Blockchain for Cyber Security in Smart Grid: A Comprehensive Survey

Peng Zhuang, *Student Member, IEEE*, Talha Zamir, and Hao Liang, *Member, IEEE*

***Abstract*—Blockchain is an immutable type of distributed ledger that is capable of storing data without relying on a third party. Blockchain technology has attracted significant interest in research areas, including its application in the smart grid for cyber security. Although significant efforts have been devoted to utilizing blockchain in the smart grid for cyber security, there is a lack of comprehensive survey on blockchain in the smart grid for cyber security in both application and technological perspectives. To fill this gap, we conducted a comprehensive survey on blockchain for smart gird cyber security. This conducted survey presents the latest insights of ideas, architectures, and techniques of implementation that are relevant to blockchain's application in the smart grid for cyber security. This paper aims at providing helpful guidance and reference for future research efforts specific to blockchain for cyber security in smart grid.**

***Index Terms*—Blockchain, cyber security, resiliency, smart contract, smart grid.**

I. Introduction

The electric grid is undergoing massive revolutions toward the smart grid to better adopt the generation with different sizes and technologies, encourage the participation of customers for active system operation, and improve the system reliability, stability, sustainability, and security [1]. The reliable and efficient smart grid operation relies heavily on the two-way communication networks for data transfers [2]. However, the current communications over TCP/IP and Ethernet-based technologies expose the smart grid to public data networks [3], which makes it vulnerable to severe cyber attacks [4].

In December 2015, the cyber attack targeted on three electric distribution companies in Ukraine successfully seized the supervisory control and data acquisition (SCADA) systems using spear-phishing emails, and remotely switched substations off, which resulted in a power outage of 230,000 customers [5]. In March 2019, a denial of service (DoS) attack was launched against part of the SCADA infrastructures of electric utilities in Utah, which resulted in the loss of observability for part of the electric grid [6]. Although this cyber attack has not led to any blackouts in Utah electric grid, it has shown that the adversaries can launch severe cyber attacks against critical infrastructures in the smart grid.

With the development of the smart grid, the advanced monitoring and control technologies are being deployed on the customer side. Nowadays, most homes are equipped with smart devices, such as smart robots and smart security systems. Since these devices can be remotely monitored and controlled through a central controller, the cyber security becomes important for customers [7]. Also, with the cutting-edge technologies, the smart grid is emerging with water/gas supply, transportation, and other services to form the smart city [8], [9]. With the high degree of interdisciplinary among different sectors in a smart city, the vulnerability of the smart grid to cyber attacks may cause severe disasters to the society, which is no longer limited to the electric systems. So, there is an urgent need to investigate the cyber security of smart grid.

In smart grid, different information and communication technologies (ICT) have been widely adopted over power generation, transmission, distribution, and utilization sectors to collect and transfer data for smart grid optimization control. For the power generation, transmission, and distribution, the data are collected using remote terminal units (RTUs) of SCADA systems, phasor measurement units (PMUs) of wide area measurement system (WAMS), sensors of intelligent electronic devices (IEDs), and geographic information system (GIS). For power utilization, the smart meters embedded in the advanced metering infrastructures (AMIs) are typically used to collect the customers' power usage data. The collected data are transferred through communication networks to SCADA systems and used for advanced management and control, such as automatic generation control (AGC), electric system state estimation (SE), distribution automation control (DAC), and demand side management (DSM).

For the efficient and reliable communications among distributed and heterogeneous components within smart grid, layered communication networks consisting of home area network (HAN), neighborhood area network (NAN), sensor network (SN) wide area network (WAN), and core network are developed. The HAN and NAN are established by networking AMIs within a local area through ZigBee/Z-wave protocols and IEEE 802.11/802.15.4/802.16 standards [10]. Within the WAN, the RTUs, WAMS, IEDs, and GIS firstly group through SN, then communicate with the SCADA systems and data centers based on distributed networking protocol 3.0 (DNP3), Modicon communication bus (ModBus), and/or cognitive radio with IEEE 802.22 standard [11]. Then, the data are transferred to the core network and used by different control authorities. In the core network, the common communication methods are TCP/IP network, WiMAX, and GPRS. For the ease of implementation in smart grid, these protocols are designed to communicate raw data with no restrictions of encryption and authentication, and there is no excessive overhead for data availability [12]. So, the smart grid can be easily exploited by cyber attacks.

The vulnerabilities of different communication protocols in smart grid are investigated in [13], and the most concerning

The authors are with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada T6G 1H9 (e-mail: {pzhuang, tzamir, hao2}@ualberta.ca).

cyber security issues can be summarized in four aspects:

- Integrity;
- Confidentiality;
- Availability;
- Accountability/Non-Repudiation.

The integrity attack is based on unauthorized and stealthy modification, alteration, or destruction of field measurement data in smart grid. The false data injection (FDI) attack is a typical integrity attack against SE. The FDI attack can compromise the field measurement data stealthily, which will alternate the SE results and mislead the control center decisions. This can cause cascade electric grid failures [14].

The confidentiality attack targets on accessing or disclosing privacy and proprietary information by unauthorized entities or individuals. In smart grid, the AMIs are major sources of the confidential breach. The adversaries can gain access to AMI through root password recovery or exploitation of system vulnerabilities [15], and obtain the customers' electricity usage information to invade customers' privacy. In smart grid, both authentications of information and authorization of accessing are required to maintain the integrity and confidentiality.

The availability that ensures timely and reliable access to information is essential for efficient and stable operation of smart grid. By interrupting the data transfers, the cyber attacks against availability can delay, block, or even corrupt the control signal, and cause severe impacts on stability, efficiency, and security of smart grid operation [16].

For the accountability/non-repudiation in smart grid, the actions made by systems or customers cannot be denied later. With the integration of distributed generators (DGs), local power trading is an important concept in smart grid. The local power trading involves valuable resources and information, which makes the cyber attacks against accountability/non-repudiation now a major issue [13]. To maintain the accountability/non-repudiation, it is required that the smart grid communication networks have high auditability so that the complete information history can be reconstructed from historical records in a trust manner [16].

For enterprise communication networks, different cyber security technologies, such as firewalls with an intrusion detection system (IDS) for network security, encryption and authentication for data security, and host IDS for device security [10]. However, due to the real-time performance requirement and continuous operation feature of smart grid communication networks, these techniques can hardly fit in smart grid [16]. Smart grid is featured by distributed generation and control; however, the communication networks in smart grid still behave in a centralized manner, which makes the smart grid extremely vulnerable to a single point of failure [17]. To address the above cyber security issues in smart grid, blockchain technology has been seen as a promising solution [18]–[20].

Blockchain is a variant of distributed ledger technology (DLT), which distributively stores and transfers data across multiple devices within a system. By leveraging blockchain technology, the field measurement data and local transaction data can be transferred in a peer-to-peer (P2P) manner within smart grid [21]. These data are replicated and stored distributively on multiple devices, instead of a single data center. The P2P data transfer and distributed replication of data storage on multiple devices prevent the smart grid from suffering from a single point of failure and guarantee high availability [22]. Also, due to the distributed data verification, validation, and storage features of blockchain, the data in blockchain-based smart grid are nearly immutable, which can protect the data integrity, confidentiality, and availability of smart grid. Once data are added to a blockchain, it can never be manipulated by attacks unless the adversaries own more than 51% of the devices in the whole system. This property maintains high auditability in blockchain-based smart grid and makes the accountability/non-repudiation attacks nearly impossible. The asymmetric cryptography in blockchain can increase the authentication and authorization levels of blockchain-based AMIs [23], which can protect the customers' privacy and integrity of electricity data [24]. Further, by leveraging the smart contract and decentralized applications (DAPPS) services, the blockchain can provide cyber-secured computation environment for advanced smart grid applications.

In the literature, there are several papers that have conducted surveys on the application of blockchain in smart grid covering various topics. A systematic review of blockchain in energy sector is conducted in [25], in which an overview of a variety of energy applications of blockchain is presented with detailed discussion on benefits and limitations of blockchain technologies in energy sector. Also, the review and classification of around 140 most recent commercial and research initiatives of energy blockchain are performed. With more focuses on blockchain-based smart grid, [26] reviews a variety of prospects and approaches for blockchain applications in smart grid. The advantages and technical challenges of implementing blockchain in smart grid are discussed, and the frameworks for key blockchain-based smart grid applications are presented. In [27], a comprehensive survey is presented for the blockchain-based P2P energy transaction in smart grid with main focuses on P2P energy trading architecture, demand response optimization models, and power routing mechanisms. Further, [28] presents a comprehensive survey for the blockchain-based P2P energy transaction from the perspective of the designing of local energy markets, in which the current research activities on local energy market mechanisms, customer preferences, demand response strategies, and impacts of energy storage are reviewed and assessed. Although the existing survey papers have mentioned the advantages of blockchain in improving smart grid cyber security. A comprehensive survey that emphasizes both application and technical perspectives of blockchain in smart grid for cyber security has not been conducted so far. To fill this gap in research, this paper presents a comprehensive survey to provide helpful guidance and reference for the research in improving cyber security of smart grid by using blockchain technology.

The remainder of this paper is organized as follows. In Section II, an overview of blockchain technology is presented. The architecture and development platforms of blockchain-based smart grid for cyber security are introduced in Section III. In Section IV, the integration of blockchain technology for cyber-

TABLE I: A Comparison among Public, Consortium, and Private Blockchains [2], [4], [21]

	Public	**Consortium**	**Private**
Participants	Anonymus	Trusted	Trusted
Consensus mechanism	Proof of Work (PoW), Proof of Stake (PoS), etc.	Multi-party voting	Strictly pre-approved nodes
Security performance	51% attack tolerance, nearly impossible to tamper, no finality	33.33% attack tolerance, could be tampered, enabled finality	
Computational complexity	High	Low	
Access	Open access	Permissioned	Strictly permissioned
Anonymity	Yes	No	No

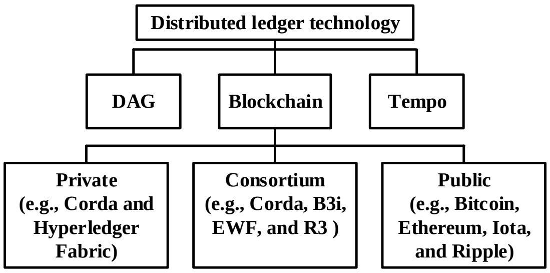
Distributed ledger technology
DAG
Blockchain
Tempo
Private (e.g., Corda and Hyperledger Fabric)
Consortium (e.g., Corda, B3i, EWF, and R3)
Public (e.g., Bitcoin, Ethereum, Iota, and Ripple)

Fig. 1: The classification of DLT and blockchain technologies.

secured smart grid will be discussed in both application and technical perspectives. At the end, the conclusion and potential future research directions will be addressed in Section V.

II. Overview of Blockchain Technology for Cyber Security of Smart Grid

DLT is defined as a database that consensually replicates, shares, and synchronizes data across geographically distributed multiple devices [29]. In DLT, the data are stored in a chronological order, which forms a digital ledger chain. Once a block containing a set of data is added in the chain, it can never be modified by any unauthorized entities or individuals, so it is inherently tamper-proof [30]. As shown in Fig. 1, according to how the data are validated and stored, the DLT can be mainly classified into three types, i.e., blockchain, directed graph data (DAG), and tempol ledger (Tempo). Among these three types of DLT, the blockchain is the most well studied one with a high degree of penetration in practical applications [29]. Blockchain is divided into blockchain 1.0 for simple cryptographic currency, 2.0 with smart contract functionality, and 3.0 for distributed application [31].

