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 cybersecurity. Although significant efforts have been devoted to utilizing blockchain in the smart grid for cybersecurity, there is a lack of comprehensive survey on blockchain in the smart grid for cybersecurity in both application and technological perspectives. To fill this gap, we conducted a comprehensive survey on blockchain for smart gird cybersecurity. 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 cybersecurity. This article aims at providing helpful guidance and reference for future research efforts specific to blockchain for cybersecurity in the smart grid.

摘要——区块链是一种不可变的分布式账本，能够在不依赖第三方的情况下存储数据。 区块链技术引起了研究领域的极大兴趣，包括其在智能电网中的网络安全应用。 尽管在智能电网中利用区块链实现网络安全已经付出了巨大的努力，但从应用和技术角度来看，智能电网中的区块链在网络安全方面缺乏全面的调查。 为了填补这一空白，我们对智能电网网络安全的区块链进行了全面调查。 这项进行的调查展示了与区块链在智能电网中的网络安全应用相关的想法、架构和实施技术的最新见解。 本文旨在为未来针对智能电网网络安全的区块链研究工作提供有益的指导和参考。

Index Terms—Blockchain, cybersecurity, resiliency, smart contract, smart grid.

索引词——区块链、网络安全、弹性、智能合约、智能电网。

1. INTRODUCTION

一、引言

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 twoway communication networks for data transfers [2]. However, the current communications over transmission control protocol (TCP)/internet protocol (IP) and ethernet-based technologies expose the smart grid to public data networks [3], which makes it vulnerable to severe cyberattacks [4].

电网正在经历大规模的智能电网革命，以更好地采用不同规模和技术的发电，鼓励客户参与积极的系统运行，提高系统的可靠性、稳定性、可持续性和安全性 [1]。 可靠高效的智能电网运行在很大程度上依赖于用于数据传输的双向通信网络 [2]。 然而，当前通过传输控制协议 (TCP)/互联网协议 (IP) 和基于以太网的技术进行的通信将智能电网暴露于公共数据网络 [3]，这使其容易受到严重的网络攻击 [4]。

In December 2015, the cyberattack 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 cyberattack has not led to any blackouts in the Utah electric grid, it has shown that the adversaries can launch severe cyberattacks against critical infrastructures in the smart grid.

2015 年 12 月，针对乌克兰 3 家配电公司的网络攻击使用鱼叉式网络钓鱼电子邮件成功夺取了监控和数据采集 (SCADA) 系统，并远程关闭了变电站，导致 23 万客户停电 [5] ]. 2019 年 3 月，针对犹他州电力公司的部分 SCADA 基础设施发起了拒绝服务 (DoS) 攻击，导致部分电网失去可观测性 [6]。 尽管这次网络攻击并未导致犹他州电网发生任何停电，但它表明对手可以对智能电网中的关键基础设施发动严重的网络攻击。

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 cybersecurity 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 cyberattacks 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 cybersecurity of the smart grid.

随着智能电网的发展，先进的监控技术正在客户侧部署。 如今，大多数家庭都配备了智能设备，例如智能机器人和智能安全系统。 由于可以通过中央控制器远程监控和控制这些设备，因此网络安全对客户来说变得很重要 [7]。 此外，随着尖端技术的发展，智能电网正在兴起，提供供水/供气、交通和其他服务，形成智慧城市 [8]、[9]。 由于智慧城市不同部门之间的高度交叉，智能电网对网络攻击的脆弱性可能会给社会带来严重的灾难，而不仅仅是电力系统。 因此，迫切需要对智能电网的网络安全进行调查。

In the 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 the 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).

在智能电网中，不同的信息和通信技术（ICT）已广泛应用于发电、输电、配电和用电部门，为智能电网优化控制收集和传输数据。 对于发电、输电和配电，使用 SCADA 系统的远程终端单元 (RTU)、广域测量系统 (WAMS) 的相量测量单元 (PMU)、智能电子设备 (IED) 的传感器收集数据， 和地理信息系统（GIS）。 对于电力利用，嵌入在高级计量基础设施 (AMI) 中的智能电表通常用于收集客户的电力使用数据。 收集的数据通过通信网络传输到SCADA系统，用于高级管理和控制，如自动发电控制（AGC）、电力系统状态估计（SE）、配电自动化控制（DAC）和需求侧管理（DSM） .

For the efficient and reliable communications among distributed and heterogeneous components within the 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 first 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 the 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 cyberattacks.

为了智能电网中分布式和异构组件之间高效可靠的通信，由家庭区域网络 (HAN)、邻域网络 (NAN)、传感器网络 (SN)、广域网络 (WAN) 和核心网络组成的分层通信网络 网络发达。 HAN 和 NAN 是通过 ZigBee/Z-wave 协议和 IEEE 802.11/802.15.4/802.16 标准 [10] 将局部区域内的 AMI 联网而建立的。 在 WAN 内，RTU、WAMS、IED 和 GIS 首先通过 SN 分组，然后基于分布式网络协议 3.0 (DNP3)、Modicon 通信总线 (ModBus) 和/或认知无线电与 SCADA 系统和数据中心通信 IEEE 802.22 标准 [11]。 然后，数据被传输到核心网络并由不同的控制机构使用。 在核心网中，常见的通信方式有TCP/IP网络、WiMAX、GPRS等。 为了便于在智能电网中实施，这些协议被设计为在没有加密和身份验证限制的情况下传输原始数据，并且没有过多的数据可用性开销 [12]。 因此，智能电网很容易被网络攻击所利用。

The vulnerabilities of different communication protocols in the smart grid are investigated in [13], and the most concerning cybersecurity issues can be summarized in four aspects:

1) integrity;

2) confidentiality;

3) availability; and

4) accountability/nonrepudiation.

The integrity attack is based on unauthorized and stealthy modification, alteration, or destruction of field measurement data in the 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].

文献[13]对智能电网中不同通信协议的漏洞进行了调查，最受关注的网络安全问题可以概括为四个方面：

1）完整性；

2）保密；

3) 可用性； 和

4) 问责制/不可否认性。

完整性攻击基于对智能电网中现场测量数据的未经授权和秘密修改、更改或破坏。 虚假数据注入（FDI）攻击是典型的针对 SE 的完整性攻击。 FDI 攻击可以悄悄地破坏现场测量数据，这将改变 SE 结果并误导控制中心的决策。 这可能导致级联电网故障 [14]。

The confidentiality attack targets on accessing or disclosing privacy and proprietary information by unauthorized entities or individuals. In the 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 the smart grid, both authentications of information and authorization of accessing are required to maintain the integrity and confidentiality.

机密性攻击针对未经授权的实体或个人访问或泄露隐私和专有信息。 在智能电网中，AMI 是机密泄露的主要来源。 攻击者可以通过恢复root密码或利用系统漏洞[15]获得AMI的访问权限，获取客户的用电信息，侵犯客户隐私。 在智能电网中，需要对信息进行身份验证和访问授权，以保持其完整性和机密性。

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

确保及时可靠地访问信息的可用性对于智能电网的高效稳定运行至关重要。 通过中断数据传输，针对可用性的网络攻击可以延迟、阻止甚至破坏控制信号，并对智能电网运行的稳定性、效率和安全性造成严重影响 [16]。

For the accountability/nonrepudiation in the 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 the smart grid. The local power trading involves valuable resources and information, which makes the cyberattacks against accountability/nonrepudiation now a major issue [13]. To maintain the accountability/nonrepudiation, 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].

对于智能电网中的责任/不可否认性，系统或客户所做的操作不能在以后被拒绝。 随着分布式发电机 (DG) 的集成，本地电力交易成为智能电网中的一个重要概念。 本地电力交易涉及宝贵的资源和信息，这使得针对问责制/不可否认性的网络攻击现在成为一个主要问题[13]。 为了保持问责制/不可否认性，要求智能电网通信网络具有高可审计性，以便可以以信任的方式从历史记录中重建完整的信息历史记录 [16]。

For enterprise communication networks, different cybersecurity 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 the smart grid [16]. The smart grid is featured by distributed generation and control; however, the communication networks in the 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 abovementioned cybersecurity issues in the smart grid, blockchain technology has been seen as a promising solution [18]–[20].

对于企业通信网络，不同的网络安全技术，例如具有用于网络安全的入侵检测系统（IDS）的防火墙，用于数据安全的加密和身份验证，以及用于设备安全的主机 IDS [10]。 然而，由于智能电网通信网络的实时性要求和连续运行的特点，这些技术很难适应智能电网[16]。 智能电网具有分布式发电和分布式控制的特点； 然而，智能电网中的通信网络仍然以集中方式运行，这使得智能电网极易受到单点故障的影响[17]。 为了解决智能电网中的上述网络安全问题，区块链技术被视为一种有前途的解决方案 [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 the 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 the blockchain-based smart grid are nearly immutable, which can protect the data integrity, confidentiality, and availability of the 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 the blockchain-based smart grid and makes the accountability/nonrepudiation attacks nearly impossible. The asymmetric cryptography in the 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]. Furthermore, by leveraging the smart contract and decentralized applications (DAPPS) services, the blockchain can provide cybersecured computation environment for advanced smart grid applications.

