systems. *J. Clean. Prod.* **2020**, *257*, 120617. [CrossRef]
5. Foley, A.M.; McIlwaine, N.; Morrow, D.J.; Hayes, B.P.; Zehir, M.A.; Mehigan, L.; Papari, B.; Edrington, C.S.; Baran, M. A critical evaluation of grid stability and codes, energy storage and smart loads in power systems with wind generation. *Energy* **2020**, *205*, 117671.
6. Balakheli, M.M.; Chahartaghi, M.; Sheykhi, M.; Hashemian, S.M.; Rafiee, N. Analysis of different arrangements of combined cooling, heating and power systems with internal combustion engine from energy, economic and environmental viewpoints. *Energy Convers. Manag.* **2020**, *203*, 112253. [CrossRef]
7. Ullah, S.; Haidar, A.M.; Hoole, P.; Zen, H.; Ahfock, T. The current state of Distributed Renewable Generation, challenges of interconnection and opportunities for energy conversion-based DC microgrids. *J. Clean. Prod.* **2020**, *273*, 122777. [CrossRef]
8. Khan, A.A.; Shaikh, A.A.; Cheikhrouhou, O.; Laghari, A.A.; Rashid, M.; Shafiq, M.; Hamam, H. IMG-forensics: Multimedia-enabled information hiding investigation using convolutional neural network. *IET Image Process* **2021**, 1–9. [CrossRef]
9. Peyghami, S.; Palensky, P.; Blaabjerg, F. An overview on the reliability of modern power electronic based power systems. *IEEE Open J. Power Electron.* **2020**, *1*, 34–50. [CrossRef]
10. Kenyon, R.W.; Bossart, M.; Marković, M.; Doubleday, K.; Matsuda-Dunn, R.; Mitova, S.; Julien, S.A.; Hale, E.T.; Hodge, B.M. Stability and control of power systems with high penetrations of inverter-based resources: An accessible review of current knowledge and open questions. *Sol. Energy* **2020**, *210*, 149–168. [CrossRef]
11. Kouhizadeh, M.; Saberi, S.; Sarkis, J. Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *Int. J. Prod. Econ.* **2021**, *231*, 107831. [CrossRef]
12. Bouachir, O.; Aloqaily, M.; Tseng, L.; Boukerche, A. Blockchain and fog computing for cyberphysical systems: The case of smart industry. *Computer* **2020**, *53*, 36–45. [CrossRef]
13. Tsao, Y.C.; Thanh, V.V. Toward blockchain-based renewable energy microgrid design considering default risk and demand uncertainty. *Renew. Energy* **2021**, *163*, 870–881.
14. Afzal, M.; Huang, Q.; Amin, W.; Umer, K.; Raza, A.; Naeem, M. Blockchain enabled distributed demand side management in community energy system with smart homes. *IEEE Access* **2020**, *8*, 37428–37439. [CrossRef]
15. Wu, J.; Tran, N.K. Application of blockchain technology in sustainable energy systems: An overview. *Sustainability* **2018**, *10*, 3067. [CrossRef]
16. Bao, J.; He, D.; Luo, M.; Choo, K.K.R. A survey of blockchain applications in the energy sector. *IEEE Syst. J.* **2020**, *15*, 3370–3381. [CrossRef]
17. Hou, J.; Wang, C.; Luo, S. How to improve the competiveness of distributed energy resources in China with blockchain technology. *Technol. Forecast. Soc. Chang.* **2020**, *151*, 119744. [CrossRef]
18. Wolsink, M. Distributed energy systems as common goods: Socio-political acceptance of renewables in intelligent microgrids. *Renew. Sustain. Energy Rev.* **2020**, *127*, 109841. [CrossRef]

19. Kumar, N.M.; Chand, A.A.; Malvoni, M.; Prasad, K.A.; Mamun, K.A.; Islam, F.R.; Chopra, S.S. Distributed energy resources; the application of AI, IoT, and blockchain in smart grids. *Energies* **2020**, *13*, 5739. [CrossRef]

20. Baggio, A.; Grimaccia, F. Blockchain as Key Enabling Technology for Future Electric Energy Exchange: A Vision. *IEEE Access* **2020**, *8*, 205250–205271. [CrossRef]

21. Iskakova, A.; Nunna, H.K.; Siano, P. Ethereum Blockchain-Based Peer-To-Peer Energy Trading Platform. In Proceedings of the 2020 IEEE International Conference on Power and Energy (PECon), Penang, Malaysia, 7–8 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 327–331.

22. Lu, J.; Wu, S.; Cheng, H.; Xiang, Z. Smart contract for distributed energy trading in virtual power plants based on blockchain. *Comput. Intell.* **2020**, *107*, 2411–2502.