Blockchain is a distributed database based on P2P network, with security enabled using multiple cryptographic technologies. Different types of blockchain have been proposed to meet different requirements for practical applications based on the consensus mechanism and network openness. As shown in Fig. 1, the most studied blockchain variants are public, consortium, and private blockchains. A comparison of these three types of blockchains is summarized in Table I. The major difference between public and consortium/private blockchains is the classes of nodes, i.e., the devices responsible for data verification, validation, transfer, and storage. For the public blockchain, the nodes are trustless and anonymous, which results in large power consumption and long transaction approval time. The nodes in consortium and private blockchains are trusted, and the consensus mechanisms based on trusted nodes have low power consumption and fast transaction approval rate.

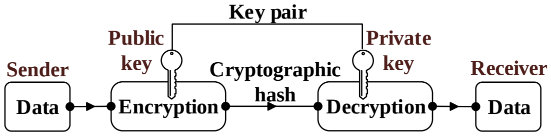

Fig. 2: Asymmetric cryptography in blockchain [82].

However, the access for consortium and private blockchain networks is permissioned, there still requires an authority to approve the permission for node. Due to a large number of nodes in public blockchain, it is nearly impossible to tamper public blockchain [32]. Theoretically, the consortium and private blockchains require less effort for tampering, in practical, they still have good performance in cyber security, since the nodes in consortium and private blockchain are authorized and can be well protected [33]. So, the selections among different types of blockchain for different applications in smart grid should consider the classes of nodes, the requirement for anonymity, computational complexity (efficiency), and restriction on access [34].

Based on the features of blockchain, some potential benefits for smart grid are summarized as below [10]–[12]:

- Reduction on cost of power transactions;
- Facilitating the adoption of DGs in smart grid;
- Improved automation control and system monitoring;
- Development of advanced control applications for smart grid on blockchain DAPPS layer;
- Improved cyber security of smart grid.

In this paper, the main focus is on the cyber security feature of blockchain for smart grid. For the rest of this section, the blockchain technology will be discussed mainly related to smart grid cyber security. Although the private, consortium, and public blockchains differ in many aspects, they share some essential components in architecture: merkel tree, timestamp, hash function, encryption and decryption, consensus mechanism, and nonce [35]. Merkel tree is a data structure used for efficiently summarizing and verifying the large sets of data in a block. Each block has a Unix time timestamp, which creates a source of variation for block hash and makes it more difficult for the adversaries to tamper a blockchain. The hash function is used to convert variable-length inputs into a fixed-length encoded output. The hash function should have characteristics like puzzle-friendly and collision-free to achieve a high level of security. The secure hash algorithm (SHA) is widely used in cryptographic hash functions, e.g., SHA-256 in Bitcoin. In blockchain, the hash function is used in merkel tree, timestamp, and encryption [36].

Encryption and decryption method in blockchain is based on asymmetric cryptography, as shown in Fig. 2. Different from symmetric cryptography, every node in blockchain has a public key and a private key. The public key is analog to account public name, and the private key is like a password that is confidential [37], [38]. In blockchain, the sender encrypts the data using the public key of the receiver, and the data encrypted can be viewed, validated, and verified by all the nodes in blockchain using the receiver's public key, which protects the data integrity and accountability/non-repudiation. Then, the encrypted data can be decrypted by the receiver using the corresponding private key. In this process, the public and private key pair provide additional authentication and authorization to smart grid, and the privacy of nodes can be protected since only public keys can be observed [39].

The consensus mechanism is used to allow data transfers with credibility and assurity that it has not been tampered with. This develops trust among nodes without the involvement of a third party. The main idea in blockchain is to time stamp all the published blocks, then running it through a SHA256 hash algorithm to maintain the data integrity. Every block also refers to the value of the previous block using the hash value. In this way, everyone can see which blocks are interconnected and what data have been transferred in the past and in what order [40], which can provide better protection on the accountability/non-repudiation in smart grid.

A simple application of blockchain in smart grid is providing cyber-secured trading platform for P2P power transaction based on distributed ledger of Bitcoin [41]. Further, with a completely new programming language named by Solidity, Ethereum has brought computational capabilities into cyber-secured environment based on blockchain [42]. Also, with the emerged smart contract functionality, many blockchain-based applications have been investigated for the DAPPS services [43]. These DAPPS services allow for the integration of more variants of advanced applications for smart grid operation into cyber-secured system built by blockchain [44]. However, most of these applications are still limited to electronic currency, such as the Initial Coin Offerings (ICO's) on Ethereum platform, which provides services for fundraising [45].

One of the major issues that have impeded the broad applications of blockchain-based DAPPS is the scalability. Many researchers have devoted great efforts in addressing this issue. In [46], a technology named IOTA that combines the blockchain technology and architecture of the internet of things (IoT), is investigated to improve the scalability of blockchain. Compared with conventional linear single chain architecture, the IOTA introduces a meshed network architecture. Improvement in scalability is also achieved in [47] by using techniques such as segwit, blocksize increment, sharding, and proof of stake algorithm. Among these techniques, the sharding, which reduces the data size of a block, has been tested to be the most efficient one to improve the scalability. Also, some discussions have been made about changing the block size by alternating the blockchain structure. In [48], a new blockchain protocol, Bitcoin-NG, is proposed. In Bitcoin-NG, the concept of micro block is introduced to accelerate the block procession and reduce the block production time from 10 minutes to 10 seconds; however, this comes with the scarification of security. The cascaded structure of blockchain with decreased block size is introduced in [49], which improves the overall performance of the blockchain. Similarly, a scalable blockchain framework is proposed in [50] to improve the scalability of blockchain for large-scale IoT systems. In which, the IoT devices are required to connect to the global blockchain as nodes directly. Instead, multiple IoT devices form a group through a fully trusted certificate authority, and the formed group of IoT devices is represented by a single peer which participate in the global blockchian. Such architecture can be beneficial for smart grid as it proves to be reliable and protective against 51% attack with reduced forking.

For the successful integration of blockchain in smart grid, the interaction between blockchain and smart grid applications should be carefully addressed to maintain the stability of a blockchain. In [51]–[53], the stability problem caused by the interaction between blockchain and applications is investigated. The incentives mismatch within a blockchain, when considering the interaction between blockchain and applications, is the main issue for potential instability, since the nodes are economically motivated to confirm transactions securely in a blockchain, and they have no direct incentive to support applications. The incentive mismatch between secure confirmation of transactions in blockchain and supporting applications may lead to the collapse of blockchain. To avoid the incentive mismatch in a blockchain, it is crucial to designing a blockchain with high portability to provide common incentives for blockchains and their applications [51].

For the blockchain with applications, there are mainly four layers, i.e., application layer, execution engines, data storage, and consensus mechanism. Most of the research works focus on the application layer, especially for DAPPS, since it can bring more functionalities to blockchain on top of smart contracts [54]. Some decentralized applications use past data to develop trust for different nodes, and Airbnb is a good example of such an application. The same methodology can be used for demand forecasting in smart grid by using blockchain-based big data analysis, which can ensure the integrity, availability, and accountability/non-repudiation of historical data [55]. Also, in [36], the standard for emerging blockchain with various applications is proposed. This standard divides blockchain usage into four layers, i.e., the infrastructure layer that provides basic hardware and network support, the platform service layer that allows users to run the cyber-secured blockchain environment on different operating systems, such as Windows and BerkeleyDB. While the node management, programming, and run-time management come under the third layer, this layer uses SDK interfaces, such as JSON RPC, Solidity, and Node.js. The last layer is the user-level application layer, which is referred to as DAPPS commonly.

The implementation of well-designed blockchain in smart grid allows improving the overall smart grid system's cyber security. It introduces cyber-secured environment for variants of advanced applications in smart grid, such as electric grid monitoring, electricity data transfers, automation power control, and local power trading [30]. In the next section, an overview of system architecture and development platforms for cyber security of smart grid using blockchain technology

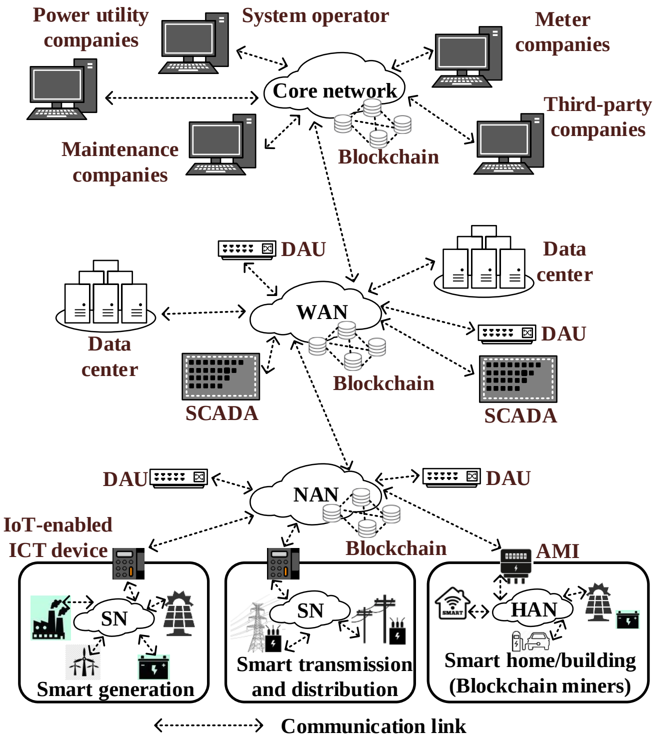

Fig. 3: System architecture of blockchain-based smart grid.

will be presented in detail.

III. System Architecture and Development Platform of Blockchain in Smart Grid for Cyber Security

The blockchains are implemented in the smart grid cyber layer to improve cyber security by protecting data integrity, confidentiality, availability, and accountability/non-repudiation. The implementation of blockchain in smart grid for cyber security can be mainly classified into four sectors that are field measurement and control, data aggregation, data management, and system operation [56]–[59]. In this section, the system architecture of blockchain-based smart grid for cyber security will be discussed. Also, the development platforms for blockchain-based smart grid will be presented.

A. System Architecture for Smart Grid Cyber Security

By incorporating blockchain in the cyber layer of smart grid, blockchain technologies can be leveraged to support the operation and development of smart grid. Considering the layered communication networks in smart grid with two-way communication links, the system architecture of blockchain in smart grid for cyber security is illustrated in Fig. 3, which is based on the communication system model in [60]. This structure is divided into four networks, i.e., core network, WAN, NAN, and SN/HAN. This architecture is embedded with blockchains in different communication networks for different smart grid applications. The core network is related to controlling authorities, such as power utility companies, system operators, meter operators, and maintenance companies, which are above the SCADA systems [61]. Users in the core network have full access to monitor, make modifications, and pass instructions (e.g., smart contracts) to the SN and HAN. Different blockchains can be used in the core network for different applications, such as energy bidding in wholesale electricity market and real-time monitoring in energy management system. WAN layer is an intermediate layer connecting the NAN with the core network. WAN in this system may be deployed on the cloud as a virtual machine, where different blockchains can be implemented for WAN applications, such as field measurement aggregation and storage. In NAN and HAN, the local producers and consumers are directly connected, and the blockchains can be used to provide various applications, such as electric vehicle charging and local energy trading.