区块链是分布式账本技术 (DLT) 的一种变体，它在系统内的多个设备之间分布式存储和传输数据。 通过利用区块链技术，现场测量数据和本地交易数据可以在智能电网中以点对点（P2P）方式传输[21]。 这些数据被复制并分布式存储在多个设备上，而不是单个数据中心。 P2P 数据传输和数据存储在多个设备上的分布式复制防止智能电网遭受单点故障并保证高可用性[22]。 同时，由于区块链分布式的数据验证、验证和存储特性，基于区块链的智能电网中的数据几乎是不可篡改的，可以保护智能电网数据的完整性、机密性和可用性。 一旦数据被添加到区块链，它就永远不会被攻击操纵，除非对手拥有整个系统中超过 51% 的设备。 此属性在基于区块链的智能电网中保持高可审计性，并使责任/不可否认攻击几乎不可能。 区块链中的非对称密码学可以提高基于区块链的 AMI [23] 的身份验证和授权级别，从而可以保护客户的隐私和电力数据的完整性 [24]。 此外，通过利用智能合约和去中心化应用程序 (DAPPS) 服务，区块链可以为高级智能电网应用程序提供网络安全计算环境。

In the literature, there are several papers that have conducted surveys on the application of the blockchain in the smart grid covering various topics. A systematic review of the blockchain in the energy sector is conducted in [25], in which an overview of a variety of energy applications of the blockchain is presented with detailed discussion on benefits and limitations of blockchain technologies in the 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 the blockchain-based smart grid, the authors in [26] review a variety of prospects and approaches for blockchain applications in the smart grid. The advantages and technical challenges of implementing the blockchain in the smart grid are discussed, and the frameworks for the key blockchain-based smart grid applications are presented. In [27], a comprehensive survey is presented for the blockchain-based P2P energy transaction in the smart grid with main focuses on the P2P energy trading architecture, demand response (DR) optimization models, and power routing mechanisms. Furthermore, the authors in [28] present 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, DR 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 cybersecurity. A comprehensive survey that emphasizes both application and technical perspectives of the blockchain in the smart grid for cybersecurity has not been conducted so far. To fill this gap in research, this article presents a comprehensive survey to provide helpful guidance and reference for the research in improving cybersecurity of the smart grid by using blockchain technology.

在文献中，有几篇论文对区块链在智能电网中的应用进行了涵盖各种主题的调查。 [25] 对能源领域的区块链进行了系统回顾，其中概述了区块链的各种能源应用，并详细讨论了区块链技术在能源领域的优势和局限性。 此外，还对大约 140 个最近的能源区块链商业和研究计划进行了审查和分类。 随着对基于区块链的智能电网的更多关注，[26] 中的作者回顾了智能电网中区块链应用的各种前景和方法。 讨论了在智能电网中实施区块链的优势和技术挑战，并提出了基于区块链的关键智能电网应用框架。 在 [27] 中，对智能电网中基于区块链的 P2P 能源交易进行了全面调查，主要关注 P2P 能源交易架构、需求响应 (DR) 优化模型和电力路由机制。 此外，[28] 中的作者从本地能源市场设计的角度对基于区块链的 P2P 能源交易进行了全面调查，其中当前对本地能源市场机制、客户偏好、DR 策略和 审查和评估储能的影响。 尽管现有的调查论文都提到了区块链在提高智能电网网络安全方面的优势。 迄今为止，尚未进行过强调区块链在网络安全智能电网中的应用和技术视角的综合调查。 为了填补这一研究空白，本文进行了全面调查，为利用区块链技术提高智能电网网络安全的研究提供有益的指导和参考。

The remainder of this article is organized as follows. In Section II, an overview of blockchain technology is presented. In Section III, the architecture and development platforms of the blockchain-based smart grid for cybersecurity are introduced. In Section IV, the integration of blockchain technology for the cybersecured smart grid will be discussed in both application and technical perspectives. Finally, Section V concludes this article.

本文的其余部分组织如下。 在第二节中，概述了区块链技术。 在第三节中，介绍了基于区块链的网络安全智能电网的架构和开发平台。 在第四节中，将从应用和技术角度讨论区块链技术在网络安全智能电网中的整合。 最后，第五节总结了本文。

1. OVERVIEW OF BLOCKCHAIN TECHNOLOGY FOR CYBERSECURITY OF SMART GRID

二。 智能电网网络安全区块链技术概述

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]. The blockchain is divided into blockchain 1.0 for simple cryptographic currency, 2.0 with smart contract functionality, and 3.0 for distributed application [31].

DLT 被定义为一个数据库，它可以跨地理分布的多个设备自愿复制、共享和同步数据 [29]。 在 DLT 中，数据按时间顺序存储，形成数字账本链。 一旦将包含一组数据的块添加到链中，它就永远不能被任何未经授权的实体或个人修改，因此它本质上是防篡改的[30]。 如图 1 所示，根据数据的验证和存储方式，DLT 主要可分为区块链、有向图数据（DAG）和临时账本（Tempo）三种类型。 在这三种类型的分布式账本技术中，区块链是研究最充分的一种，在实际应用中的渗透度很高[29]。 区块链分为简单加密货币的区块链1.0、具有智能合约功能的2.0和分布式应用的3.0[31]。

The blockchain is a distributed database based on the P2P network, with security enabled using multiple cryptographic technologies. Different types of the 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. However, the access for consortium and private blockchain networks is permissioned, there still requires an authority to approve the permission for the node. Due to a large number of nodes in the public blockchain, it is nearly impossible to tamper the public blockchain [32]. Theoretically, the consortium and private blockchains require less effort for tampering, in practical, they still have good performance in cybersecurity, 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 the smart grid should consider the classes of nodes, the requirement for anonymity, computational complexity (efficiency), and restriction on access [34].

区块链是基于 P2P 网络的分布式数据库，使用多种密码技术实现安全性。 基于共识机制和网络开放性，人们提出了不同类型的区块链以满足实际应用的不同需求。 如图 1 所示，研究最多的区块链变体是公共、联盟和私有区块链。 表 I 总结了这三种类型的区块链的比较。公共和联盟/私有区块链之间的主要区别在于节点的类别，即负责数据验证、验证、传输和存储的设备。 对于公共区块链，节点是去信任和匿名的，这导致功耗大和交易批准时间长。 联盟链和私有链中的节点是可信的，基于可信节点的共识机制功耗低，交易通过率快。 但是，联盟链和私有区块链网络的访问是需要许可的，仍然需要一个权限来批准节点的权限。 由于公共区块链中的大量节点，几乎不可能篡改公共区块链[32]。 从理论上讲，联盟链和私有链需要更少的篡改努力，实际上，它们在网络安全方面仍然具有良好的性能，因为联盟链和私有链中的节点是经过授权的并且可以得到很好的保护[33]。 因此，为智能电网中的不同应用选择不同类型的区块链应考虑节点的类别、匿名性要求、计算复杂性（效率）和访问限制 [34]。

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

1) reduction on the cost of power transactions;

2) facilitating the adoption of DGs in the smart grid;

3) improved automation control and system monitoring;

4) development of advanced control applications for the smart grid on the blockchain DAPPS layer; and

5) improved cybersecurity of the smart grid.

基于区块链的特点，智能电网的一些潜在好处总结如下[10]-[12]：

1）降低电力交易成本；

2) 促进 DG 在智能电网中的采用；

3）改进了自动化控制和系统监控；

4）在区块链DAPPS层开发智能电网高级控制应用； 和

5) 改进智能电网的网络安全。

In this article, the main focus is on the cybersecurity feature of the blockchain for the smart grid. For the rest of this section, the blockchain technology will be discussed mainly related to the smart grid cybersecurity. Although the private, consortium, and public blockchains differ in many aspects, they share some essential components in the architecture: Merkel tree, timestamp, hash function, encryption and decryption, consensus mechanism, and nonce [35]. The 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 the blockchain, the hash function is used in the Merkel tree, timestamp, and encryption [36].

在本文中，主要关注智能电网区块链的网络安全特性。 在本节的其余部分，将主要讨论与智能电网网络安全相关的区块链技术。 尽管私有链、联盟链和公有链在许多方面有所不同，但它们在架构中共享一些基本组件：默克尔树、时间戳、哈希函数、加密和解密、共识机制和随机数 [35]。 默克尔树是一种数据结构，用于高效地汇总和验证区块中的大型数据集。 每个区块都有一个 Unix 时间戳，这为区块哈希创建了一个变异源，使对手更难篡改区块链。 散列函数用于将可变长度输入转换为固定长度编码输出。 散列函数应具有易拼图和无碰撞等特性，以实现高级别的安全性。 安全哈希算法 (SHA) 广泛用于加密哈希函数，例如比特币中的 SHA-256。 在区块链中，哈希函数用于默克尔树、时间戳和加密[36]。

The encryption and decryption method in the blockchain is based on asymmetric cryptography, as shown in Fig. 2. Different from symmetric cryptography, every node in the 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 the 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 the blockchain using the receiver’s public key, which protects the data integrity and accountability/nonrepudiation. 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 the smart grid, and the privacy of nodes can be protected since only public keys can be observed [39].

区块链中的加密和解密方法基于非对称密码学，如图2所示。与对称密码学不同的是，区块链中的每个节点都有一个公钥和一个私钥。 公钥类似于账户公钥，私钥类似于保密的密码[37]，[38]。 在区块链中，发送方使用接收方的公钥对数据进行加密，加密后的数据可以被区块链中的所有节点使用接收方的公钥查看、验证和验证，从而保护了数据的完整性和可问责性/ 不可否认性。 然后，接收方可以使用相应的私钥对加密数据进行解密。 在此过程中，公钥和私钥对为智能电网提供额外的身份验证和授权，并且节点的隐私可以得到保护，因为只能观察到公钥 [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 the 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/nonrepudiation in the smart grid.

共识机制用于允许数据传输具有可信度和保证它没有被篡改。 这在没有第三方参与的情况下建立了节点之间的信任。 区块链的主要思想是为所有已发布的区块打上时间戳，然后通过 SHA256 哈希算法运行它以保持数据完整性。 每个块还使用哈希值引用前一个块的值。 通过这种方式，每个人都可以看到哪些块是互连的，哪些数据在过去以什么顺序传输[40]，这可以为智能电网中的问责制/不可否认性提供更好的保护。

A simple application of the blockchain in the smart grid is providing cybersecured trading platform for P2P power transaction based on the distributed ledger of Bitcoin [41]. Furthermore, with a completely new programming language named by Solidity, Ethereum has brought computational capabilities into cybersecured environment based on the 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 the smart grid operation into the cybersecured system built by the 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].

