A survey on blockchain-enabled smart grids: advances, applications and challenges

Received: 7 January 2021 | Revised: 29 April 2021 | Accepted: 30 April 2021

IET Smart Cities

DOI: 10.1049/smc2.12010

The Institution of Engineering and Technology WILEY

REVIEW

A survey on blockchain-enabled smart grids: Advances, applications and challenges

Chao Liu[1] | Xiaoshuai Zhang[1] | Kok Koeng Chai[1] | Jonathan Loo[2] | Yue Chen[1]

[1]School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK

[2]School of Computing and Engineering, University of West London, London, UK

Correspondence

Xiaoshuai Zhang, School of Electronic Engineering and Computer Science, Queen Mary University of London, London, E1 4NS, UK.
Email: xiaoshuai.zhang@qmul.ac.uk

Funding information

UK Research and Innovation, Grant/Award Number: 104317

Abstract

Electric power grid infrastructure has revolutionized our world and changed the way of living. So has blockchain technology. The hierarchical electric power grid has been shifting from a centralized structure to a decentralized structure to achieve higher flexibility and stability, and blockchain technology has been widely adopted in the energy sector to deal with grid management, billing, metering, and so on, because of its nature of decentralization. Here, the aim is to provide a multi-dimensional review on the technological advances of the blockchain in smart grids. Its corresponding applications based on these advances, including company projects and use cases, are summarized. Furthermore, the security threat issues in smart grids, Ethereum Virtual Machine (i.e. the operating environment of consensus mechanisms), and smart contracts are analysed, with a brief conclusion to manifest the prior tasks in building secure blockchain-based infrastructures in smart grids. As such, the challenges and features of different protocols and their applicability in each use case are identified to provide an insightful guide for future research studies.

1 | INTRODUCTION

Traditional power grids are generally used to carry power from central generators to a large number of customers. According to some literature studies, the characteristics of this power network mode are summarized as follows [1, 2]. Firstly, the high distribution loss is caused by long distance transmission. Secondly, distribution stations must be built, and there are high civil and installation costs. The risk rate of large-scale power supply accidents is high due to the use of integrated power supply. It is difficult to control and monitor regional power quality and performance. At present, thermal power generation is still widely used, which brings more environmental problems. In addition, its information services are lagging behind the needs of our times. The traditional power network is a rigid system. The access and exit of power supply and the transmission of electric energy are inelastic, which leads to the lack of dynamic flexibility and grouping of the power network. The vertical multilevel control mechanism is slow to respond and cannot build real-time, configurable and reconfigurable systems. The self-healing and self-recovery capability of the system is completely dependent on entity redundancy. There are many information islands in the system which lack information sharing. Although the degree of local automation is constantly improving, due to the imperfection of information and due to weak sharing ability, the multiple automation systems in the system are fragmented, local and isolated, and unable to form a real-time organic unified whole, so the intelligence degree of the entire power grid is low.

In contrast, Smart Grid (SG) uses two-way flows of electricity and information to create an automated and distributed advanced energy delivery network, which is expected to be the next-generation power grid [3]. SG utilizes modern information technologies and computational intelligence in an integrated version to deliver power, which is characterized by self-monitoring, adaptive recovery and distributed generation. The new features of smart grid technology can be concluded as follows:

- Two-way flow: Through the use of electromechanical components, conventional grid transfers electricity and the information goes from power generating units and utilities to consumers in a single direction way. In a smart grid, it adopts Information and Communication Technology (ICT) to allow two-way communication flow, and the electricity can be delivered bidirectionally [3].
- Distributed energy resources: Smart grid utilizes micro-sources such as renewable energy to form a microgrid to support distributed energy systems; however, the traditional grid system is centralized where generation and distribution are hierarchical.

By utilizing micro-sources, SG can control and optimize electricity demands of local areas in a more economical and reliable way. The distributed generation promotes the development of new grid paradigms, which benefits from smart energy subsystem technologies. Storage systems can be used in virtual power plants or nearby loads. The storage system comprises the distributed electricity generators (including renewable energy from the wind, sun, tide and so on) and fast response devices including batteries and EVs, which add flexibility to the control of the microgrid. By storing energy at times of excess power and generating electricity at times of low generation, the microgrid system is capable of accommodating the power demand profile fluctuation. Furthermore, the characteristics of different storage devices can be utilized to tune the frequent and rapid power changes in renewable resources, which brings economic advantages for the microgrid as well as improves the power quality. The technological advances in the smart grid can be categorized into four groups including power and energy technologies, power system capacity, power system performance, and end-user integration [4].