Also, as discussed in the recent research works [60], [62], based on the two-way communication links in smart grid, the trustless local producers and consumers connecting to HAN can be selected as nodes to provide mining power for public blockchains in smart grid. Initially, the mining power could be provided by standard home computers; however, with the introduction of the application-specific integrated circuit (ASIC) miners, the home computers are no longer capable of mining [25]. To address this issue, different mining algorithms have been proposed and examined. For example, the Ethash algorithm of Ethereum [63] and Equihash algorithm of Zcash [64] are ASIC-resistant PoW algorithms, which allow for the home computer-based mining through CPUs and GPUs. Moreover, some smart grid-specific mining strategies are also proposed. For example, based on CyClean in [65] and SolarCoin [66], the coins are mined in advance and are rewarded to local producers and consumers based on the generation and consumption of renewable energy, and the mining powers are distributed among nodes based on the holding rewards. For the consortium and private blockchains in smart grid, the trusted nodes that are typically selected from smart grid controlling authorities and distributed generation owners with large capacities will participate in consensus process.

The data flow through these networks is published on corresponding blockchains, and that published data (verified by the nodes) is used and communicated among networks with added security, transparency, automation, and privacy protection functionalities [67]. However, the existing research mainly focused on developing independent blockchains for specific applications in each communication network. Significant research efforts are still required to investigate different blockchains' interoperability, especially for the synchronization of data flow through different blockchains.

In smart grid, the smart generation, smart transmission and distribution, and smart homes/buildings are monitored and directly controlled by field IoT-enabled ICT devices, such as RTUs, IEDs, and WAMS for system operation, and AMIs for smart homes/building management [68]. By incorporating the field measurement and control blockchain with smart contracts to these IoT-enabled ICT devices in WAN, NAN, and SN/HAN, the field measurement data can be securely and automatically collected [69]. Further, with the DAPPS services, the blockchain-enabled AMIs can perform decentralized demand response, local power management, and local power trading within cyber-secured environment [70].

The field measurement data will be aggregated by selected data aggregators while utilizing data aggregation blockchain in WAN and NAN. The purpose of using blockchain for data aggregation is mainly for additional data confidentiality protection in smart grid [71]. After received by multiple receivers of meter operators or SCADA systems and data centers, the aggregated data will be automatically processed and stored by the data management blockchain with smart contracts and DAPPS services [72], where the blockchain can protect the integrity and auditability of stored data. For system operation blockchain within WAN, by utilizing the smart contracts and DAPPS services, the system operation decisions can be made automatically with less human interface, which can reduce the risk of cyber securities caused by human mistakes [73]. Also, the storage of historical records of decisions in blockchain can provide better audiability in smart grid.

The data flow within and among these four networks is verified and stored by the blockchains with a high degree of cyber security, and the replications of data storage across multiple devices can effectively protect the data availability from a single point of failure [74]. With the advancement in blockchain technology, power transaction functionality can be integrated using specially designed blockchain built over the DAPPS layer. For system operation, the blockchain is able to increase the cyber security and efficiency of wholesale electricity market [25]. Some start-up companies, such as Power Ledger, Grid+, and Greeneum, have started to use blockchain for local power transactions [59]. In this method, the authentication and authorization can be involved in power transactions at low risk of confidential breach, and the integrity, availability, and accountability/non-repudiation of transaction data can be well protected. In some works, the applications of blockchain for data management in EV charging stations are also investigated, which mainly aim at providing confidentiality protection and data availability.

B. Development Platforms for Smart Grid Cyber Security

Special applications and programs specific to smart grid can be developed on IBM and Microsoft Azure development environments which ensure cyber security of blockchain. Furthermore, the Ethereum platform can also be used to deploy smart contracts that are publicly available and verifiable. Ethereum development can be done on Microsoft Visual basic platform or online using Solidity remix. Ethereum platform is open-source, easy to implement, and has more security features; however, the usage of Ethereum for large-scale smart grid applications is inefficient, due to the gas limits and gas costs [75]. Like Ethereum, other platforms also support smart contract functionality, such as Quorum, Wan chain, Aternity, Zen, Counter party, Root Stock, Rchain, and Qtum. All these blockchains are different variants of Ethereum with some modifications. For example, Quorum has a major advantage of no gas usage for its transaction [76], which is more suitable in large-scale smart grid applications. Quorum platform comes with functionality that Solidity can be embedded [22]. Quorum is capable of executing private transactions between selected parties using constellation.

Some North American start-up companies have developed their blockchain platforms, which are specifically for smart grid. BTL is a Canadian company that is working on cross-border, large-scale, and cyber-secured power trading platform backed by Interbit private blockchain. Similarly, Drift is an American company working on efficient and secure grid transactions with multi-authentication and privacy protection on its blockchain. A German company is using IBM-Hyperledger fabric blockchain for P2P power transactions with integrity and confidentiality protection. Companies like Engro, Xi-Watt, and Consensys are using public blockchains for P2P power transactions. A Spain company, named Pylon Networks, uses the Litecoin public type blockchain for AMIs, aiming to provide high auditability for power tracing. Omega grid has developed smart grid management platform for cyber-secured system operation, which is based on privately running blockchain [77]–[80]. A start-up blockchain company named by Tenup proposes an architecture with high power efficiency for remote areas and works on a mixed consensus mechanism, in which the maximum transaction time is 60 seconds, which makes it useful for large-scale smart grid implementation [81].

TABLE II: A Summary of Reviewed Research Works for the Applications of Blockchain in Field Measurement and Communications

Works	Main contribution
[22], [42], [92], and [113]	Smart grid, blockchain, guaranteed immutability, mitigation of cyber attacks, data collection, transfer, and storage
[55], [93], and [94]	Smart grid, blockchain, big data analysis, secured and traceable data flow and storage
[95] and [96]	Smart grid, blockchain, big data sharing, bad data detection, data integrity protection
[101]-[103]	Smart grid, blockchain, real-time data storage and transfer, distributed cloud-based architecture, software defined networking, IoT system

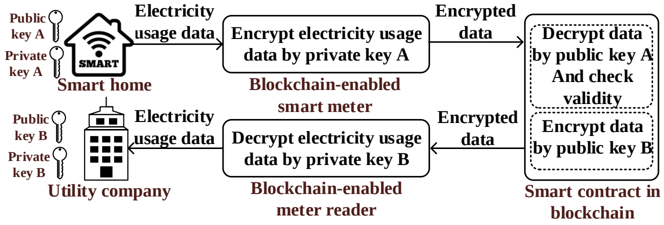
Public key A
Private key A
SMART
Smart home
Electricity usage data
Encrypt electricity usage data by private key A
Blockchain-enabled smart meter
Encrypted data
Decrypt data by public key A And check validity
Encrypt data by public key B
Smart contract in blockchain
Encrypted data
Decrypt electricity usage data by private key B
Blockchain-enabled meter reader
Electricity usage data
Public key B
Private key B
Utility company

Fig. 4: Operational procedure of blockchain-based smart meter [22].

IV. Applications of Blockchain in Smart Grid for Cyber Security

In literature, the research on blockchain for smart grid cyber security can be mainly categorized into three levels, i.e., field measurement and communications, power generation and transmission, and power distribution and utilization. In this section, the details of blockchain applications at different levels will be presented. The application of blockchain for smart grid cyber security against data integrity attack will be discussed in detail to better illustrate the cyber security mechanism of blockchain-based smart grid.

A. Blockchain for Field Measurement and Communications

Blockchain technology can have wide applications in smart grid for field measurement and communications, where a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2998479, IEEE Transactions on Industrial Informatics

summary of such research works is presented in Table II. IoT-enabled ICT devices connected to the nodes in a blockchain network to establish P2P communications in smart grid for field measurement data uploading, fetching, and transferring. For the stability and reliability of blockchain-based smart grid for cyber-secured field data measurement and transfer, all these ICT devices connected to this system should be perfectly synchronized with the deployed blockchain. In [44], [82], different types of architectures and synchronizing protocols have been explained and discussed. Selected IoT-enabled ICT devices are used to create a connection with blockchain network and to store the copies of blockchain and smart contracts locally [83]. Specific commands can be sent to blockchain using these ICT devices to initiate or call the smart contracts. For the case of AMIs in smart grid, they can be wirelessly connected to the blockchain and thus create a way to operate such devices on smart grid through blockchain [23], [84]. The power trading and security enhancement (ETSE) module, designated in [23], can be implemented to allow for the cyber-secured P2P communications among different AMIs within the same blockchain network. If the smart contracts are deployed on a particular part of smart grid, automated commands can be provided by blockchain to the smart grid.

Among different cyber attacks, the data integrity attack is a major threat in smart grid [85]–[87]. FDI attack is a type of cyber attack against data integrity, which stealthily manipulates the measurements [88]–[91]. Possible attacks include tampering with consumption data for fraudulent purposes, maliciously altering power trading transactions to destabilize the grid, invading customer's privacy by collecting and analyzing consumer data, and remotely controlling critical IEDs to switch them off [90]. Many papers have introduced firewall based methods to defend against such attacks. However, due to the low computational power of IoT-enabled ICT devices, such as AMIs, firewall techniques are sluggish and are vulnerable to cyber attacks cite44.

The blockchain has been proved to be a better and more efficient alternative to protect the smart grid against FDI attacks [92]. Some solutions are introduced in [22], [42], [92], [113] for using blockchain to provide guaranteed immutability of stored data, and mitigation of cyber attacks against data collection and transfer. In [22], the blockchain-based smart meter is proposed to protect the integrity and confidentiality of customers' electricity usage data. As shown in Fig. 4, the smart meter, and utility company have their public and private key pairs. The electricity usage data measured by smart meter are firstly encrypted by the private key of smart meter, i.e., private key A. Then, the smart contract in blockchain will decrypt the encrypted data by using the public key of smart meter, i.e., public key A, and check the validity. For the validity check, if public key A can successfully decrypt the encrypted data, then the encrypted data has not been compromised since the private key of smart meter can not be obtained by adversaries, which protects the data integrity. Further, the data will be encrypted by using the public key of the utility company, i.e., public key B, and only the utility company with the corresponding private key, i.e., private key B, can access the data. This can protect the confidentiality of customers' data.

Also, blockchain provides tamper-proof and traceable features for data flows, which are required in smart grid for data integrity and accountability/non-repudiation protections. In [55], [93], [94], blockchain is enabled for big data analysis with secured data flow and storage. If old data presented is faulty and is not trustable, all the future estimations and predictions will be inaccurate. For example, the wrong estimation of wind speed or solar intensity for a specific period can cause substantial economic loss and even destabilize the smart grid. A decentralized blockchain architecture with bad data detection mechanism is introduced in cite48 for secured and trustful big data analysis; however, the synchronization of blockchain and data fetch and upload delays have not been accounted for. These factors will affect the simulation timings and decrease the efficiency of big data analysis. To address this issue, Hyperledger fabric blockchain is used in [96] to work with crowdsourced power markets, which is fast because of the usage of PBFT consensus and is more secure.

In [72], [97], [98], surveys are conducted for blockchain usage for cyber security of IoT system, and blockchain-based marketplace for business models with blockchain-IoT combination is introduced. Comparisons among different blockchain architectures and their connection with IoT devices are explained in [57], [99]. Methods of using smart contracts with IoT devices are further elaborated, and some new robust techniques are introduced in [57]. Big data analysis for renewable power generation forecasting can be performed locally with less computing resources usage, and data can be published on blockchain in a tamper-proof manner, smart contracts will be executed based on the published forecasted data, automatically. Special blockchain developed in [94] is specific for big data analysis with proven high scalability and security; mechanisms of this can also be utilized to develop blockchain for more cyber-secured applications in smart grid.