区块链在智能电网中的一个简单应用是为基于比特币分布式账本的 P2P 电力交易提供网络安全交易平台 [41]。 此外，以太坊通过一种名为 Solidity 的全新编程语言，将计算能力带入了基于区块链的网络安全环境 [42]。 此外，随着智能合约功能的出现，许多基于区块链的应用程序已经被研究用于 DAPPS 服务 [43]。 这些 DAPPS 服务允许将智能电网运行的更多高级应用程序变体集成到由区块链构建的网络安全系统中 [44]。 然而，这些应用中的大多数仍然仅限于电子货币，例如以太坊平台上的初始硬币产品（ICO），它提供筹款服务 [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 the blockchain. Compared with conventional linear single chain architecture, the IOTA introduces a meshed network architecture. Improvement in the 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 min to 10 s; however, this comes with the scarification of security. The cascaded structure of the blockchain with the 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 the 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 the smart grid, as it proves to be reliable and protective against 51% attack with reduced forking.

阻碍基于区块链的 DAPPS 广泛应用的主要问题之一是可扩展性。 许多研究人员为解决这个问题付出了巨大的努力。 在 [46] 中，研究了一种名为 IOTA 的技术，它结合了区块链技术和物联网 (IoT) 架构，以提高区块链的可扩展性。 与传统的线性单链架构相比，IOTA引入了网状网络架构。 [47] 中还通过使用诸如隔离见证、块大小增量、分片和权益证明算法等技术实现了可扩展性的改进。 在这些技术中，减少块数据大小的分片已被测试为提高可扩展性的最有效技术。 此外，已经进行了一些关于通过交替区块链结构来改变块大小的讨论。 在 [48] 中，提出了一种新的区块链协议 Bitcoin-NG。 Bitcoin-NG中引入微块的概念，加速出块过程，将出块时间从10分钟缩短到10秒； 然而，这伴随着安全性的削弱。 [49]中引入了块大小减小的区块链级联结构，提高了区块链的整体性能。 同样，在[50]中提出了一个可扩展的区块链框架，以提高区块链在大规模物联网系统中的可扩展性。 其中，物联网设备需要作为节点直接连接到全球区块链。 相反，多个物联网设备通过完全信任的证书颁发机构组成一个组，并且形成的物联网设备组由参与全球区块链的单个对等体表示。 这种架构对智能电网可能是有益的，因为它被证明是可靠的，并且可以通过减少分叉来防止 51% 的攻击。

For the successful integration of the blockchain in the 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 the 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 the blockchain and supporting applications may lead to the collapse of the 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].

为了将区块链成功集成到智能电网中，应谨慎处理区块链与智能电网应用程序之间的交互，以保持区块链的稳定性。 在[51]-[53]中，研究了由区块链和应用程序之间的交互引起的稳定性问题。 在考虑区块链和应用程序之间的交互时，区块链内的激励不匹配是潜在不稳定的主要问题，因为节点在经济上有动机在区块链中安全地确认交易，并且它们没有直接的激励来支持应用程序。 区块链中交易的安全确认与支持应用程序之间的激励不匹配可能导致区块链崩溃。 为了避免区块链中的激励不匹配，设计具有高可移植性的区块链为区块链及其应用程序提供共同激励是至关重要的[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 the blockchain on top of smart contracts [54]. Some DAPPS 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 the smart grid by using blockchain-based big data analysis, which can ensure the integrity, availability, and accountability/nonrepudiation 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 cybersecured 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.

对于有应用的区块链，主要有四层，即应用层、执行引擎、数据存储和共识机制。 大多数研究工作都集中在应用层，尤其是 DAPPS，因为它可以在智能合约之上为区块链带来更多功能 [54]。 一些 DAPPS 使用过去的数据为不同的节点建立信任，Airbnb 就是此类应用的一个很好的例子。 通过使用基于区块链的大数据分析，可以将相同的方法用于智能电网中的需求预测，这可以确保历史数据的完整性、可用性和责任性/不可否认性 [55]。 此外，在[36]中，提出了具有各种应用的新兴区块链标准。 该标准将区块链的使用分为四层，即提供基础硬件和网络支持的基础设施层，允许用户在不同操作系统（如 Windows 和 BerkeleyDB）上运行网络安全区块链环境的平台服务层。 节点管理、编程和运行时管理属于第三层，这一层使用 SDK 接口，如 JSON RPC、Solidity 和 Node.js。 最后一层是用户级应用层，俗称DAPPS。

The implementation of well-designed blockchain in the smart grid allows improving the overall smart grid system’s cybersecurity. It introduces cybersecured environment for variants of advanced applications in the smart grid, such as electric grid monitoring, electricity data transfers, automation power control, and local power trading [30]. In the following section, an overview of system architecture and development platforms for cybersecurity of the smart grid using blockchain technology will be presented in detail.

在智能电网中实施精心设计的区块链可以提高整个智能电网系统的网络安全。 它为智能电网中高级应用程序的变体引入了网络安全环境，例如电网监控、电力数据传输、自动化电力控制和本地电力交易 [30]。 在下一节中，将详细介绍基于区块链技术的智能电网网络安全系统架构和开发平台。

1. SYSTEM ARCHITECTURE AND DEVELOPMENT PLATFORM OF BLOCKCHAIN IN SMART GRID FOR CYBERSECURITY

三、 网络安全智能电网中区块链的系统架构与开发平台

The blockchains are implemented in the smart grid cyberlayer to improve cybersecurity by protecting data integrity, confidentiality, availability, and accountability/nonrepudiation. The implementation of blockchain in the smart grid for cybersecurity 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 cybersecurity will be discussed. Also, the development platforms for the blockchain-based smart grid will be presented.

区块链在智能电网网络层中实施，以通过保护数据完整性、机密性、可用性和问责制/不可否认性来提高网络安全。 区块链在网络安全智能电网中的实施主要分为四个部分，即现场测量和控制、数据聚合、数据管理和系统运行[56]-[59]。 在本节中，将讨论基于区块链的网络安全智能电网的系统架构。 此外，还将介绍基于区块链的智能电网的开发平台。

1. System Architecture for Smart Grid Cybersecurity

A. 智能电网网络安全系统架构

By incorporating the blockchain in the cyberayer of the smart grid, blockchain technologies can be leveraged to support the operation and development of the smart grid. Considering the layered communication networks in the smart grid with two-way communication links, the system architecture of the blockchain in the smart grid for cybersecurity 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 the wholesale electricity market and real-time monitoring in the energy management system. The 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.

通过将区块链纳入智能电网的网络层，可以利用区块链技术支持智能电网的运行和发展。 考虑到智能电网中具有双向通信链路的分层通信网络，智能电网中用于网络安全的区块链系统架构如图 3 所示，该架构基于 [60] 中的通信系统模型。 这种结构分为四个网络，即核心网、WAN、NAN和SN/HAN。 该架构在不同的智能电网应用程序的不同通信网络中嵌入了区块链。 核心网络与 SCADA 系统之上的控制机构相关，例如电力公司、系统运营商、电表运营商和维护公司 [61]。 核心网络中的用户可以完全访问监控、修改和向 SN 和 HAN 传递指令（例如智能合约）。 不同的区块链可以在核心网络中用于不同的应用，例如批发电力市场中的能源招标和能源管理系统中的实时监控。 WAN层是连接NAN和核心网的中间层。 本系统中的广域网可以作为虚拟机部署在云端，不同的区块链可以实现广域网应用，如现场测量聚合和存储。 在 NAN 和 HAN 中，本地生产者和消费者直接相连，区块链可用于提供各种应用，例如电动汽车充电和本地能源交易。

Also, as discussed in the recent research works [60], [62], based on the two-way communication links in the smart grid, the trustless local producers and consumers connecting to HAN can be selected as nodes to provide mining power for public blockchains in the 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 the smart grid, the trusted nodes that are typically selected from smart grid controlling authorities and distributed generation owners with large capacities will participate in the consensus process.

此外，正如最近的研究工作 [60]、[62] 所讨论的，基于智能电网中的双向通信链路，可以选择连接到 HAN 的无需信任的本地生产者和消费者作为节点，为公众提供挖矿能力 智能电网中的区块链。 最初，挖矿能力可以由标准的家用电脑提供； 然而，随着专用集成电路 (ASIC) 矿机的推出，家用电脑不再能够挖矿 [25]。 为了解决这个问题，已经提出并检查了不同的挖掘算法。 例如，Ethereum [63] 的 Ethash 算法和 Zcash [64] 的 Equihash 算法是抗 ASIC 的 PoW 算法，允许通过 CPU 和 GPU 进行基于家庭计算机的挖掘。 此外，还提出了一些智能电网特定的挖掘策略。 例如，基于 [65] 中的 CyClean 和 SolarCoin [66]，硬币被提前开采并根据可再生能源的产生和消耗奖励给当地生产者和消费者，并且采矿权力基于 持股奖励。 对于智能电网中的联盟链和私有链，通常从智能电网控制机构和大容量分布式发电所有者中选出的可信节点将参与共识过程。

The data flow through these networks is published on corresponding blockchains, and that published data (verified by the nodes) are 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.