23. Petri, I.; Barati, M.; Rezgui, Y.; Rana, O.F. Blockchain for energy sharing; trading in distributed prosumer communities. *Comput. Ind.* **2020**, *123*, 103282. [CrossRef]

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

25. Di Silvestre, M.L.; Gallo, P.; Guerrero, J.M.; Musca, R.; Sanseverino, E.R.; Sciumè, G.; Vásquez, J.C.; Zizzo, G. Blockchain for power systems: Current trends; future applications. *Renew. Sustain. Energy Rev.* **2020**, *119*, 109585. [CrossRef]

26. Ibrahim, M.S.; Dong, W.; Yang, Q. Machine learning driven smart electric power systems: Current trends and new perspectives. *Appl. Energy* **2020**, *272*, 115237. [CrossRef]

27. Duarte, Y.S.; Szpytko, J.; del Castillo Serpa, A.M. Monte Carlo simulation model to coordinate the preventive maintenance scheduling of generating units in isolated distributed Power Systems. *Electr. Power Syst. Res.* **2020**, *182*, 106237. [CrossRef]

28. Rathore, H.; Mohamed, A.; Guizani, M. A survey of blockchain enabled cyber-physical systems. *Sensors* **2020**, *20*, 282. [CrossRef]

29. Ali, F.S.; Aloqaily, M.; Alfandi, O.; Ozkasap, O. Cyberphysical blockchain-enabled peer-to-peer energy trading. *Computer* **2020**, *53*, 56–65. [CrossRef]

30. Vatankhah Barenji, A.; Li, Z.; Wang, W.M.; Huang, G.Q.; Guerra-Zubiaga, D.A. Blockchain-based ubiquitous manufacturing: A secure and reliable cyber-physical system. *Int. J. Prod. Res.* **2020**, *58*, 2200–2221. [CrossRef]

31. Graf, M.; Küsters, R.; Rausch, D. Accountability in a Permissioned Blockchain: Formal Analysis of Hyperledger Fabric. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P), Genova, Italy, 7–11 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 236–255.

32. Moriggl, P.; Asprion, P.M.; Schneider, B. Blockchain Technologies Towards Data Privacy—Hyperledger Sawtooth as Unit of Analysis. In *New Trends in Business Information Systems and Technology*; Springer: Berlin, Germany, 2020; pp. 299–313.

33. Vivek, S.K.; Yashank, R.S.; Prashanth, Y.; Yashas, N.; Namratha, M. E-Voting System using Hyperledger Sawtooth. In Proceedings of the 2020 International Conference on Advances in Computing, Communication & Materials (ICACCM), Dehradun, India, 21–22 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 29–35.

34. Uddin, M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *Int. J. Pharm.* **2021**, *597*, 120235. [CrossRef]

35. Moschou, K.; Theodouli, A.; Terzi, S.; Votis, K.; Tzovaras, D.; Karamitros, D.; Diamantopoulos, S. Performance Evaluation of different Hyperledger Sawtooth transaction processors for Blockchain log storage with varying workloads. In Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2–6 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 476–481.

36. Perboli, G.; Capocasale, V.; Gotta, D. Blockchain-based transaction management in Smart Logistics: A Sawtooth framework. In Proceedings of the 2020 IEEE 44th Annual Computers Software and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1713–1718.

37. Wang, R.; Ye, K.; Meng, T.; Xu, C.Z. Performance Evaluation on Blockchain Systems: A Case Study on Ethereum, Fabric, Sawtooth and Fisco-Bcos. In Proceedings of the International Conference on Services Computing, Honolulu, HI, USA, 22–26 June 2020; Springer: Berlin, Germany, 2020; pp. 120–134.

38. Zhao, Y.; Peng, K.; Xu, B.; Liu, Y.; Xiong, W.; Han, Y. Applied engineering programs of energy blockchain in US. *Energy Procedia* **2019**, *158*, 2787–2793. [CrossRef]

39. Namasudra, S.; Deka, G.C.; Johri, P.; Hosseinpour, M.; Gandomi, A.H. The revolution of blockchain: State-of-the-art and research challenges. *Arch. Comput. Methods Eng.* **2021**, *28*, 1497–1515. [CrossRef]

40. Shafiq, M.; Tian, Z.; Bashir, A.K.; Jolfaei, A.; Yu, X. Data mining and machine learning methods for sustainable smart cities traffic classification: A survey. *Sustain. Cities Soc.* **2020**, *60*, 102177. [CrossRef]

41. Uriarte, R.B.; Zhou, H.; Kritikos, K.; Shi, Z.; Zhao, Z.; De Nicola, R. Distributed service-level agreement management with smart contracts and blockchain. *Concurr. Comput. Pract. Exp.* **2020**, *33*, e5800. [CrossRef]

42. Shafiq, M.; Tian, Z.; Bashir, A.K.; Du, X.; Guizani, M. Corrauc: A malicious bot-iot traffic detection method in iot network using machine learning techniques. *IEEE Internet Things J.* **2020**, *99*, 3242–3254. [CrossRef]

43. Khan, A.A.; Uddin, M.; Shaikh, A.; Laghari, A.A.; Rajput, A. MF-Ledger: Blockchain Hyperledger Sawtooth-enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture. *IEEE Access* **2021**, *9*, 103637–103650. [CrossRef]

44. Shafiq, M.; Tian, Z.; Sun, Y.; Du, X.; Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Gener. Comput. Syst.* **2020**, *107*, 433–442. [CrossRef]
45. Khan, A.A.; Laghari, A.A.; Awan, S.; Jumani, A.K. Fourth Industrial Revolution Application: Network Forensics Cloud Security Issues. In *Security Issues and Privacy Concerns in Industry 4.0 Applications*; WILEY: Hoboken, NJ, USA, 2021; pp. 15–33.