In [100], a new cloud-based architecture for blockchain-based IoT system is proposed to improve the performances in real-time data storage and transfer with low latency. Distributed cloud-based architecture with controller fog nodes has been proven to be a good alternative, as they provide low-cost, secured, and on-demand access to the users [101]. Fog node is based on software-defined networking (SDN) and blockchain [100]. A significant reduction of end-to-end delay between IoT devices can be achieved in this architecture. In [102], a comparison among the speeds of some typical blockchains, e.g., Hyperledger fabric (i.e., PBFT consensus algorithm), Parity, Ethereum, and H-Store blockchains, has been conducted. H-Store can achieve the best throughput, while the throughput rate of Hyperledger fabric ranks second. Also, the P2P file system for data transfer based on blockchain is discussed in [103]. Inter Planetary File System (IPFS) can be used in combination with blockchain to achieve improved throughput, especially for big data analysis.

B. Blockchain for Power Generation and Transmission

In this section, the applications of blockchain for power generation and transmission will be discussed, where a summary of such research works is presented in Table III Along with

TABLE III: A Summary of Reviewed Research Works for the Applications of Blockchain in Power Generation and Transmission

Works	Main contribution
[59], [84], and [107] -[112]	Smart grid, blockchain, smart contracts, automatic P2P power transaction, local electricity market, cyber security, reduced cost
[77] and [113]-[115]	Smart grid, blockchain, smart contracts, DAPPS services, secured economic dispatch, electricity wholesale market, renewable power certification
[58] and [116]-[120]	Smart grid, blockchain, power system state estimation, system state integrity protection, improved bad data detection capability
[77], [121], and [122]	Smart grid, blockchain, smart contracts, secured dynamic load redistribution, differential voltage relays, voltage control transformers

the development of smart grid, the conventional non-renewable and centralized power generation is being replaced by renewable power-based DGs. The utilities usually face high costs for cyber-secured and efficient communications and control infrastructures to control these DGs in conventional centralized structure [104]. Also, the centralized control structure exposes the generation control of DGs to a single point of failure. To effectively and securely control the DGs, the idea of microgrid has emerged under the smart grid topic. In a microgrid, the local DGs, energy storage systems, and local power demands are controlled by microgrid operators to operate in either isolated or grid-connected mode. Then, the power generation and transmission for smart grid with integrated DGs at high penetration level can be effectively controlled by leveraging the microgrids using a decentralized multi-agent-based control system (DMACS) [44], [105], [106].

Based on the structure of DMACS for power generation and transmission systems, researchers have introduced the blockchain-based smart contracts to securely exchange power between consumers and prosumers within and among microgrids in local electricity market [59], [84], [107]–[112]. The main idea behind the blockchain-based smart contract functionality for local power transactions is to allow the consumers to buy power from local prosumers through P2P power transactions while encourage the local prosumers to help utility in meeting local demands [84], [107]. By using the blockchain-based smart contracts, the power generation by local DGs and power transmission through P2P power transactions can be verified and securely recorded in a blockchain without a third party's need. The transparency of blockchain can prevent fraud attempts in power trading processes [111]. The asymmetric cryptography and tamper-proof feature of blockchain can provide authentication and authorization to protect the integrity and accountability/non-repudiation of power transactions. Also, the public-private key pair in asymmetric cryptography can better protect the confidentiality of data [112].

Moreover, independence on a third party significantly reduces the power transaction costs, which further facilitates the usage of DGs [110]. Due to the cyber security and potential economic benefits that the blockchain can bring to the power generation and transmission, some start-up companies have developed their local electricity market platforms for the implementation of power transactions and power bidding backed by blockchain, including Piclo in the UK, Vandebron in the Netherlands, and Brooklyn Microgrid in the US. The details about these start-up companies and the practical application cases of blockchain in power generation and transmission are introduced in [109].

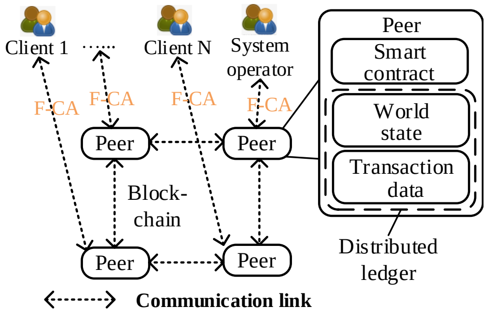

Fig. 5: Blockchain-assisted economic dispatch mechanism [113].

The optimization techniques, such as economic dispatch and dynamic load redistribution in transmission systems, can also be integrated with blockchain by leveraging smart contracts and DAPPS services [77], [113]. With blockchain, the economic dispatch function can automatically request the biddings from participating generators, clear the electricity wholesale market based on biddings, and make the requested power values and settled procurement electricity prices publicly available. In [113], a blockchain-assisted economic dispatch mechanism is proposed for power distribution system operation. As shown in Fig. 5, within blockchain, the peers are responsible for executing transactions and smart contracts, and maintaining the world state and transaction data as distributed ledgers. The clients and system operators join the blockchain by communicating with a peer through fabric certification (F-CA) mechanisms. After joining the blockchain, the clients will update their electricity usage/generation preferences, e.g., marginal costs for electricity generation and marginal utilities for electricity usage, and the updated preferences will be stored as world state in blockchain. The system operators can read the preference data from the world state and perform the economic dispatch to get the locational marginal electricity price, which will be used to form smart contracts. The smart contracts will be used by the peers to commit the power transactions among their corresponding clients automatically. This mechanism can significantly improve the efficiency and security of power system economic dispatches. This method offers data protection and resiliency against cyber attacks in electricity wholesale market, such as DoS attack on economic dispatch [114]. Further, the blockchain-enabled AMIs can also be implemented for renewable power certification [115].

The integrity and accountability/non-repudiation of distributed electric power system state estimation results are crucial for dynamic load redistribution in transmission systems. However, the current state estimation is vulnerable to FDI attacks. By utilizing the blockchain-enabled ICT devices in smart grid, the blockchain-based distributed state estimation function can reduce the risk of data tampering by providing integrity protection and help detect manipulations of data in addition to traditional bad data detection mechanisms [58].

TABLE IV: A Summary of Reviewed Research Works for the Applications of Blockchain in Power Distribution and Utilization

Works	Main contribution
[44], [125], [134], and [135]	HAN, blockchain, home energy management, bill data storage and access, remote bill payment , improved privacy protection and cyber security
[74], [132], [136], and [137]	Smart grid, blockchain, secured and trusted demand response, real-time electricity price publication, DAPPS services, demand response regulation, improved fairness and cyber security
[44], [82], [126]-[131], [138]-[143]	Smart grid, blockchain, smart contracts, automated and cyber-secured EV charging management, vehicle-to-grid/vehicle-to-vehicle service management, autonomous vehicles

Other severe data integrity attacks against state estimation, such as distributed DoS (DDoS), data framing, and cyber topology attacks, can also be defended using blockchain technology [116], [117]. For example, during DDoS attack, the AMIs communications is not functional, but DAPPS layer of blockchain can still provide actual data of power consumption [118]. Instead of protecting the measurement data from AMIs communication failure caused by DDoS attack, the blockchain-based IoT system can also support the smart grid for DDoS detection by using counter and comparator components implemented in the smart contract [119] and for DDoS prevention by implementing distributively static resource allocation mechanism on blockchian-based IoT system [120]. Moreover, the utility can easily and securely detect and redirect power to the affected area in case of an emergency, as SCADA and PLC control is available through smart contracts in blockchain network [118]. This enhances the performance of dynamic load redistribution in transmission system [121].

With the blockchain-based distributed state estimation function and embedded IoT system in smart grid, the blockchain can provide variant functionalities for secured and reliable distributed power transmission system operation [122]. For example, the static var compensator can be continuously and securely monitored and controlled using smart contract. Protection relays like long-distance and differential voltage relays can be controlled by distributed blockchain ledgers, which can prevent the loss of control signals. Voltage control transformers at transmission level can be monitored by a smart contract to provide automated functionality. Besides protecting data integrity and accountability/non-repudiation, the blockchain has a strong advantage in guaranteeing the data availability for distributed power transmission system operation [77]. Moreover, some parts of the computation power of blockchain can be potentially utilized to calculate demand forecasting and AC power flow in a distributed manner.

C. Blockchain for Power Distribution and Utilization

For power distribution and customer-side power utilization, the blockchain also provides a variant of cyber security functionalities [30], [44], [79], [82], [123]–[132]. A summary of such research works is shown in Table IV. The conventional power distribution system is typically designated with enough reserve of capacity to provide electrical power for the customers stably and is left with a low degree of monitoring and control. However, with the integration of DGs with bidirectional power flow and at high penetration level, the traditional load and power flow patterns have changed significantly. To address this issue, the power distribution system is being redeveloped to integrate a large amount of IoT-enabled ICT devices, to improve the system observability and controllability. This redeveloped power distribution system is defined as an active cyber-physical distribution system (A-CPDS) [133]. The P2P data transfer, cyber security, confidentiality protection, and transparency features of blockchain technology have made the blockchain a promising solution to improve the cyber security and efficiency of A-CPDS [132].

Under the context of A-CPDS, the smart homes equipped with a variant of IoT-enabled ICT devices, such as AMIs and power management systems, have created great interconnectivity between individual customer and electric grid. This improves the performance of power utilization on the customer side. However, the concerns about privacy leakage and smart grid data integrity attack caused by bad data intrusion from the customer side have greatly impeded the development of smart homes [68]. The blockchain has been seen as a suitable method to facilitate the development of smart homes by providing integrity, confidentiality, and accountability/non-reputation protections and improve the authentication/authorization levels for customer-side ICT devices [134].

In [134], [135], the private blockchain is established, based on the HAN, to allow for secured electrical appliances usage data uploading to the cloud server of power management system. The usage of private blockchain is to provide better privacy protection for customers. Based on the uploaded usage data, the policy for home power management can be implemented into the smart contract for automation control. Since the policy is replicated and stored distributively, any abnormal power usage action can be easily detected and analyzed [134]. Also, based on the blockchain cloud server for smart homes, the remote electricity bill payment function with high level of cyber security against theft of electricity is added in [44], [125]. With the blockchain-enabled smart meter, the electricity bill can be automatically generated and uploaded to the blockchain cloud server, which is tamper-proof. With the proper private key, the user can easily access the bill information and make payment remotely.