通过这些网络的数据流发布在相应的区块链上，发布的数据（由节点验证）在网络之间使用和通信，具有更高的安全性、透明度、自动化和隐私保护功能 [67]。 然而，现有的研究主要集中在为每个通信网络中的特定应用开发独立的区块链。 仍然需要大量的研究工作来调查不同区块链的互操作性，特别是对于通过不同区块链的数据流的同步。

In the 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]. Furthermore, with the DAPPS services, the blockchain-enabled AMIs can perform decentralized DR, local power management, and local power trading within cybersecured environment [70].

在智能电网中，智能发电、智能输配电和智能家居/楼宇由现场支持物联网的 ICT 设备监控和直接控制，例如用于系统运行的 RTU、IED 和 WAMS，以及用于智能家居/的 AMI/ 建筑管理 [68]。 通过将现场测量和控制区块链与智能合约结合到 WAN、NAN 和 SN/HAN 中这些支持物联网的 ICT 设备，可以安全、自动地收集现场测量数据 [69]。 此外，借助 DAPPS 服务，支持区块链的 AMI 可以在网络安全环境中执行分散式 DR、本地电源管理和本地电源交易 [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 the 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 cybersecurities caused by human mistakes [73]. Also, the storage of historical records of decisions in the blockchain can provide better audibility in the smart grid.

现场测量数据将由选定的数据聚合器聚合，同时利用 WAN 和 NAN 中的数据聚合区块链。 使用区块链进行数据聚合的目的主要是为了在智能电网中提供额外的数据机密性保护[71]。 在被仪表运营商或 SCADA 系统和数据中心的多个接收者接收后，聚合数据将通过智能合约和 DAPPS 服务 [72] 由数据管理区块链自动处理和存储，区块链可以保护存储的完整性和可审计性 数据。 对于 WAN 内的系统操作区块链，通过利用智能合约和 DAPPS 服务，可以自动做出系统操作决策，减少人机界面，从而降低人为错误造成的网络安全风险 [73]。 此外，在区块链中存储决策的历史记录可以在智能电网中提供更好的可听性。

The data flow within and among these four networks is verified and stored by the blockchains with a high degree of cybersecurity, 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 the 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 cybersecurity and efficiency of the wholesale electricity market [25]. Some start-up companies, such as Power Ledger, Grid+, and Greeneum, have started to use the 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/nonrepudiation of transaction data can be well protected. In some works, the applications of the blockchain for data management in EV charging stations are also investigated, which mainly aim at providing confidentiality protection and data availability.

这四个网络内部和之间的数据流由具有高度网络安全性的区块链验证和存储，跨多个设备的数据存储复制可以有效地保护数据可用性免受单点故障[74]。随着 随着区块链技术的进步，可以使用在 DAPPS 层上构建的专门设计的区块链来集成电力交易功能。 对于系统操作，区块链能够提高批发电力市场的网络安全和效率 [25]。 一些初创公司，如 Power Ledger、Grid+ 和 Greeneum，已经开始使用区块链进行本地电力交易 [59]。 在这种方法中，可以在低机密泄露风险的情况下参与电力交易的认证和授权，并且可以很好地保护交易数据的完整性、可用性和可说明性/不可否认性。 在一些工作中，还研究了区块链在电动汽车充电站数据管理中的应用，主要旨在提供机密性保护和数据可用性。

1. Development Platforms for Smart Grid Cybersecurity

B. 智能电网网络安全开发平台

Special applications and programs specific to the smart grid can be developed on IBM and Microsoft Azure development environments, which ensure cybersecurity of the 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 the Microsoft Visual basic platform or online using Solidity remix. The 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.

可以在 IBM 和 Microsoft Azure 开发环境上开发针对智能电网的特殊应用和程序，从而确保区块链的网络安全。 此外，以太坊平台还可用于部署公开可用且可验证的智能合约。 以太坊开发可以在 Microsoft Visual basic 平台上完成，也可以使用 Solidity remix 在线完成。 以太坊平台是开源的，易于实施，并且具有更多的安全特性； 然而，由于气体限制和气体成本，以太坊在大规模智能电网应用中的使用效率低下 [75]。 与以太坊一样，其他平台也支持智能合约功能，例如 Quorum、万链、Aternity、Zen、Counter party、Root Stock、Rchain 和 Qtum。 所有这些区块链都是经过一些修改的以太坊的不同变体。 例如，Quorum 的一大优势是其交易不使用 gas [76]，这更适合大规模智能电网应用。 Quorum 平台具有可以嵌入 Solidity 的功能 [22]。 Quorum 能够使用星座在选定的各方之间执行私人交易。

Some North American start-up companies have developed their blockchain platforms, which are specifically for the smart grid. BTL is a Canadian company that is working on crossborder, large-scale, and cybersecured power trading platform backed by the Interbit private blockchain. Similarly, Drift is an American company working on efficient and secure grid transactions with multiauthentication 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, XiWatt, 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. The Omega grid has developed a smart grid management platform for cybersecured system operation, which is based on a 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 s, which makes it useful for large-scale smart grid implementation [81].

一些北美初创公司开发了他们的区块链平台，专门针对智能电网。 BTL 是一家加拿大公司，致力于开发由 Interbit 私有区块链支持的跨境、大规模和网络安全的电力交易平台。 同样，Drift 是一家美国公司，致力于通过其区块链上的多重身份验证和隐私保护来实现高效、安全的网格交易。 一家德国公司正在使用 IBM-Hyperledger 结构区块链进行具有完整性和机密性保护的 P2P 电力交易。 Engro、XiWatt 和 Consensys 等公司正在使用公共区块链进行 P2P 电力交易。 一家名为 Pylon Networks 的西班牙公司为 AMI 使用莱特币公共类型区块链，旨在为电力追踪提供高可审计性。 Omega 电网开发了一个用于网络安全系统运行的智能电网管理平台，该平台基于私有运行的区块链 [77]-[80]。 一家名为 Tenup 的初创区块链公司提出了一种针对偏远地区的高能效架构，并致力于混合共识机制，其中最大交易时间为 60 秒，这有助于大规模智能电网的实施 [81] ].

1. APPLICATIONS OF BLOCKCHAIN IN SMART GRID FOR CYBERSECURITY

四、 区块链在网络安全智能电网中的应用

In the literature, the research on the blockchain for the smart grid cybersecurity 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 the blockchain for the smart grid cybersecurity against data integrity attack will be discussed in detail to better illustrate the cybersecurity mechanism of the blockchain-based smart grid.

在文献中，针对智能电网网络安全的区块链研究主要分为现场测量与通信、发电与输电、配电与用电三个层面。 在本节中，将介绍不同级别的区块链应用程序的详细信息。 将详细讨论区块链在智能电网网络安全中对抗数据完整性攻击的应用，以更好地说明基于区块链的智能电网网络安全机制。

1. Blockchain for Field Measurement and Communications

A. 用于现场测量和通信的区块链

Blockchain technology can have wide applications in the smart grid for field measurement and communications, where a 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 the smart grid for field measurement data uploading, fetching, and transferring. For the stability and reliability of the blockchain-based smart grid for cybersecured field data measurement and transfer, all these ICT devices connected to this system should be perfectly synchronized with the deployed blockchain. In [44] and [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 the blockchain network and to store the copies of blockchain and smart contracts locally [83]. Specific commands can be sent to the blockchain using these ICT devices to initiate or call the smart contracts. For the case of AMIs in the smart grid, they can be wirelessly connected to the blockchain and, thus, create a way to operate such devices on the smart grid through the blockchain [23], [84]. The power trading and security enhancement (ETSE) module, designated in [23], can be implemented to allow for the cybersecured P2P communications among different AMIs within the same blockchain network. If the smart contracts are deployed on a particular part of the smart grid, automated commands can be provided by the blockchain to the smart grid.

区块链技术可以在智能电网中广泛应用，用于现场测量和通信，这些研究工作的总结如表二所示。 支持物联网的 ICT 设备连接到区块链网络中的节点，以在智能电网中建立 P2P 通信，用于现场测量数据的上传、获取和传输。 为了基于区块链的智能电网用于网络安全现场数据测量和传输的稳定性和可靠性，连接到该系统的所有这些 ICT 设备都应与部署的区块链完美同步。 在 [44] 和 [82] 中，已经解释和讨论了不同类型的体系结构和同步协议。 选定的支持物联网的 ICT 设备用于创建与区块链网络的连接，并在本地存储区块链和智能合约的副本 [83]。 使用这些 ICT 设备可以将特定命令发送到区块链以启动或调用智能合约。 对于智能电网中的 AMI，它们可以无线连接到区块链，从而创建一种通过区块链 [23]、[84] 在智能电网上操作此类设备的方法。 可以实施 [23] 中指定的电力交易和安全增强 (ETSE) 模块，以允许同一区块链网络内不同 AMI 之间的网络安全 P2P 通信。 如果智能合约部署在智能电网的特定部分，则可以通过区块链向智能电网提供自动化命令。

Among different cyberattacks, the data integrity attack is a major threat in the smart grid [85]–[87]. FDI attack is a type of cyberattack 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 cyberattacks [91].

在不同的网络攻击中，数据完整性攻击是智能电网中的主要威胁[85]-[87]。 FDI 攻击是一种针对数据完整性的网络攻击，它会偷偷地操纵测量结果 [88]-[91]。 可能的攻击包括出于欺诈目的篡改消费数据，恶意改变电力交易交易以破坏电网稳定，通过收集和分析消费者数据侵犯客户隐私，以及远程控制关键 IED 将其关闭 [90]。 许多论文都介绍了基于防火墙的方法来防御此类攻击。 然而，由于支持物联网的 ICT 设备（例如 AMI）的计算能力较低，防火墙技术运行缓慢且容易受到网络攻击 [91]。

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 [42], [22], [92] and [112] for using the blockchain to provide guaranteed immutability of stored data, and mitigation of cyberattacks 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 first encrypted by the private key of smart meter, i.e., private key A. Then, the smart contract in the 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 have not been compromised since the private key of the smart meter cannot be obtained by adversaries, which protects the data integrity. Furthermore, 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.