In the process of energy decentralization and digitalization from a traditional hierarchical grid network to a smart grid, the main challenge is to explore the most suitable control paradigm and distributed technologies. Blockchain is a shared decentralized ledger that can support permissioned or permissionless user participation, which provides scalability, security, redundancy and adaptable applications [5]. The inherent nature and recent development of blockchain technology have made it a promising solution for energy grid advancement. Furthermore, compared with conventional SG that fully depends on the redundancy of each entity to ensure system reliability, blockchain can utilize distributed ledger technology (DLT) and consensus mechanisms that can be continuously replicated on all or at least a group of nodes in a blockchain network to avoid a single point of failure. Despite the assistance from blockchain technology, the transformation from the traditional grid structure to the smart grid still faces huge workloads from the infrastructure design, installation and requirements from various stakeholders. The challenges of the smart grid system based on the analysis of current applications are addressed as follows:

1. Integration: The massive distributed energy resources such as solar panels and wind turbines need to be integrated into the smart grid system where power generation is intermediate and unpredictable. The interactions between the distributed resources and grid operators are highly random with different control standards and protocols so that an automated control system is required to accommodate more types of decentralized participants.
2. Scalability: As mentioned above, the rise in the number of participants will increase the number of transactions. The latency will increase with higher user participation. And there is inherent latency of the system response time for communication, power delivery and settlement, which serves the system's scalability [6].
3. Security: Security concern has two aspects, data privacy and the vulnerabilities and mitigations in both blockchain and smart grids. The transaction data in a traditional grid system is exposed to various attacks which can be inferred from a user's identity and activity patterns [7]. Moreover, smart grid systems that utilize advanced ICT protocols can be compromised or eavesdropped due to fake or malicious data attacks in the network [8].

In this regard, this paper presents a comprehensive review of the blockchain technology solution to smart grid transformation from the point of technological advances in its industrial applications and, finally, the challenges and opportunities. Various use cases of blockchain applications in the energy sector demonstrate that blockchain technology will be a game changer in the future. Furthermore, the discussed challenges involve not only the security concerns in blockchain itself but also the threats and safeguards to smart grids that will act as holistic lessons for advancing the combination of blockchain and smart grids in future. Compared with the surveys [9, 10] that do not involve the security concerns related to blockchain-enabled smart grids or only show some high-level security concepts, the strength of our survey is to provide in depth security discussions on both blockchain and smart grids. Meanwhile, compared with two other surveys [11, 12] that only focus on the security and privacy of blockchain, this work also presents the challenges and countermeasures from the perspective of smart grids to offer a broader view of security and privacy for different researchers in the fields of blockchain and smart grids. Our contributions focus on technological insight to evaluate the novelty and feasibility of blockchain technology:

1. This work provides an in-depth understanding of the advances in blockchain technology in the smart grid. We present a comprehensive state-of-the-art solution from a technical perspective which includes consensus mechanisms and smart contracts, and SG operational side, including energy infrastructure and markets.
2. Based on the technological advances, the blockchain-enabled energy sector applications with prospective fields are identified from current pilot projects and trials. A systematic review of the current use cases is provided according to the consensus mechanism type, which emphasizes on the energy system infrastructure design for different scenarios.

3. By analysing the security issues in the smart contract and Ethereum Virtual Machine (EVM), which are two fundamental entities for storing and running consensus mechanisms applied in the energy sector, we conclude the primary missions to develop a more secure running environment for consensus mechanisms in future.

The rest of the paper is organized as follows: Section 2 provides an overview of blockchain technology including terminologies and technologies. In Section 3, blockchain technology in smart grids is presented with key elements and advances. Section 4 reviews state-of-the-art real use cases from pilot projects based on consensus mechanism applications. Section 5 presents a security threat analysis and the challenges exposed in the smart grid and blockchains, and Section 6 provides the conclusion and the scope of future work. A list of abbreviations is also included in Table 1.

TABLE 1 A list of common abbreviations

Smart Grid	SG
Electric vehicle	EV
The Internet of Things	IoT
Information and Communication Technology	ICT
Environment Virtual Machine	EVM
Peer-to-peer	P2P
Proof of Work	PoW
Proof of Stake	PoS
Byzantine Fault Tolerance	BFT
Proof of Authority	PoA

2 | OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Blockchain technology is primarily known from cryptocurrency applications which are viewed as the first stage blockchain. However, blockchain technology is envisaged to have the capacity to reform financial markets, supply chains and business-to-business services [21]:

- Digital securities trading: proof of ownership for asset registries and title transfer of hard assets to secure recording of intangible assets [22].
- Foreign exchange: executes currency exchange and conversions such as Coinbase (wallet) and Kraken [23].
- Digital identity: protects the privacy of consumers by providing an immutable digital identity for users.
- Supply chain: improves transparency in supply chain records with the certification of manufactured products or diamonds certification [24].

The variety of proposed applications expect blockchain technology to bring significant process optimization and novel business models. The potential lies in the DLT which can redefine digital trust and remove intermediaries which disrupt traditional forms of hierarchical governance. The disruptive nature of blockchain technology is able to use consensus within the network to enable an open-source and transparent community to support decision-making and system running.