In addition to providing cyber security for integrity, confidentiality, and accountability/non-reputation of electricity usage bill, the blockchain-based remote electricity bill payment function can also significantly reduce the bill payment cost and settlement time [125]. In A-CPDS, the blockchain with smart contract functionality can also be used for secured and trusted demand response (DR) of smart homes [132], [136], [137]. By using blockchain technology, the latency of real-time electricity price publications can be reduced, which can guarantee the fairness and effectiveness of DR. Also, the smart contract can be used to ensure that the requested DR power is provided by the customers which can prevent fraud activities. Moreover, by leveraging the DAPPS services of blockchain for AMIs, the distributed DR can be implemented. The blockchain

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2998479, IEEE Transactions on Industrial Informatics

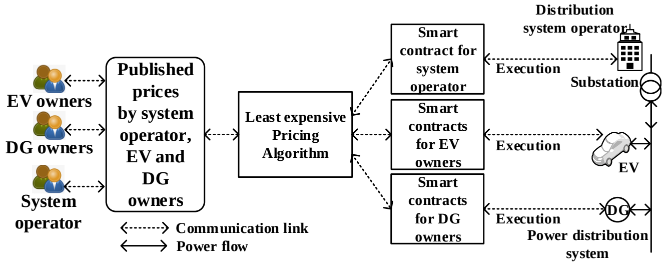
Distribution system operator
Smart contract for system operator
Execution
Substation
EV owners
DG owners
System operator
Published prices by system operator, EV and DG owners
Least expensive Pricing Algorithm
Smart contracts for EV owners
Execution
EV
Smart contracts for DG owners
Execution
DG
Power distribution system
Communication link
Power flow

Fig. 6: Blockchain-based G2V and V2G/V2V bidding platform [44].

can protect the availability of critical data, such as electricity pricing signal, ancillary service signal, and regional system states, for distributed DR. Also, the auditability of blockchain can ensure that the abnormal DR actions can be regulated and/or punished in a trust and fairway [74].

Further, the blockchain-enabled automated and cyber-secured machine-to-machine transactions, which includes auctions, bidding, and payment, can be utilized for the smart charging of EVs [138]. In [139], [140], the blockchain-based billing system for EV charging is investigated, where this billing system is designated for the electricity transaction between EV and charging station in grid-to-vehicle (G2V) mode. By using the blockchain-based billing system, the EV users can have a real-time charging price and immediately make the payment after charging services. Also, the mutual authentication for payment settlement in blockchain can guarantee that the payment is cleared only when the user and charging station provider agrees on the realized charging amount [139]. The cyber-resiliency nature of blockchain can protect the billing system from adversary data manipulation.

An extension of the blockchain-based billing system is proposed in [138], which also considers the autonomous EV charging optimization by using smart contract functionality in blockchain. By using smart contract, the EV users can request several bids from different charging stations to minimize the charging costs while satisfying the charging demand. Different from G2V mode, which considers only unidirectional power flow from grid to EV, the vehicle-to-grid (V2G) and vehicle-to-vehicle (V2V) modes can be used to balance the supply and demand, reduce load fluctuation, and support voltage stability in power distribution system [124].

The techniques proposed in [44], [82], [126], [140]–[143] introduce methodologies where connected EVs can request charging/discharging from the smart grid with blockchain-enabled trading platform, and they are given incentives if they support grid, through V2G or V2V, in return. For example, power can be exchanged among EVs and grid using AdBEV through the smart bidding algorithm implemented in the smart contract [44]. As shown in Fig. 6, the electricity prices for purchasing power from the grid, other EVs, and DGs can be published through blockchain for publicly reviewing, in which the integrity and confidentiality of the data can be well protected. The least expensive pricing algorithm implemented in the smart contract can be used to select the preferred power suppliers, and the smart contracts are issued between the users and selected power suppliers. After the mutual authentication of smart contracts, the power flow and payments can be automatically executed by the smart contracts without any delays. Due to the auditability of blockchain, the transaction and EV charging/discharging data can be easily traced, which can help the system analyze and identify any susceptible adversary behaviors.

IBM predicts that autonomous vehicles and self-driving cars will be in demand abundantly by 2020 [127]. In [128], cyber security for these vehicles are provided by blockchain-based IoT system. Data collected from sensors flow through the blockchain with smart contracts and DAPPS services with pre-defined logic. For example, if a sensor detects any issue with EV, based on smart contract, it will automatically schedule a booking with the manufacturer and will go there on a specified time. More blockchain-based processes such as fueling, charging, electronic parking, and repairs are introduced in [127]. These processes need high level of security and can only be handled by a trusted system, which is, in fact, the main feature of blockchain. The same process can be implemented on smart grid for automatic maintenance. Such add-ons in smart grid operation will provide customer satisfaction and increased levels of serviceability, reliability, and security.

Smart contract functionality backed by the proof of power algorithm is introduced in [129], which was adopted to reduce the consensus delay. This algorithm proves to be better for the case of peer to peer power transaction and can be beneficial for G2V and V2G/V2V. A comparison of this technique with Hyperledger-PBFT consensus can be done to obtain further insights into this consensus. Furthermore, proof of probability algorithm also shows good performance [130], which can also be adapted in grid space to achieve fewer transaction delays. Anonymous power trading between EVs is discussed in [131], with performance analysis and proof of practicality of blockchain for cyber-secured V2G/V2V applications.

V. Potential Future Research Directions

A comprehensive review for blockchain in smart grid for cyber security is presented above. In which, the system architectures, implementation platforms, and applications for field measurement and communications, power generation and transmission, and power distribution and utilization of blockchain for smart grid cyber security have been discussed. However, as an emerging technology, the usage of blockchain in smart grid still faces great challenges. In the rest of this section, some major issues that have not been fully considered in the research work for cyber security of blockchain-based smart grid mentioned above and recent advances in blockchain technologies for these challenges will be discussed. In the end, potential future research directions in power transmission and distribution systems will be highlighted.

A. *Major Issues and Recent Advances*

For the wide applications of blockchain for cyber security in smart grid, the size of distributed ledger will increase, and storage requirements will be enormous. This will slow down the blockchain network for data processing and affect the efficiency and reliability of smart grid operation. In [144], an efficient architecture based on network coding (NC) and distributed storage (DS) for blockchain storage is proposed to reduce the storage room and improve the efficiency of blockchain for large-scale applications. However, the framework proposed in this paper is vulnerable to pollution attacks. Advancement in this framework is being investigated to make it more robust against cyber attacks. Furthermore, a fast, low storage, and nonlinear fashioned blockchain is developed in [145], which utilizes a lightweight node to connect to the blockchain network. These lightweight nodes only carry the headers and are designated for verification without carrying much data. Such a blockchain was proven to be resilient to DDoS attacks and can provide better performances in robustness and efficiency compared with the NC- and DS-based architecture [146]. The study in [147] casts light on types of blockchains that can be used for industrial and other generic applications, and the work in [147] illustrates its applicability. Furthermore, researchers have discussed the impact of using different consensus algorithms on the performance of blockchain-based IoT systems. A more comprehensive analysis about these impacts can be found in [148], where the usage of PBFT consensus is studied in depth. Further, the comparison between PBFT and PoW in [149] proves that PBFT is more suitable for blockchain-based IoT systems.

Currently, the lack of scalability is still a great challenge impeding the practical applications of blockchain in smart grid for cyber security [150]. To address the scalability issue, consortium blockchain is used for cyber-secured microgrid operation in [150] [151] and data regulation mechanism in [71] for data aggregation in smart grid. The consortium blockchain introduced proves to be much faster and secure. Computational complexity in blockchain has been reduced significantly. Permissioned blockchain is used in [152] to perform a comparison between gas consumption with a focus on privacy in smart grid. The usage of such modified blockchains gives a better computational performance with a sacrifice on confidentiality protection. A fast and public blockchain is the best choice for blockchain operation in the smart grid. Yet, modifications are required to provide better privacy protection.

Numerous research works have tried to improve privacy protection by adopting an anonymous external system. For example, in [153], a blockchain-based anonymous reputation system (BARS) is established to provide a privacy-preserving trust model for public blockchains. By leveraging BARS, the certificate and revocation transparency can be effectively implemented in a public blockchain by leveraging the proofs of presence/absence for public keys. The usage of 5G technique is discussed in [154] for smart grid application to decrease the delay in communication time. However, high infrastructure costs will be a great challenge when it starts rolling out. Hyperledger fabric technology that gives owner authority to control the accesses of nodes has been proven to be a potential solution for cyber security of large-scale smart grid [155].

However, since Hyperledger fabric involves a small number of nodes and focuses mainly on the validation of data being added to a block, it still suffers from low cyber security levels [156]. In [156], a lightweight proof of block and trade (PoBT) consensus algorithm is proposed to improve the cyber security of private blockchains, which allows for both data and block validations. More importantly, with a varying number of participated nodes, the PoBT can achieve a better throughput rate and a lower communication bandwidth requirement than Hyperledger fabric. However, the PoBT proposed in [156] is explicitly designated for business applications, where a trusted certified authority is required to guarantee the security and efficiency of PoBT. In smart grid, there is a large number of authorities, e.g., transmission/distribution system operator (T/DSO), microgrid operator (MGO), and EV aggregator, and they represent different parties. There is no discussion in [156] on selecting a trusted certified authority out of a group of authorities representing different parties for the entire smart grid system, which causes great challenges for applying PoBT in smart grid. One possible solution to address this issue is considering the extension of PoBT consensus algorithm in [156] to consortium blockchains, with an added layer for trusted certified authority/authorities selection in a way similar to the voting process of PBFT consensus algorithm. Another possible solution is to leverage the cross-chain framework in smart grid. Multiple sidechains are established in the cross-chain framework for different application scenarios, e.g., distribution system management, microgrid operation, and EV charging management, with the main blockchain as the backbone. In this way, the trusted certified authority for each sidechain can be easily selected based on their application scenarios. In [157], the cross-chain framework for IoT data management has been studied. However, there are still many challenges that need to be addressed for the application of cross-chain framework in smart grid, e.g., the sidechain interoperability [158].

The public blockchain provides better cyber security by devoting the great computational power of mining nodes. However, the increasing computational power attributes great impacts on the energy efficiency of blockchain-based smart grid. For example, the widely used PoW consensus mechanism in public blockchain requires large energy consumption for the consensus process and has a significant carbon footprint and electronic waste. The existing consensus mechanism is not in support of the sustainable development of smart grid. The design of proper incentive and penalty mechanisms that encourage the reduction of energy consumption and usage of renewable energy generation for consensus mechanisms is a crucial future research direction for the particular application of blockchain in smart grid.

Since blockchain still suffers from several cyber security vulnerabilities [159], the integration of blockchain may expose smart grid to new types of cyber security issues. In the past few years, cryptanalysis of hash function has been an active research area, and various types of cyber attacks against hash function in blockchain have been proposed [160]. With the successful alternating hash function, the transaction malleability attack can mislead the energy consumers in P2P energy transactions to pay twice. A routing attack that partitions the blockchain network that prevents nodes from communicating with each other is able to tamper data in smart grid through delay attack. Targeting on the whole blockchain network, the DDoS cyber attack can disconnect multiple nodes from the network. As an important component of blockchain-based smart grid, smart contracts' vulnerabilities have severe impacts

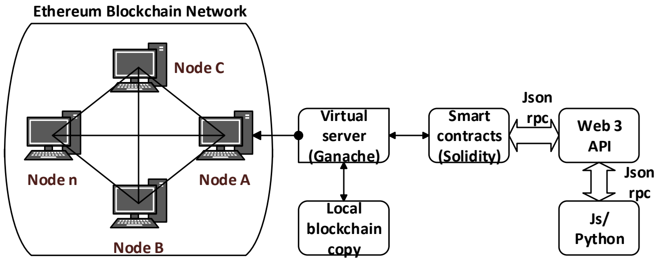

Fig. 7: Voltage profile stabilization using smart contracts.