区块链已被证明是保护智能电网免受 FDI 攻击的更好、更有效的替代方案 [92]。 [42]、[22]、[92] 和 [112] 中介绍了一些解决方案，使用区块链来保证存储数据的不变性，并减轻针对数据收集和传输的网络攻击。 在 [22] 中，提出了基于区块链的智能电表来保护客户用电数据的完整性和机密性。 如图 4 所示，智能电表和公用事业公司都有自己的公钥和私钥对。 智能电表计量的用电量数据首先通过智能电表的私钥即私钥A进行加密，然后区块链中的智能合约会使用智能电表的公钥即public对加密后的数据进行解密 密钥A，并检查有效性。 对于有效性检查，如果公钥 A 可以成功解密加密数据，则加密数据未被泄露，因为对手无法获得智能电表的私钥，从而保护了数据的完整性。 此外，数据将使用公用事业公司的公钥即公钥B进行加密，只有拥有相应私钥即私钥B的公用事业公司才能访问数据。 这可以保护客户数据的机密性。

Also, blockchain provides tamper-proof and traceable features for data flows, which are required in the smart grid for data integrity and accountability/nonrepudiation protections. In [55], [93], and [94], the 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 [95] for secured and trustful big data analysis; however, the synchronization of the 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, the 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.

此外，区块链为数据流提供防篡改和可追溯功能，这是智能电网中数据完整性和责任/不可否认保护所必需的。 在 [55]、[93] 和 [94] 中，区块链启用了安全数据流和存储的大数据分析。 如果提供的旧数据有错误且不可信，则所有未来的估计和预测都将不准确。 例如，对特定时期的风速或太阳能强度的错误估计会造成重大经济损失，甚至会破坏智能电网的稳定。 [95] 中引入了一种具有不良数据检测机制的去中心化区块链架构，用于安全可靠的大数据分析； 但是，尚未考虑区块链的同步以及数据获取和上传延迟。 这些因素都会影响仿真时序，降低大数据分析的效率。 为了解决这个问题，[96] 中使用了 Hyperledger fabric 区块链来与众包电力市场合作，由于使用了 PBFT 共识，因此速度更快，并且更安全。

In [72], [97], and [98], surveys are conducted for blockchain usage for cybersecurity of the 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] and [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 the 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 cybersecured applications in the smart grid.

在 [72]、[97] 和 [98] 中，针对物联网系统网络安全的区块链使用情况进行了调查，并介绍了基于区块链的商业模式市场以及区块链-物联网组合。 [57] 和 [99] 中解释了不同区块链架构之间的比较及其与物联网设备的连接。 在 [57] 中进一步阐述了将智能合约与物联网设备一起使用的方法，并介绍了一些新的稳健技术。 可再生能源发电预测的大数据分析可以在本地进行，计算资源占用少，数据可以以不可篡改的方式发布在区块链上，智能合约将根据发布的预测数据自动执行。 [94]中开发的特殊区块链专门用于大数据分析，具有高可扩展性和安全性； 这种机制也可用于为智能电网中更多网络安全应用程序开发区块链。

In [100], a new cloud-based architecture for the blockchainbased 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 lowcost, secured, and on-demand access to the users [101]. The 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. HStore can achieve the best throughput, while the throughput rate of Hyperledger fabric ranks second. Also, the P2P file system for data transfer based on the blockchain is discussed in [103]. The InterPlanetary File System (IPFS) can be used in combination with the blockchain to achieve improved throughput, especially for big data analysis.

在 [100] 中，提出了一种用于基于区块链的物联网系统的新的基于云的架构，以提高实时数据存储和低延迟传输的性能。 具有控制器雾节点的分布式基于云的架构已被证明是一个很好的选择，因为它们为用户提供低成本、安全和按需访问 [101]。 雾节点基于软件定义网络 (SDN) 和区块链 [100]。 在此架构中可以显着减少物联网设备之间的端到端延迟。 在 [102] 中，对一些典型区块链的速度进行了比较，例如 Hyperledger fabric（即 PBFT 共识算法）、Parity、Ethereum 和 H-Store 区块链。 HStore可以达到最好的吞吐量，而Hyperledger fabric的吞吐率排名第二。 此外，在[103]中讨论了基于区块链的用于数据传输的 P2P 文件系统。 星际文件系统（IPFS）可以与区块链结合使用以提高吞吐量，特别是对于大数据分析。

1. Blockchain for Power Generation and Transmission

B. 用于发电和输电的区块链

In this section, the applications of the blockchain for power generation and transmission will be discussed, where a summary of such research works is presented in Table III. Along with the development of the smart grid, the conventional nonrenewable and centralized power generation is being replaced by renewable power-based DGs. The utilities usually face high costs for cybersecured 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 the 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 the isolated or grid-connected mode. Then, the power generation and transmission for the smart grid with integrated DGs at a high penetration level can be effectively controlled by leveraging the microgrids using a decentralized multiagent-based control system (DMACS) [44], [74], [105].

在本节中，将讨论区块链在发电和输电方面的应用，此类研究工作的总结如表 III 所示。 随着智能电网的发展，传统的不可再生能源和集中式发电正在被基于可再生能源的分布式发电机所取代。 公用事业公司通常面临高成本的网络安全和高效通信和控制基础设施，以控制传统集中式结构中的这些 DG [104]。 此外，集中式控制结构使 DG 的发电控制面临单点故障。 为了有效和安全地控制 DG，在智能电网主题下出现了微电网的想法。 在微电网中，本地 DG、储能系统和本地电力需求由微电网运营商控制，以隔离或并网模式运行。 然后，通过使用分散式多智能体控制系统 (DMACS) [44]、[74]、[105] 来利用微电网，可以有效地控制具有高渗透水平的集成 DG 的智能电网的发电和传输。

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 the local electricity market [59], [84], [106]–[111]. 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 encouraging the local prosumers to help utility in meeting local demands [84], [106]. 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 the blockchain can prevent fraud attempts in power trading processes [110]. The asymmetric cryptography and tamper-proof feature of the blockchain can provide authentication and authorization to protect the integrity and accountability/nonrepudiation of power transactions. Also, the public–private key pair in asymmetric cryptography can better protect the confidentiality of data [111].

基于发电和输电系统的 DMACS 结构，研究人员引入了基于区块链的智能合约，以在当地电力市场的微电网内部和微电网之间安全地交换消费者和产消者之间的电力 [59]、[84]、[106] –[111]。 基于区块链的本地电力交易智能合约功能背后的主要思想是允许消费者通过 P2P 电力交易从本地产消者那里购买电力，同时鼓励当地产消者帮助公用事业满足当地需求 [84]，[106]。 通过使用基于区块链的智能合约，本地 DG 的发电量和通过 P2P 电力交易进行的电力传输可以在无需第三方的情况下被验证并安全地记录在区块链中。 区块链的透明度可以防止电力交易过程中的欺诈企图 [110]。 区块链的非对称密码学和防篡改特性可以提供身份验证和授权，以保护电力交易的完整性和可问责性/不可否认性。 此外，非对称密码学中的公私钥对可以更好地保护数据的机密性[111]。

Moreover, independence on a third party significantly reduces the power transaction costs, which further facilitates the usage of DGs [109]. Due to the cybersecurity 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 the 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 the blockchain in power generation and transmission are introduced in [108]. The optimization techniques, such as economic dispatch and dynamic load redistribution in transmission systems, can also be integrated with the blockchain by leveraging smart contracts and DAPPS services [77], [112]. With the 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 [112], a blockchain-assisted economic dispatch mechanism is proposed for power distribution system operation. As shown in Fig. 5, within the 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 the 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 cyberattacks in the electricity wholesale market, such as DoS attack on economic dispatch [113]. Furthermore, the blockchain-enabled AMIs can also be implemented for renewable power certification [114].

此外，对第三方的独立性显着降低了电力交易成本，进一步促进了 DG 的使用 [109]。 由于区块链可以为发电和输电带来网络安全和潜在的经济利益，一些初创公司开发了当地的电力市场平台，以实施区块链支持的电力交易和电力招标，包括 Piclo 在 英国、荷兰的 Vandebron 和美国的 Brooklyn Microgrid。 在[108]中介绍了这些初创公司的详细信息以及区块链在发电和输电方面的实际应用案例。 传输系统中的经济调度和动态负载再分配等优化技术也可以通过利用智能合约和 DAPPS 服务 [77]、[112] 与区块链集成。 借助区块链，经济调度功能可以自动向参与的发电商招标，根据招标出清电力批发市场，并公开招标的电价和结算的采购电价。 在[112]中，提出了一种用于配电系统运行的区块链辅助经济调度机制。 如图 5 所示，在区块链内部，节点负责执行交易和智能合约，并以分布式账本的形式维护世界状态和交易数据。 客户和系统运营商通过结构认证 (F-CA) 机制与对等方通信来加入区块链。 加入区块链后，客户将更新他们的用电/发电偏好，例如发电的边际成本和用电的边际效用，更新后的偏好将作为世界状态存储在区块链中。 系统运营商可以从世界状态中读取偏好数据，进行经济调度，得到区域边际电价，用于形成智能合约。 节点将使用智能合约自动提交相应客户之间的电力交易。 该机制可以显着提高电力系统经济调度的效率和安全性。 这种方法为电力批发市场的网络攻击提供了数据保护和弹性，例如对经济调度的 DoS 攻击 [113]。 此外，支持区块链的 AMI 也可以用于可再生能源认证 [114]。

The integrity and accountability/nonrepudiation of distributed electric power system SE results are crucial for dynamic load redistribution in transmission systems. However, the current SE is vulnerable to FDI attacks. By utilizing the blockchain-enabled ICT devices in the smart grid, the blockchain-based distributed SE 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]. Other severe data integrity attacks against SE, such as distributed DoS (DDoS), data framing, and cybertopology attacks, can also be defended using the blockchain technology [115], [116]. For example, during the DDoS attack, the AMIs communications is not functional, but DAPPS layer of blockchain can still provide actual data of power consumption [117]. Instead of protecting the measurement data from AMIs communication failure caused by the 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 [118] and for DDoS prevention by implementing distributively static resource allocation mechanism on the blockchian-based IoT system [119]. 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 the blockchain network [117]. This enhances the performance of dynamic load redistribution in the transmission system [120].

分布式电力系统 SE 结果的完整性和责任性/不可否认性对于传输系统中的动态负载重新分配至关重要。 然而，当前的 SE 容易受到 FDI 攻击。 通过在智能电网中利用支持区块链的 ICT 设备，基于区块链的分布式 SE 功能可以通过提供完整性保护来降低数据篡改的风险，并帮助检测除传统不良数据检测机制之外的数据操纵 [58]。 其他针对 SE 的严重数据完整性攻击，例如分布式 DoS (DDoS)、数据框架和网络拓扑攻击，也可以使用区块链技术 [115]、[116] 进行防御。 例如，在 DDoS 攻击期间，AMI 通信不起作用，但区块链的 DAPPS 层仍然可以提供实际的功耗数据 [117]。 基于区块链的物联网系统不是保护测量数据免受 DDoS 攻击引起的 AMI 通信故障，而是通过使用智能合约 [118] 中实现的计数器和比较器组件支持智能电网进行 DDoS 检测，并通过 DDoS 预防 在基于区块链的物联网系统上实施分布式静态资源分配机制 [119]。 此外，由于 SCADA 和 PLC 控制可通过区块链网络中的智能合约获得，因此公用事业可以在紧急情况下轻松安全地检测并将电力重定向到受影响的区域 [117]。 这增强了传输系统中动态负载重新分配的性能 [120]。

With the blockchain-based distributed SE function and embedded IoT system in the smart grid, the blockchain can provide variant functionalities for secured and reliable distributed power transmission system operation [121]. For example, the static var compensator can be continuously and securely monitored and controlled using smart contract. Protection relays like longdistance and differential voltage relays can be controlled by distributed blockchain ledgers, which can prevent the loss of control signals. Voltage control transformers at a transmission level can be monitored by a smart contract to provide automated functionality. Besides protecting data integrity and accountability/nonrepudiation, 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 the blockchain can be potentially utilized to calculate demand forecasting and ac power flow in a distributed manner.

借助智能电网中基于区块链的分布式 SE 功能和嵌入式物联网系统，区块链可以为安全可靠的分布式电力传输系统运行提供多种功能 [121]。 例如，可以使用智能合约对静态无功补偿器进行持续、安全的监控。 远程和差压继电器等保护继电器可以通过分布式区块链账本进行控制，可以防止控制信号丢失。 传输级别的电压控制变压器可以通过智能合约进行监控，以提供自动化功能。 除了保护数据完整性和责任/不可否认性，区块链在保证分布式电力传输系统运行的数据可用性方面具有强大的优势[77]。 此外，区块链的部分计算能力可以潜在地用于以分布式方式计算需求预测和交流潮流。

1. Blockchain for Power Distribution and Utilization

C. 配电与用电区块链

For power distribution and customer-side power utilization, the blockchain also provides a variant of cybersecurity functionalities [28], [30], [44], [79], [82], [122]–[127], [129], [130]. A summary of such research works is described 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 a 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 cyberphysical distribution system (A-CPDS) [131]. The P2P data transfer, cybersecurity, confidentiality protection, and transparency features of the blockchain technology have made the blockchain a promising solution to improve the cybersecurity and efficiency of A-CPDS [130].

对于配电和客户端用电，区块链还提供了网络安全功能的变体 [28]、[30]、[44]、[79]、[82]、[122]-[127]、[129] ，[130]。 表 IV 中描述了此类研究工作的摘要。 传统的配电系统通常被指定具有足够的容量储备来稳定地为客户提供电力并且留下低程度的监视和控制。 然而，随着具有双向潮流和高渗透率的 DG 并网，传统的负荷和潮流模式发生了显着变化。 为解决这一问题，配电系统正在重新开发，以集成大量支持物联网的ICT设备，以提高系统的可观察性和可控性。 这种重新开发的配电系统被定义为主动网络物理配电系统 (A-CPDS) [131]。 区块链技术的 P2P 数据传输、网络安全、机密保护和透明特性使区块链成为提高 A-CPDS 网络安全和效率的有前途的解决方案 [130]。

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 the 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/nonreputation protections and improve the authentication/authorization levels for customer-side ICT devices [132].

在 A-CPDS 的背景下，智能家居配备了各种支持物联网的 ICT 设备，例如 AMI 和电源管理系统，在个人客户和电网之间建立了良好的互连性。 这提高了客户侧的电力利用性能。 然而，来自客户端的不良数据入侵引起的隐私泄露和智能电网数据完整性攻击的担忧极大地阻碍了智能家居的发展[68]。 区块链被视为通过提供完整性、机密性和问责制/无名誉保护并提高客户端 ICT 设备的身份验证/授权级别 [132] 来促进智能家居发展的合适方法。

In [132] and [133], the private blockchain is established, based on the HAN, to allow for secured electrical appliances usage data uploading to the cloud server of the power management system. The usage of the 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 [132]. Also, based on the blockchain cloud server for smart homes, the remote electricity bill payment function with high level of cybersecurity against theft of electricity is added in [44] and [124]. 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.

在 [132] 和 [133] 中，基于 HAN 建立了私有区块链，以允许将安全的电器使用数据上传到电源管理系统的云服务器。 私有区块链的使用是为了为客户提供更好的隐私保护。 根据上传的使用数据，可以将家庭电源管理策略实施到智能合约中，实现自动化控制。 由于该策略是分布式复制和存储的，因此可以轻松检测和分析任何异常用电行为[132]。 此外，基于智能家居的区块链云服务器，在[44]和[124]中增加了具有高网络安全性的远程电费支付功能以防止窃电。 使用区块链智能电表，可以自动生成电费单并上传到区块链云服务器，不可篡改。 使用适当的私钥，用户可以轻松访问账单信息并进行远程支付。

In addition to providing cybersecurity for integrity, confidentiality, and accountability/nonreputation of electricity usage bill, the blockchain-based remote electricity bill payment function can also significantly reduce the bill payment cost and settlement time [124]. In A-CPDS, the blockchain with smart contract functionality can also be used for secured and trusted DR of smart homes [74], [130], [134]. 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 the blockchain for AMIs, the distributed DR can be implemented. The blockchain 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 the blockchain can ensure that the abnormal DR actions can be regulated and/or punished in a trust and fairway [74].

除了为用电账单的完整性、机密性和问责性/无信誉性提供网络安全外，基于区块链的远程电费支付功能还可以显着降低账单支付成本和结算时间[124]。 在 A-CPDS 中，具有智能合约功能的区块链也可用于智能家居的安全可信 DR [74]、[130]、[134]。 通过使用区块链技术，可以降低实时电价发布的时延，保证需求响应的公平性和有效性。 此外，智能合约可用于确保客户提供所请求的 DR 电力，从而防止欺诈活动。 此外，利用区块链的 DAPPS 服务为 AMI 实现分布式容灾。 区块链可以保护关键数据的可用性，如电价信号、辅助服务信号和区域系统状态，用于分布式 DR。 此外，区块链的可审计性可以确保异常的 DR 行为可以在信任和公平的道路上得到监管和/或惩罚 [74]。

Furthermore, the blockchain-enabled automated and cybersecured machine-to-machine transactions, which includes auctions, bidding, and payment, can be utilized for the smart charging of EVs [135]. In [136] and [137], 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 the 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 the blockchain can guarantee that the payment is cleared only when the user and charging station provider agrees on the realized charging amount [136]. The cyberresiliency nature of the blockchain can protect the billing system from adversary data manipulation.

此外，支持区块链的自动化和网络安全的机器对机器交易，包括拍卖、投标和支付，可用于电动汽车的智能充电 [135]。 在[136]和[137]中，研究了基于区块链的电动汽车充电计费系统，该计费系统指定用于电网到车辆（G2V）模式下电动汽车与充电站之间的电力交易。 通过使用基于区块链的计费系统，电动汽车用户可以获得实时充电价格，并在充电服务后立即进行支付。 此外，区块链中支付结算的相互认证可以保证只有当用户和充电站提供商就实现的充电量达成一致时，支付才会被清算[136]。 区块链的网络弹性特性可以保护计费系统免受对手数据操纵。

An extension of the blockchain-based billing system is proposed in [135], which also considers the autonomous EV charging optimization by using smart contract functionality in the 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 the G2V mode, which considers only unidirectional power flow from the grid to EV, the vehicle-to-grid (V2G) and vehicleto-vehicle (V2V) modes can be used to balance the supply and demand, reduce load fluctuation, and support voltage stability in the power distribution system [123]. The techniques proposed in [44], [82], [125], [137]–[140] 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 the 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 the 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 the blockchain, the transaction and EV charging/discharging data can be easily traced, which can help the system analyze and identify any susceptible adversary behaviors.