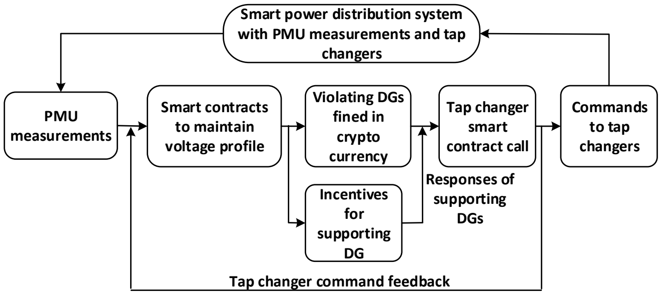
Smart power distribution system with PMU measurements and tap changers
PMU measurements
Smart contracts to maintain voltage profile
Violating DGs fined in crypto currency
Tap changer smart contract call
Commands to tap changers
Incentives for supporting DG
Responses of supporting DGs
Tap changer command feedback

Fig. 8: Interface of testing system for smart contract in smart grid.

on the stability and reliability of smart grid operation. As discussed in [161], the smart contracts can be easily tampered through alternating source code, penetrating virtual machines, and modifying runtime environment. Moreover, usability is also a big challenge as some users may lose their private keys, which lead to their accounts get locked forever. Some of these issues are already corrected by new blockchains, but that leads to decreased privacy of the users. Currently, such trade-offs still require great attention. Cyber attacks on blockchain like DAO, which occurred in 2016 on Ethereum, only strengthened and helped evolve this technology to be more cyber-resilient and robust [162]. Attacks like these will expose more loopholes in the coming future.

Several blockchain technologies that differ from each other in protocols, mechanisms, and techniques are being investigated and developed for blockchain-based smart grids. Also, due to the geographical and operational complexities of smart grid, multiple blockchains may be required to achieve effective operation of smart grid, among which different entities may be responsible for different blockchains with distinctive objectives. However, there still lacks proper and widely accepted standards for seamless interoperability among different blockchains with unique technologies. Therefore, there is an urgent need to achieve blockchain standardization in smart grid under no centralized authority that allows for seamless, cyber-resilient, and efficient exchange of data among different blockchains with distinctive technologies and objectives. Blockchain technology is an excellent alternative to many, but it still needs more refinement, especially for smart grid.

B. Potential Future Research Directions

To better address the issues mentioned above, some research topics can be further studied. The development of blockchain-based smart grid framework with an intrusion detection system and DAPPS specifically for smart grid applications can be studied further with different architectures. Testing framework for blockchain-enabled smart grid can be investigated and developed, considering DDoS attacks, Sybil attacks, routing attacks, and man-in-the-middle attacks. In this paper, we will highlight the potential future research directions in power transmission and distribution systems.

1) Distributed Power Transmission System Monitoring: The blockchain with smart contract functionalities may be implemented in a distributed manner, in which the blockchain network of the whole transmission system can be established by incorporating multiple distributed blockchain networks. This enables the distributively and cyber-secured monitoring and control of transmission system, which can potentially address the increased penetration level of DGs and prevent the power transmission system operation from a single point of failure. For example, a power transmission system may be divided into different regions, which are monitored by different sets of IoT-enabled ICT devices with smart contracts that contain controlling logic and algorithms. One region may be selected as the command center, and a mechanism can be developed to invoke contracts between divided regions while considering the synchronization of measurements and control signals. Also, the distributed control algorithm is required to allow for each divided region having its subcontracts for controlling generation and utilization within its region.

2) Power Distribution System Automation System: The blockchain-based smart contracts may also be developed with complex algorithms for cyber-secured RTUs and IEDs control in smart grid. For example, in power distribution system, blockchain-based smart contracts can be used to control tap changers for voltage regulation. A potential control procedure for blockchain-based voltage regulation is shown in Fig.7. The smart contracts can be deployed in PMUs to measure voltage levels. The measurements can be published on a public blockchain and used by the smart contracts deployed in tap changers to stabilize the voltage levels. The smart contracts may also be deployed in DG controllers and used to command the DG outputs to respond to voltage regulation requirements. Further, a performance scoring mechanism can be developed to find the DGs that violate voltage regulation requirements and credit the supporting DGs by using smart contracts. Moreover, a testing system based on a common blockchain platform can be developed to test the blockchain-based smart grid control system. The Ethereum blockchain with a flexible smart contract design feature may be used as the blockchain network for the testing system. A potential interface of Ethereum-based testing system is shown in Fig. 8. In the testing system, some common coding languages, e.g., JavaScript and Python, can be used to encode the smart contracts. Also, smart contracts need to be able to interact with the Ethereum blockchain network. A potential method is to embed smart contracts in Solidicity in the local server, then interact with Ethereum blockchain through Ganache virtual server.

VI. Conclusion

With the development of smart grid, new challenges arise to improve the cyber security of smart grid. Many methods have been proposed to make the smart grid more resilient against cyber attacks. Among these methods, the blockchain is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2020.2998479, IEEE Transactions on Industrial Informatics

a promising solution for protecting smart grid cyber security. In this paper, a comprehensive review of blockchain-based protection mechanism for cyber security of smart grid is conducted. Data protection is enabled by storing data in blockchain network and is validated by peers within the same network. The verified data can then be used for advanced smart grid operations, such as load forecasting, local redistribution, and demand response. Blockchain-based platforms, applications, and services suitable for smart grid with an emphasis on cyber-security are studied in-depth in this paper. Many types of applications can be structured on blockchain DAPPS layer, which helps establish control of smart grid with security over cloud and autonomy. Therefore, blockchain can improve the cyber security for data collection, storage, transfers, as well as control execution in smart grid. Blockchain is a promising solution for smart grid cyber security improvement. However, there are still great challenges from both the perspective of the vulnerabilities of blockchian technologies and the implementation of blockchain in smart grid. In this paper, the potential future research directions are discussed in detail to provide some guidance for the research on blockchain-based smart grid.

References

[1] C. Greer, D. A. Wollman, D. E. Prochaska, and P. A. Boynton, *NIST framework and roadmap for smart grid interoperability*. Accessed: Aug. 11, 2019. [Online]. Available: https://www.nist.gov.

[2] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 24442453, Sep. 2015.

[3] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Mag.*, vol. 8, no. 1, pp. 18-28, July 2010.

[4] A. Stefanov and C. Liu, "Cyber-power system security in a smart grid environment," in *Proc. IEEE ISGT'12*, Jan. 2012.

[5] Electricity Information Sharing and Analysis Center, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Accessed: Aug. 11, 2019. [Online]. Available: https://ics.sans.org/media/E-ISAC.

[6] *The Highly Dangerous 'Triton' Hackers Have Probed the US Grid*. Accessed: Aug. 11, 2019. [Online]. Available: https://www.wired.com/story/triton-hackers-scan-us-power-grid.

[7] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain based solutions to security and privacy issues in the internet of things," *IEEE Wirel. Commun.*, vol. 25, no. 6, pp. 12-18, Dec. 2018.

[8] M. Curiale, "From smart grids to smart city," in *Proc. IEEE SASG*, Dec. 2014.

[9] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A Survey of blockchain technology applied to smart cities: research issues and challenges," in *Proc. IEEE Commun. Surv. Tutor.*, Feb. 2019.

[10] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. ElGhazi, "Cybersecurity in smart grid: Survey and challenges," *Comput. Elect. Eng.*, vol. 67, no. 1, pp. 469482, Apr. 2018.

[11] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Datastream based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study," *IEEE Syst. J.*, vol. 9, no. 1, pp. 3144, Mar. 2015.

[12] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls Into the Modern Power Infrastructure*. Waltham, MA, USA: Syngress, 2013.

[13] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali, "Smart grid cyber security: challenges and solutions," in *Proc. IEEE ICSGCE*, Oct. 2015.

[14] R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 2871-2881, May 2019.

[15] M. R. Asghar, G. Dan, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: a survey," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 4, pp. 2820-2835, Sept. 2017.

[16] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 998-1010, Sept. 2012.

[17] A. Bani-Ahmed, M. Rashidi, A. Nasiri, and H. Hosseini, "Reliability analysis of a decentralized microgrid control architecture," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3910-3918, July 2019.

[18] Q. Yu, "Design, implementation, evaluation of a blockchain-enabled multi-energy transaction system for district energy systems," *M.S thesis, ETH Zurich Research Collection*, Apr. 2018.

[19] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, no. 1, pp. 22922303, May. 2016.

[20] M. Marchesi, "Why blockchain is important for software developers, and why software engineering is important for blockchain software," in *Proc. IEEE IWBOSE'18*, Mar. 2018.

[21] P. Danzi, M. Angjelichinoski, C. Stefanovic, and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," in *Proc. IEEE SmartGridComm'17*, Oct. 2017.

[22] T. M. G. L. Winter, "The advantages and challenges of the blockchain for smart grids," *M.S thesis, TU Delft University of Technology*, May 2018.

[23] F. Lombard, L. Aniello, S. D. Angelis, A. Margheri, and V. Sassone., "A blockchain based infrastructure for reliable and cost-effective IoT-aided smart grids," in *Proc. IEEE iThings'18*, Mar. 2018.

[24] G. C. Lazaroiu, "Blockchain and smart metering towards sustainable prosumers," in *Proc. IEEE SPEEDAM'18*, Jun. 2018.

[25] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: a systematic review of challenges and opportunities," *Renew. Sustain Energy Rev.*, vol. 100, pp. 143-174, Feb. 2019.

[26] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain applications in smart gridreview and frameworks," *IEEE Access*, vol. 7, pp. 86746-86757, June 2019.

[27] J. Abdella and K. Shuaib, "Peer to peer distributed energy trading in smart grids: s survey," *Energies*, vol. 11, no. 6, pp. 1560-1573, May 2018.

[28] P. Siano, G. De Marco, A. Rolan, and V. Loia, "A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets," *IEEE Syst. J.*, vol. 13, no. 3, pp. 3454-3466, Sept. 2019.

[29] R. Kuhn, D. Yaga, and J. Voas, "Rethinking distributed ledger technology," in *Computer*, vol. 52, no. 2, pp. 68-72, Feb. 2019.

[30] M. Mylrea and S. N. G. Gourisetti, "Blockchain: a path to grid modernization and cyber resiliency," in *Proc. IEEE NAPS'17*, Sep. 2017.

[31] S. Li, "Application of blockchain technology in smart city infrastructure," in *Proc. IEEE SmartIoT'18*, Aug. 2018.

[32] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328-22370, Jan. 2019.

[33] E. B. Hamida, K. L. Brousmiche, H. Levard, and E. Thea, "Blockchain for enterprise: overview, opportunities and challenges," in *Proc. ICWMC'13*, Jul. 2017.

[34] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 31543164, May 2017.

[35] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: a comprehensive survey," in *Proc. IEEE Commun. Surv. Tutor.*, Dec. 2018.

[36] Z. Ma, W. Huang, and H. Gao, "Secure DRM scheme based on blockchain with high credibility," *Chinese J. Electron.*, vol. 27, no. 5, pp. 1025-1036, Sep. 2018.

[37] S. Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*. Accessed: 22 March 2018. [Online]. Available: https://bitcoin.pdf.

[38] X. Wu, B. Duan, Y. Yan, and Y. Zhong, "M2M blockchain: the case of demand side management of smart grid," in *Proc. IEEE ICPADS'17*, Dec. 2017.

[39] M. T. Devine and P. Cuffe, "Blockchain electricity trading under demurrage," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2323-2325, Mar. 2019.