[135] 中提出了基于区块链的计费系统的扩展，它还考虑了通过在区块链中使用智能合约功能来优化自主 EV 充电。 通过使用智能合约，EV 用户可以向不同的充电站请求多个投标，以在满足充电需求的同时最大限度地降低充电成本。 与仅考虑从电网到电动汽车的单向功率流的 G2V 模式不同，车辆到电网 (V2G) 和车辆到车辆 (V2V) 模式可以用于平衡供需，减少负载波动，以及 支持配电系统中的电压稳定性 [123]。 [44]、[82]、[125]、[137]-[140] 中提出的技术介绍了联网电动汽车可以使用支持区块链的交易平台从智能电网请求充电/放电的方法，如果 作为回报，他们通过 V2G 或 V2V 支持电网。 例如，可以通过智能合约 [44] 中实施的智能竞价算法使用 AdBEV 在电动汽车和电网之间交换电力。 如图 6 所示，从电网、其他 EV 和 DG 购买电力的电价可以通过区块链发布供公众审查，其中数据的完整性和机密性可以得到很好的保护。 智能合约中实现的最便宜的定价算法可以用来选择首选的电力供应商，智能合约在用户和选定的电力供应商之间发布。 智能合约相互认证后，电力流动和支付可以由智能合约自动执行，没有任何延迟。 由于区块链的可审计性，交易和电动汽车充电/放电数据可以很容易地被追踪，这可以帮助系统分析和识别任何易受影响的对手行为。

IBM predicts that autonomous vehicles and self-driving cars will be in demand abundantly by 2020 [126]. In [127], cybersecurity for these vehicles is provided by the blockchain-based IoT system. Data collected from sensors flow through the blockchain with smart contracts and DAPPS services with predefined 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 [126]. These processes need a high level of security and can only be handled by a trusted system, which is, in fact, the main feature of the blockchain. The same process can be implemented on the smart grid for automatic maintenance. Such add-ons in the smart grid operation will provide customer satisfaction and increased levels of serviceability, reliability, and security.

IBM 预测，到 2020 年，自动驾驶汽车和自动驾驶汽车的需求量将很大 [126]。 在 [127] 中，这些车辆的网络安全由基于区块链的物联网系统提供。 从传感器收集的数据通过具有预定义逻辑的智能合约和 DAPPS 服务的区块链流动。 例如，如果传感器检测到电动汽车有任何问题，基于智能合约，它会自动安排与制造商的预订，并在指定时间前往那里。 [126] 中介绍了更多基于区块链的流程，例如加油、充电、电子停车和维修。 这些过程需要高度的安全性，并且只能由可信系统来处理，这实际上是区块链的主要特征。 可以在智能电网上实现相同的过程以进行自动维护。 智能电网运营中的此类附加组件将提供客户满意度和更高水平的可服务性、可靠性和安全性。

Smart contract functionality backed by the proof of power algorithm is introduced in [28], which was adopted to reduce the consensus delay. This algorithm proves to be better for the case of P2P power transaction and can be beneficial for G2V and V2G/V2V. A comparison of this technique with HyperledgerPBFT consensus can be done to obtain further insights into this consensus. Furthermore, proof of probability algorithm also shows good performance [128], which can also be adapted in the grid space to achieve fewer transaction delays. Anonymous power trading between EVs is discussed in [129], with performance analysis and proof of practicality of the blockchain for cybersecured V2G/V2V applications.

[28] 中引入了由权力证明算法支持的智能合约功能，用于减少共识延迟。 该算法被证明对 P2P 电力交易的情况更好，并且可以有利于 G2V 和 V2G/V2V。 可以将该技术与 HyperledgerPBFT 共识进行比较，以进一步了解该共识。 此外，概率证明算法也显示出良好的性能[128]，它也可以在网格空间中进行调整以实现更少的交易延迟。 [129] 中讨论了 EV 之间的匿名电力交易，以及网络安全 V2G/V2V 应用程序区块链的性能分析和实用性证明。

1. POTENTIAL FUTURE RESEARCH DIRECTIONS

五、未来可能的研究方向

A comprehensive review for the blockchain in the smart grid for cybersecurity 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 the blockchain for smart grid cybersecurity have been discussed. However, as an emerging technology, the usage of the blockchain in the 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 cybersecurity of the 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.

上文对智能电网中的区块链网络安全进行了全面审查。 其中，探讨了区块链在智能电网网络安全领域的系统架构、实现平台和应用。 然而，作为一项新兴技术，区块链在智能电网中的应用仍然面临着巨大的挑战。 在本节的其余部分，将讨论上述基于区块链的智能电网网络安全研究工作中尚未充分考虑的一些主要问题以及应对这些挑战的区块链技术的最新进展。 最后，将强调输配电系统未来潜在的研究方向。

1. Major Issues and Recent Advances

A、主要问题和最新进展

For the wide applications of the blockchain for cybersecurity in the 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 [141], 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 the blockchain for largescale applications. However, the framework proposed in this article is vulnerable to pollution attacks. Advancement in this framework is being investigated to make it more robust against cyberattacks. Furthermore, a fast, low storage, and a nonlinear fashioned blockchain is developed in [142], 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 [143]. The study in [144] casts light on types of blockchains that can be used for industrial and other generic applications, and the work in [144] 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 [145], where the usage of PBFT consensus is studied in depth. Furthermore, the comparison between PBFT and PoW in [146] proves that PBFT is more suitable for blockchain-based IoT systems.

随着区块链在智能电网网络安全领域的广泛应用，分布式账本的规模将越来越大，存储需求将变得巨大。 这将减慢用于数据处理的区块链网络，并影响智能电网运行的效率和可靠性。 在[141]中，提出了一种基于网络编码（NC）和分布式存储（DS）的高效区块链存储架构，以减少存储空间并提高区块链的大规模应用效率。 然而，本文提出的框架容易受到污染攻击。 正在研究此框架的进展，以使其更强大地抵御网络攻击。 此外，在 [142] 中开发了一种快速、低存储和非线性模式的区块链，它利用轻量级节点连接到区块链网络。 这些轻量级节点仅携带标头并指定用于验证，而不会携带太多数据。 与基于 NC 和 DS 的架构相比，这样的区块链被证明可以抵御 DDoS 攻击，并且可以在稳健性和效率方面提供更好的性能 [143]。 [144] 中的研究阐明了可用于工业和其他通用应用程序的区块链类型，[144] 中的工作说明了其适用性。 此外，研究人员还讨论了使用不同共识算法对基于区块链的物联网系统性能的影响。 关于这些影响的更全面的分析可以在 [145] 中找到，其中深入研究了 PBFT 共识的使用。 此外，[146] 中 PBFT 和 PoW 的比较证明 PBFT 更适合基于区块链的物联网系统。

Currently, the lack of scalability is still a great challenge impeding the practical applications of the blockchain in the smart grid for cybersecurity [147]. To address the scalability issue, consortium blockchain is used for cybersecured microgrid operation in [147] and [148] and data regulation mechanism in [71] for data aggregation in the smart grid. The consortium blockchain introduced proves to be much faster and secure. Computational complexity in the blockchain has been reduced significantly. The permissioned blockchain is used in [149] to perform a comparison between gas consumption with a focus on privacy in the 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.

目前，缺乏可扩展性仍然是阻碍区块链在网络安全智能电网中实际应用的一大挑战[147]。 为了解决可扩展性问题，联盟区块链用于 [147] 和 [148] 中的网络安全微电网操作，以及 [71] 中的数据监管机制用于智能电网中的数据聚合。 事实证明，引入的联盟区块链更快、更安全。 区块链中的计算复杂性已大大降低。 在[149]中使用许可的区块链来比较智能电网中的天然气消耗和隐私。 使用这种修改后的区块链可以提供更好的计算性能，同时牺牲机密性保护。 快速公有的区块链是智能电网区块链运行的最佳选择。 然而，需要进行修改以提供更好的隐私保护。

Numerous research works have tried to improve privacy protection by adopting an anonymous external system. For example, in [150], 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 the 5G technique is discussed in [151] 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 cybersecurity of the large-scale smart grid [152].

许多研究工作试图通过采用匿名外部系统来提高隐私保护。 例如，在[150]中，建立了一个基于区块链的匿名信誉系统（BARS），为公共区块链提供一个隐私保护的信任模型。 通过利用 BARS，可以通过利用公钥存在/不存在证明在公共区块链中有效地实现证书和撤销透明度。 [151] 中讨论了 5G 技术在智能电网应用中的使用，以减少通信时间的延迟。 然而，当它开始推出时，高昂的基础设施成本将是一个巨大的挑战。 Hyperledger 结构技术赋予所有者控制节点访问的权限，已被证明是大规模智能电网网络安全的潜在解决方案 [152]。

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 cybersecurity levels [153]. In [153], a lightweight proof of block and trade (PoBT) consensus algorithm is proposed to improve the cybersecurity 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 [153] is explicitly designated for business applications, where a trusted certified authority is required to guarantee the security and efficiency of PoBT. In the 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 [153] 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 the smart grid. One possible solution to address this issue is considering the extension of PoBT consensus algorithm in [153] 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 the 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 [154], 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 a cross-chain framework in the smart grid, e.g., the side chain interoperability [155].

然而，由于 Hyperledger 结构涉及少量节点并且主要侧重于验证添加到块中的数据，因此它仍然存在低网络安全级别 [153]。 在 [153] 中，提出了一种轻量级的区块和交易证明（PoBT）共识算法来提高私有区块链的网络安全性，它允许数据和区块验证。 更重要的是，随着参与节点数量的变化，PoBT 可以实现比 Hyperledger fabric 更好的吞吐率和更低的通信带宽要求。 然而，[153] 中提出的 PoBT 明确指定用于业务应用程序，其中需要受信任的认证机构来保证 PoBT 的安全性和效率。 在智能电网中，存在大量的权威机构，例如输配电系统运营商（T/DSO）、微电网运营商（MGO）和电动汽车聚合商，它们代表着不同的主体。 [153]中没有讨论从代表整个智能电网系统不同方的一组权威中选择一个可信的认证权威，这给在智能电网中应用 PoBT 带来了巨大的挑战。 解决这个问题的一个可能的解决方案是考虑将 [153] 中的 PoBT 共识算法扩展到联盟区块链，以类似于 PBFT 共识算法的投票过程的方式增加一个用于可信认证机构/权威选择的层。 另一种可能的解决方案是利用智能电网中的跨链框架。 针对配电系统管理、微电网运行、电动汽车充电管理等不同应用场景，跨链框架中建立了多条侧链，以主链为骨干。 这样，可以很容易地根据应用场景选择每个侧链的可信认证机构。 在[154]中，研究了物联网数据管理的跨链框架。 然而，跨链框架在智能电网中的应用仍有许多挑战需要解决，例如侧链互操作性[155]。

The public blockchain provides better cybersecurity by devoting the great computational power of mining nodes. However, the increasing computational power attributes great impacts on the energy efficiency of the 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 the 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 the blockchain in the smart grid.

公共区块链通过投入挖掘节点的强大计算能力来提供更好的网络安全。 然而，不断增加的计算能力对基于区块链的智能电网的能源效率产生了巨大影响。 例如，公链中广泛使用的PoW共识机制，共识过程需要消耗大量能源，碳足迹和电子垃圾也很大。 现有的共识机制不支持智能电网的可持续发展。 为共识机制设计适当的鼓励和惩罚机制，鼓励减少能源消耗和使用可再生能源发电，是区块链在智能电网中特定应用的未来重要研究方向。

Since the blockchain still suffers from several cybersecurity vulnerabilities [156], the integration of the blockchain may expose the smart grid to new types of cybersecurity issues. In the past few years, cryptanalysis of the hash function has been an active research area, and various types of cyberattacks against the hash function in the blockchain have been proposed [157]. 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 the smart grid through delay attack. Targeting on the whole blockchain network, the DDoS cyberattack can disconnect multiple nodes from the network. As an important component of the blockchain-based smart grid, smart contracts’ vulnerabilities have severe impacts on the stability and reliability of the smart grid operation. As discussed in [158], the smart contracts can be easily tampered through an 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 tradeoffs still require great attention. Cyberattacks on the blockchain like DAO, which occurred in 2016 on Ethereum, only strengthened and helped evolve this technology to be more cyberresilient and robust [159]. Attacks like these will expose more loopholes in the coming future.

由于区块链仍然存在一些网络安全漏洞[156]，区块链的集成可能会使智能电网面临新型网络安全问题。 在过去的几年里，哈希函数的密码分析一直是一个活跃的研究领域，并且已经提出了针对区块链中哈希函数的各种类型的网络攻击[157]。 利用成功的交替哈希函数，交易延展性攻击可以误导能源消费者在 P2P 能源交易中进行两次支付。 将区块链网络分区以防止节点相互通信的路由攻击能够通过延迟攻击篡改智能电网中的数据。 针对整个区块链网络，DDoS 网络攻击可以断开多个节点与网络的连接。 作为基于区块链的智能电网的重要组成部分，智能合约的漏洞严重影响智能电网运行的稳定性和可靠性。 正如 [158] 中所讨论的，智能合约可以通过交替源代码、渗透虚拟机和修改运行时环境轻松篡改。 此外，可用性也是一个很大的挑战，因为一些用户可能会丢失他们的私钥，从而导致他们的账户永远被锁定。 其中一些问题已经被新的区块链纠正，但这会导致用户隐私的减少。 目前，这种权衡仍然需要引起高度重视。 2016 年在以太坊上发生的 DAO 等区块链网络攻击只会加强并帮助发展这项技术，使其更具网络弹性和稳健性 [159]。 像这样的攻击将在未来暴露出更多的漏洞。

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 the smart grid, multiple blockchains may be required to achieve effective operation of the 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 the smart grid under no centralized authority that allows for seamless, cyberresilient, 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 the smart grid.

正在为基于区块链的智能电网研究和开发在协议、机制和技术方面彼此不同的几种区块链技术。 此外，由于智能电网的地理和运营复杂性，可能需要多个区块链才能实现智能电网的有效运营，其中不同实体可能负责具有不同目标的不同区块链。 然而，对于具有独特技术的不同区块链之间的无缝互操作性，仍然缺乏适当且被广泛接受的标准。 因此，迫切需要在没有中央集权的情况下在智能电网中实现区块链标准化，以允许在具有不同技术和目标的不同区块链之间无缝、网络弹性和高效地交换数据。 区块链技术对许多人来说是一个很好的替代方案，但它仍然需要更多的改进，特别是对于智能电网。

1. Potential Future Research Directions

B. 潜在的未来研究方向

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

为了更好地解决上述问题，可以进一步研究一些研究课题。 可以用不同的体系结构进一步研究基于区块链的智能电网框架的开发，该框架具有专门用于智能电网应用程序的 IDS 和 DAPPS。 可以研究和开发基于区块链的智能电网测试框架，考虑 DDoS 攻击、Sybil 攻击、路由攻击和中间人攻击。 在本文中，我们将重点介绍输配电系统未来可能的研究方向。

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 cybersecured monitoring and control of the 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.

1）分布式输电系统监控：具有智能合约功能的区块链可以分布式实现，通过多个分布式区块链网络组成整个输电系统的区块链网络。 这使得对传输系统的分布式和网络安全监控成为可能，这可能会解决 DG 渗透水平提高的问题，并防止输电系统运行出现单点故障。 例如，电力传输系统可能被划分为不同的区域，这些区域由不同的支持物联网的 ICT 设备组监控，这些设备具有包含控制逻辑和算法的智能合约。 可以选择一个区域作为指挥中心，并可以开发一种机制来调用划分区域之间的合同，同时考虑测量和控制信号的同步。 此外，分布式控制算法需要允许每个划分的区域都有其子合同来控制其区域内的发电和利用。

2) Power Distribution System Automation System: The blockchain-based smart contracts may also be developed with complex algorithms for cybersecured RTUs and IEDs control in the smart grid. For example, in the 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. Furthermore, 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 the 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 the Ganache virtual server.

2) 配电系统自动化系统：基于区块链的智能合约也可以用复杂的算法开发，用于智能电网中的网络安全 RTU 和 IED 控制。 例如，在配电系统中，可以使用基于区块链的智能合约来控制分接开关以进行电压调节。 图 7 显示了基于区块链的电压调节的潜在控制程序。智能合约可以部署在 PMU 中以测量电压水平。 测量结果可以发布在公共区块链上，并由部署在抽头变换器中的智能合约使用，以稳定电压水平。 智能合约也可以部署在 DG 控制器中，用于命令 DG 输出响应电压调节要求。 此外，还可以开发性能评分机制，以发现违反电压调节要求的 DG，并通过使用智能合约为支持的 DG 打分。 此外，还可以开发基于通用区块链平台的测试系统，对基于区块链的智能电网控制系统进行测试。 具有灵活的智能合约设计特点的以太坊区块链可以作为测试系统的区块链网络。 基于以太坊的测试系统的潜在接口如图 8 所示。在测试系统中，可以使用一些常见的编码语言，例如 JavaScript 和 Python，对智能合约进行编码。 此外，智能合约需要能够与以太坊区块链网络进行交互。 一种潜在的方法是在本地服务器中嵌入 Solidicity 中的智能合约，然后通过 Ganache 虚拟服务器与以太坊区块链进行交互。

VI. CONCLUSION

六。 结论

With the development of the smart grid, new challenges arise to improve the cybersecurity of the smart grid. Many methods have been proposed to make the smart grid more resilient against cyberattacks. Among these methods, the blockchain is a promising solution for protecting smart grid cybersecurity. In this article, a comprehensive review of blockchain-based protection mechanism for cybersecurity of the smart grid was conducted. Data protection was enabled by storing data in blockchain network and was validated by peers within the same network. The verified data could then be used for advanced smart grid operations, such as load forecasting, local redistribution, and DR. Blockchain-based platforms, applications, and services suitable for the smart grid with an emphasis on cybersecurity were studied in-depth in this article. Many types of applications can be structured on blockchain DAPPS layer, which helped establish control of the smart grid with security over cloud and autonomy. Therefore, blockchain could improve the cybersecurity for data collection, storage, transfers, as well as control execution in the smart grid. Blockchain is a promising solution for the smart grid cybersecurity improvement. However, there were still great challenges from both the perspective of the vulnerabilities of blockchian technologies and the implementation of blockchain in the smart grid. In this article, the potential future research directions were discussed in detail to provide some guidance for the research on the blockchain-based smart grid.

随着智能电网的发展，提高智能电网的网络安全也面临着新的挑战。 已经提出了许多方法来使智能电网更能抵御网络攻击。 在这些方法中，区块链是保护智能电网网络安全的一个很有前途的解决方案。 在本文中，对基于区块链的智能电网网络安全保护机制进行了全面回顾。 数据保护是通过将数据存储在区块链网络中实现的，并由同一网络中的同行验证。 然后，经过验证的数据可用于高级智能电网操作，例如负荷预测、本地再分配和 DR。 本文深入研究了适用于强调网络安全的智能电网的基于区块链的平台、应用程序和服务。 许多类型的应用程序可以构建在区块链 DAPPS 层上，这有助于建立对具有云安全性和自治性的智能电网的控制。 因此，区块链可以提高智能电网中数据收集、存储、传输以及控制执行的网络安全。 区块链是智能电网网络安全改进的有前途的解决方案。 然而，无论从区块链技术的脆弱性还是区块链在智能电网中的实施来看，都还存在很大的挑战。 本文详细讨论了未来可能的研究方向，为基于区块链的智能电网的研究提供一定的指导。