[40] D. Fakhri and K. Mutijarsa, "Secure IoT communication using blockchain technology," in *Proc. IEEEISESD'18* Oct. 2018.

[41] M. M. Esfahani and O. A. Mohammed, "Secure blockchain-based energy transaction framework in smart power systems," in *Proc. IEEE IECON'18*, Oct. 2018.

[42] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Trans. Syst. Man Cybern. Syst.*, Feb. 2019.

[43] Bitcoin Project Group, *The Bitcoin project*. Accessed: Mar. 22, 2018. [Online]. Available: https://Bitcoin.org, 2018-3-16.

[44] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 2565725665, May 2018.

[45] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized applications: the blockchain empowered software system," *IEEE Access*, vol. 6, pp. 53019-53033, Sep. 2018.

[46] C. Ehmke, F. Wessling, and C. M. Friedrich, "Proof-of-property - a lightweight and scalable blockchain protocol," in *Proc. IEEE/ACM WETSEB'18*, May - Jun. 2018.

[47] D. Mechkaroska, V. Dimitrova, and A. Popovska-Mitrovikj, "Analysis of the possibilities for improvement of blockchain technology," in *Proc. IEEE TELFOR'18*, Nov. 2018.

[48] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: a scalable blockchain protocol," in *Proc. NSDI'16*, Mar. 2016.

[49] Z. Qi, Y. Zhang, Y. Wang, J. Wang, and Y. Wu, "A cascade structure for blockchain," in *Proc. IEEE HotICN'18*, Aug. 2018.

[50] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things*, vol. 6, no. 3, pp. 4650-4659, June 2019.

[51] K. Shudo, R. Kanda, and K. Saito, "Towards application portability on blockchains," in *Proc. IEEE HotICN'18*, Aug. 2018.

[52] R. Abe, K. Nakamura, K. Teramoto, and M. Takahashi, "Attack incentive and security of exchanging tokens on proof-of-work blockchain," in *Proc. AINTEC '18*, Nov. 2018.

[53] M. Westerkamp, "Verifiable smart contract portability," in *Proc. IEEE ICBC'19*, May 2019.

[54] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K. L. Tan, Untangling blockchain: a data processing view of Blockchain systems, in *IEEE TKDE*, vol. 30, no. 7, pp. 13661385, Jul. 2018.

[55] H. Hassani, X. Huang, and E. Silva, "Big-crypto: big data, blockchain and cryptocurrency," *BDCC*, vol. 2, no. 4, pp. 34-50, June 2018.

[56] S. Aggarwal, R. Chaudhary, G.S. Aujla, A. Jindal, A. Dua, and N. Kumar, "EnergyChain: enabling energy trading for smart homes using blockchains in smart grid ecosystem," in *Proc. ACM NCSC'18*, Jun. 2018.

[57] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: challenges and directions," *IEEE Secur. Priv.*, vol. 16, no. 4, pp. 3845, Aug. 2018.

[58] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: exchanging distributed energy at speed, scale and security," in *Proc. IEEE RWS'17*, Sept. 2017.

[59] E. R. Sanseverino, M. L. D. Silvestre, P. Gallo, G. Zizzo, and M. Ippolito, "The blockchain in microgrids for transacting energy and attributing losses," in *Proc. IEEE GreenCom'17*, Jun. 2017.

[60] Z. Guan, G. Si ; X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82-88, July 2018.

[61] I. Ullah and Q. H. Mahmoud, "An intrusion detection framework for the smart grid," in *Proc. IEEE CCECE'17*, Apr. 2017.

[62] T. Alladi, V. Chamola, J. J. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: a review on different use cases," *Sensors*, vol. 19, no. 22, pp. 4862, Nov. 2019.

[63] V. Buterin, *The Ethereum project*. Accessed: Nov. 12, 2019. [Online]. Available: https://www.Ethereum.org.

[64] Zcash, *Privacy-protecting digital currency*. Accessed: Nov. 12, 2019. [Online]. Available: https://z.cash/.

[65] M.B. Mollah, J. Zhao, D. Niyato, K. Y. Lam, X. Zhang, A. M.Y.M. Ghias, L. H. Koh, and L. Yang, *Blockchain for future smart grid: a comprehensive survey*. Accessed: Sept. 15, 2019. [Online]. Available: https://arxiv.org/pdf/1911.03298.pdf.

[66] SolarCoin, *One megawatt hour one SolarCoin*. Accessed: Sept. 15, 2019. [Online]. Available: https://solarcoin.org/wp-content/uploads/SolarCoinPresentation.pdf.

[67] J. Fiaidhi, S. Mohammed, and S. Mohammed, "EDI with blockchain as an enabler for extreme automation," in *IT skilled*, vol. 20, no. 4, pp. 6672, Aug. 2018.

[68] B.L.R. Stojkoska and K.V. Trivodaliev, "A review of Internet of Things for smart home: challenges and solutions," *J. Clean Prod.*, vol. 140, n0. 3, pp. 1454-1464, Jan. 2017.

[69] A. Pieroni, N. Scarpato, L. D. Nunzio, F. Fallucchi, and M. Raso, "Smarter city: smart energy grid based on blockchain technology," *IJASEIT*, vol. 8, no. 1, pp. 298-307, Sept. 2018.

[70] S. Noor, W. Yang, M. Guo, K. H. van Dam, and X. Wang, "Energy demand side management within micro-grid networks enhanced by blockchain," *Appl. Energy*, vol. 228, no. 15, pp. 1385-1398, Oct. 2018.

[71] M. Fan and X. Zhang, "Consortium blockchain based data aggregation and regulation mechanism for smart grid," *IEEE Access*, vol. 7, no. 1, pp. 35929-35940, Mar. 2019.

[72] T. H. Kim and J. Lampkins, "BRICS: blockchain based resilient information control system," in *Proc. IEEE Big Data'18*, Dec. 2018.

[73] L. Thomas, Y. Zhou, C. Long, J. Wu, and N. Jenkins, "A general form of smart contract for decentralized energy systems management," *Nature Energy*, vol. 4, no. 1, pp. 140-149, Jan. 2019.

[74] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids", *SENSORS*, vol. 18, no. 1, pp. 162, Jan. 2018..

[75] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. Rahman, *Blockchain-based privacy-preserving charging coordination mechanism for energy storage units*. Accessed: Mar. 22, 2018. [Online]. Available: https://arxiv.org/abs/1811.02001.

[76] J. P. Morgan, *Quorum, advancing blockchain technology*. Accessed: 23-Mar-2018. [Online]. Available: https://www.jpmorgan.com/global/Quorum.

[77] D. Livingston, V. Sivaram, and M. Freeman, *Applying blockchain technology to electric power systems*. Accessed: Mar. 22, 2018. [Online]. Available: https://cfrd8-files.cfr.org. [Accessed: Mar. 22, 2018].

[78] G. Zizzo, E. R. Sanseverino, M. G. Ippolito, M. L. D. Silvestre, and P. Gallo, "A technical approach to P2P energy transactions in microgrids," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4792-4803, Nov. 2018.

[79] J. A. F. Castellanos, D. Coll-Mayor, and J. A. Notholt, "Cryptocurrency as guarantees of origin: simulating a green certificate market with the Ethereum blockchain," in *Proc. IEEE SEGE'17*, Aug. 2017.

[80] H. N. Vaibhav Saini, *An encyclopedia of 40+ smart contract platforms*. Accessed: 19-Jan-2019. [Online]. Available: https://hackernoon.com/contractpedia-an-encyclopedia-of-40-smart-contract-platforms-4867f66da1e5.

[81] Tenup Team, *Tenup white paper*. Accessed: Mar. 22, 2018. [Online]. Available: https://tenup.io/Content/TenUp-Whitepaper.pdf.

[82] P. Danzi, A. E. Kalr, . Stefanovi, and P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices," in *Proc. IEEE ICC'18*, May. 2018.

[83] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou, and B. Zhang, "A high performance blockchain platform for intelligent devices," in *Proc. IEEE HotICN'18*, Aug. 2018.

[84] C. Plaza, J. Gil, F. D. Chezelles, and K. A. Strang, "Distributed solar self consumption and blockchain solar energy exchanges on the public grid within an energy community," in *Proc. IEEE EEEIC'18*, Jun. 2018.

[85] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 33173318, Jul. 2017.

[86] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *ICS E-ISAC*, vol. 1, no. 1, pp.1-29, Mar. 2016.

[87] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 16301638, Jul. 2017.

[88] A. Rahman and H. Mohsenian-rad, "False data injection attacks against nonlinear state estimation in smart power grids," in *Proc. IEEE PESGM'13*, Nov. 2013.

[89] J. Zhu and X. Wei, "Defending false data injection attacks against power system state estimation: a stealthiness corruption oriented method," in *Proc. IEEE POWERCON'16*, Sep. 2016.

[90] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Informat*, vol. 11, no. 5, pp. 11981209, Oct. 2015.

[91] S. Tan, W. Song, S. Member, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in

smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 313-322, Jan. 2018.

[92] M. N. Kurtm, Y. Yilmaz, and X. Wang, "Secure distributed dynamic state estimation in wide-area smart grids," *CoRR*, vol. 1, no. 1, pp. 1902-1918, Jul. 2019.

[93] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *Proc. IEEE BIGCOM'17*, Aug. 2017.

[94] E. Bandara, W. K. Ng, K. D. Zoysa, N. Fernando, S. Tharaka, P. Maurakirinathan, and N. Jayasuriya, "Mystiko blockchain meets big data," in *Proc. IEEE Big Data'18*, Dec. 2018.

[95] L.Yue, H.Junqin, Q.Shengzhi, and W.Ruijin, "Big data model of security sharing based on blockchain," in *Proc. IEEE 2017 BDCC'17*, Aug. 2017.

[96] F. Luo, J. Zhao, Z. Y. Dong, Y. Chen, Y. Xu, X. Zhang, and K. P. Wong., "Cloud based information infrastructure for next generation power grid: conception, architecture, and applications," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 18961912, Jul. 2016.

[97] P. K. Sharma, M. Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, no. 1, pp. 115124, Sep. 2018.

[98] T. M. Fernndez-Carams and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, no. 1, pp. 3297933001, May. 2018.

[99] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, no. 1, pp. 18611-18621, Jan. 2019.

[100] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: a data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 13661385, Jul. 2018.

[101] S. Prianga, R. Sagana, and E. Sharon, "Evolutionary survey on data security in cloud computing using blockchain," in *Proc. IEEE ICSCA'18*, Jul. 2018.

[102] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved P2P file system scheme based on IPFS and Blockchain," in *Proc. IEEE Big Data'17*, Dec. 2017.

[103] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. R. Sanseverino, and G. Zizzo, "A technical approach to the energy blockchain in microgrids," *IEEE Trans. Ind. Informat.* , vol. 14, no. 11, pp. 47924803, Nov. 2018.

[104] S. Mhanna, A. C. Chapman, and G. Verbic, "A fast distributed algorithm for large-scale demand response aggregation," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 20942107, Jul. 2016.

[105] K. Dehghanpour, C. Colson, and H. Nehrir, "A survey on smart agent-based microgrids for resilient/self-healing grids," *Energies*, vol. 10, no. 5, pp. 620-645, May 2017.

[106] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, pp. 162-184, Jan. 2018.

[107] A. Goranovic, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl, and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," in *Proc. IEEE IES'17*, Oct. 2017.

[108] M. Faschang, T. G. Deutsch, and G. Kienesberger, "Transition roadmap from centralized to massively decentralized grid control systems," *Wissenschaftlicher Bericht fur die FFG Eigenverlag der Energy&IT Group*, pp. 75, 2015, ISBN 978-3-200-04337-4.

[109] A. Paudel, K. Chaudhari, C. Long, and H. B. Gooi, "Peer-to-Peer energy trading in a prosumer based community microgrid: a game-theoretic model," *IEEE Trans. Ind. Electron.*, vol. 66, no. 8, pp. 6087-6097, Aug. 2019.

[110] E. Munsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *Proc. IEEE CCTA'17*, Aug. 2017.

[111] A. Alam, M. T. Islam, and A. Ferdous, "Towards blockchain-based electricity trading system and cyber resilient microgrids," in *Proc. ECCE'19*, Feb. 2019.

[112] S. J. Pee, E. S. Kang, J. G. Song, and J. W. Jang, "Blockchain based smart energy trading platform using smart contract," in *Proc. ICAIIC'19*, Feb. 2019.

[113] S. Wang, A. F. Taha, and J. Wang, "Blockchain assisted crowd-sourced energy systems," in *Proc. IEEE PESGM'18*, Aug. 2018.

[114] J. Kim, L. Tong, and R. J. Thomas, "Dynamic attacks on power systems economic dispatch," in *Proc. IEEE ACSSC'15*, Nov. 2015.

[115] D. Canto and D. Enel, "Blockchain: which use cases in the energy industry," in *Proc. IET CIRED'17*, June 2017.

[116] K. Singh and S. C. Choube, "Using blockchain against cyber attacks on smart grids," in *Proc. IEEE SCEECS'18*, Feb. 2018.

[117] H. Sedjelmaci and S. M. Senouci, "Smart grid security: a new approach to detect intruders in a smart grid neighborhood area network," in *Proc. IEEE WINCOM'16*, Oct. 2016.

[118] J. Gao, K. O. Asamoah, E.l B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, and G. Dong, "Grid monitoring: secured sovereign blockchain based monitoring on smart grid," *IEEE Access*, vol. 6, no. 1, pp. 99179925, Feb. 2018.

[119] Z. Ahmed Khan, N. Afaqui, and O. Humayun, "Detection and prevention of DDoS attacks on software defined networks controllers for smart grid," *IJCA*, vol. 181, no. 45, pp.16-21, Mar. 2019.

[120] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating loT device based DDoS attacks using blockchain," in *Proc. CryBlock'18*, June 2018.

[121] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 112, Mar. 2018.

[122] C. Burger, A. Kuhlmann, P. Richard, J. Weinmann, "Blockchain in the energy transition: a survey among decision-makers in the German energy industry," *Deutsche Energie-Agentur GmbH (dena) - German Energy Agency*, Nov. 2016.

[123] M. E. Elkhatib, R. E. Shatshat, and M. M. A. Salama, "Decentralized reactive power control for advanced distribution automation systems," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1482-1490, Sep. 2012.

[124] W. Tang, S. Bi, and Y. J. A. Zhang, "Online coordinated charging decision algorithm for electric vehicles without future information," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 28102824, Nov. 2014.

[125] L. DOriano, G. Mastandrea, G. Rana, G. Raveduto, V. Croce, M. Verber, and M. Bertoncini, "Decentralized blockchain flexibility system for smart grids: requirements engineering and use cases," in *Proc. IEEE CANDO-EPE'18*, Nov. 2018.

[126] C. Liu, K. K. Chai, E. T. Lau, Y. Wang, and Y. Chen, "Optimised electric vehicles charging scheme with uncertain user-behaviours in smart grids," in *Proc. IEEE PIMRC'17*, Oct. 2017.

[127] B. A. Scriber, "A framework for determining blockchain applicability," *IEEE Softw.*, vol. 35, no. 4, pp. 7077, Jul. 2018.

[128] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "Trust chain: establishing trust in the iot based applications ecosystem using blockchain," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 1223, Aug. 2018.

[129] P. Siano, G. De Marco, A. Roln, and V. Loia, "A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets," *IEEE Syst. J.*, Mar. 2019.

[130] S. Kim and J. Kim, "Mining with proof of probability in blockchain," in *Proc. ACM ASIACCS'18*, Jun. 2018.

[131] H. Wang, Q. Wang, D. He, Q. Li, and Z. Liu, "BBARS: blockchain based anonymous rewarding scheme for V2G networks," in *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3676 - 3687, Jan. 2019.

[132] P. Danzi, S. Hambridge, . Stefanovi, and P. Popovski, "Blockchain-based and multi-layered electricity imbalance settlement architecture," in *Proc. IEEE SmartGridComm'18*, Oct. 2018.

[133] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 7096-7108, Nov. 2018.

[134] Y. N. Aung and T. Tantidham, "Review of Ethereum: smart home case study," in *Proc. IEEE InCIT'17*, Nov. 2017.

[135] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, "A blockchain-based energy trading platform for smart homes in a microgrid," in *Proc. IEEE ICCCS'18*, Apr. 2018.

[136] Pop Claudia, Tudor Cioara, Marcel Antal, Ionut Anghel, Ioan Salomie, and Massimo Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, pp. 162-183, Jan. 2018.

[137] X. Luo, J. Wang, M. Dooner, and J. Clarke, "Overview of current development in electrical energy storage technologies and the application potential in power system operation," *Appl. Energy*, vol. 137, no. C, pp. 511-536, Jan. 2015.

[138] M. Pustiek, A. Kos, and U. Sedlar, "Blockchain based autonomous selection of electric vehicle charging station," in *Proc. IEEE IIKI'16*, Oct. 2016.

[139] S. Jeong, N. Dao, Y. Lee, C. Lee, and S. Cho, "Blockchain based billing system for electric vehicle and charging station," in *Proc. IEEE ICUFN'18*, July 2018.

[140] N. H. Kim, S. M. Kang, and C. S. Hong, "Mobile charger billing system using lightweight Blockchain," in *Proc. APNOMS'17*, Sept. 2017.

[141] P. Fraga-Lamas and T. M. Fernndez-Carams, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578-17598, Jan. 2019.

[142] K. Xiang, B. Chen, H. Lin, Y. Shen, Y. Du, and T. Yan, "Automatic demand response strategy of local pure electric vehicle with battery energy storage system based on blockchain technology," in *Proc. IEEE EI2'18*, Nov. 2018.

[143] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184-192, Nov. 2018.

[144] J. Hinckeldeyn and K. Jochen, "Developing a smart storage container for a blockchain based supply chain application," in *Proc. IEEE CVCBT'18*, Nov. 2018.

[145] Y. Xu, "Section-Blockchain: a storage reduced blockchain protocol, the foundation of an autotrophic decentralized storage architecture," in *Proc. IEEE ICECCS'18*, Dec. 2018.

[146] M. Saad, M. T. Thai, and A. Mohaisen, "Deterring DDoS attacks on blockchain based cryptocurrencies through mempool optimization," in *Proc. ACM ASIACCS'18*, Jun. 2018.

[147] H. Sukhwani, J. M. Martnez, X. Chang, K. S. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network," in *Proc. IEEE SRDS'17*, Sep. 2017.

[148] M. Vukolic , "The quest for scalable blockchain fabric: proof of work vs BFT replication," in *Proc. iNetSec'15*, May 2015.

[149] D. Miller, "Blockchain and the internet of things in the industrial sector," *IT Prof.*, vol. 20, no. 3, pp. 1518, May. 2018.

[150] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," *IEEE Access*, vol. 6, no. 1, pp. 2297022975, Mar. 2018.

[151] J. Bergquist, A. Laszka, M. Sturm, and A. Dubey, "On the design of communication and transaction anonymity in blockchain based transactive microgrids," in *Proc. ACM SRIDL'17*, Dec. 2017.

[152] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy preserving smart grid networks," *IEEE Internet Things J.*, Mar. 2019.

[153] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, no. 1, pp. 45655-45664, Aug. 2018.

[154] K. Valtanen, J. Backman, and S. Yrjola, "Blockchain powered value creation in the 5G and smart grid use cases," *IEEE Access*, vol. 7, no. 1, pp. 25690-25707, Feb. 2019.

[155] The Linux Foundation, *The hyperledger project: august 12, 2015*. Accessed: Mar. 22, 2018. [Online]. Available: https://www.hyperledger.org.

[156] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: a lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343-2355, March 2020.

[157] Y. Jiang, C. Wang, Y. Wang, and G. Lang, "A cross-chain solution to integrating multiple blockchains for IoT data management," *Sensor*, vol. 19, no. 9, pp. 2042-2060, May 2019.

[158] S. Johnson, P. Robinson, and J. Brainard, "Sidechains and interoperability". Accessed: 23-Mar-2019. [Online]. Available: Available: https://arxiv.org/pdf/1903.04077.pdf

[159] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen, "Exploring the attack surface of blockchain: a systematic overview," *arXiv preprint arXiv*:1904.03487 2019.

[160] J. J. Hoch, A. Shamir, "On the strength of the concatenated hash combiner when all the hash functions are weak," in *Proc. ICALP'08*, Jan. 2008.

[161] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3416-3452, May 2018.

[162] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts SoK," in *Proc. ACM PST'17*, Apr. 2017.

Peng Zhuang (S'15) received the B.Sc. degree in electrical and computer engineering from University of Alberta, Edmonton, AB, Canada, in 2015. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada. His current research interests include stochastic modeling and optimization in smart grid, cyber-physical security of smart grid, microgrid planning, operation, control, and self-healing, distribution system operation with distributed generation and energy storage devices, computational intelligence and optimization, and big data analytics.

Talha Zamir received the B.Sc. degree from University of Management and Technology, Lahore, Pakistan in 2013 and Master of Engineering degree from University of Alberta Edmonton, AB, Canada, in 2019. During his Masters, he started working as a researcher in the field of smart grids and came up with new ideas related to integration of blockchain in grid communication space to achieve robust cyber security. He specializes in the field of power system protection, coordination, instrumentation, and renewable energy systems. He is currently working with Dynawest Engineering Ltd., Edmonton, AB, Canada as an Electrical EIT. His research interests include smart grid, cyber security, power system protection and power quality.

Hao Liang (S'09-M'14) is an Assistant Professor and Canada Research Chair in the Department of Electrical and Computer Engineering at the University of Alberta, Canada. He received his Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2013. From 2013 to 2014, he was a postdoctoral research fellow in the Broadband Communications Research (BBCR) Lab and Electricity Market Simulation and Optimization Lab (EMSOL) at the University of Waterloo.

Dr. Liang's current research interests are in the areas of smart grid, cyber-physical systems, wireless communications, and wireless networking. He is a co-recipient of the IEEE Power & Energy Society (PES) Prize Paper Award 2018, the Best Conference Papers on Electric Vehicles, Energy Storage, Microgrids, and Demand Response from the 2016 IEEE Power & Energy Society General Meeting (PES GM'16), Boston, MA, USA, and the Best Student Paper Award from the IEEE 72nd Vehicular Technology Conference (VTC Fall-2010), Ottawa, ON, Canada. He serves/served as an Editor for IET Communications, a Guest Editor for IEEE Transactions on Emerging Topics in Computing, and the Chair of Electric Vehicles, Vehicular Electronics, and Intelligent Transportation Track for IEEE VTC Fall-2020. He was the System Administrator of IEEE Transactions on Vehicular Technology (2009-2013).