2.1 | Blockchain deployment

Blockchain is a shared and trusted DLT that permits the recording of any digital asset transaction between parties over a decentralized network, which is initially developed as a mechanism to record financial transaction [25]. Bitcoin is known as the first blockchain application, and the technology is continuously evolving [26]. The advanced features of blockchain are a genuine combination of several techniques including distributed computing, cryptography, peer-to-peer (P2P) communication and game theory, where technological and economic primitives are elegantly considered [27]. Data integrity is guaranteed via the nature of the distributed feature, and the encryption system that uses public and private keys offers users the ability to sign transactions [28].

Blockchain can also be classified as the parent chain and side chain according to the relationship between chains. The comparison between different types of blockchain is demonstrated in the Table 2.

- In a public blockchain, there are no access restrictions for any participant. The transactions on the blockchain are available for checking and all peers are allowed to make transactions. Typical applications include Bitcoin and Ethereum. A public blockchain is used in cryptocurrency, e-commerce, Internet banking, etc. [29].
- In a consortium blockchain, update operations are only allowed for its consortium members. Only the selected set of nodes are responsible for executing the consensus mechanism in the network. It is generally suitable for making payments, accounting and auditing between banks where one block can be globally confirmed after confirmation from two-thirds of the nodes.
- A private blockchain is applied in private organizations for database management and auditing. The value of private blockchain is that it provides a secure, trackable, immutable and automated platform [28].

2.2 | Blockchain operations

A complete blockchain system is composed of complex technologies, for example, digital signature and time stamps for data storage, consensus mechanisms in the P2P network, mining and PoW, bitcoin wallet for an anonymous transaction technique, Merkle tree for data structure, and so on [30]. It is because of the aforementioned technologies that the blockchain system is constantly transacting, validating and

TABLE 2 Comparison among public blockchain, consortium blockchain and private blockchain

	Public blockchain	Consortium blockchain	Private blockchain
Consensus process	Permissionless participation	Consortium member (permissioned participation)	Permissioned participation
Centralized	Decentralized	Multi-centred	Centralized
Data transparency	Public	Private	Private
Reward policy [13]	Yes	Optional	No
Trust model	Untrusted	Semi-trusted	Trusted
Consensus mechanisms	PoW, PoS, DPoS [14]	BFT-based (e.g. PBFT, RAFT [15])	BFT-based (e.g. RAFT [16])
	Large energy consumption	Low energy consumption	Low energy consumption
Finality [17]	No	Enabled	Enabled
Scalability	Good	Bad	Bad
Transaction throughput (per second)	3–200,000	1000–10,000	1000–100,000
Transaction approval frequency	Slow	Medium	Fast
Use cases	Cryptocurrency [18]	Payment, accounting [19]	Auditing, database management (within the organization) [20]

expanding. The fundamental components of blockchain technology are shown below:

- Data block: Transactions are stored in the data block where the block generation rate is roughly 10 min for each block, and each data block contains a header and body. The header encapsulates the version, previous block address, timestamp, nonce, Merkel root, etc., and the body contains the transaction counts and details [31]. Each transaction is permanently stored in the data block and available for checking by anyone. And the Merkle tree in the block body applies a digital signature to each transaction so as to ensure that the transactions are not repeated or forged [32].
- Mining and forks: Mining is the process of searching a random number (nonce) which makes the hash value satisfy the requirement for gaining the right block selection [33]. The newly generated block will be broadcast immediately for validation in case of fraud, and the blocks can be traced back through the hash value. However, there will be forks when two miners successfully mine two blocks at almost the same time. After forking, the system will continue mining and choose the parent chain by calculating the maximum proof-of-work where the fork chain will be abandoned [34]. It has also been noted that some mining techniques require huge energy consumption to compute, which can have significant social and economic impacts [35].
- Timestamps: In the blockchain system, the node needs to add the time stamp when generating a new block to record the block write time. The following block will add an approved time stamp to certify the previous block, which forms a long-term increasing time chain. The timestamp is a significant parameter for the proof of existence, which ensures the immutability of the blockchain system [36].
- Unspent Transaction Outputs (UTXO) [37]: UTXO is the basic unit in the bitcoin transaction process. Except for the genesis block, all transactions (Tx) in the block contain the origin of the funds (TX_in) and the output of the funds (Tx_out). Only the UTXO stored in the network nodes with the digital signature can be transacted. In this way, the system does not need to check its complete transaction history to confirm its legitimacy.
- Hash function: The hash function codes the original transaction data into a fixed-length string, which is composed of numbers and alphabets [38]. This process is single directed so that the coded hash value cannot be interpreted [39]. SHA 256 is the most commonly applied hash function using the Merkle–Damgard function to generate a 256-bit hash value [40].
- P2P network [41]: P2P network is a distributed application framework that is used to assign tasks and workloads between peers. A blockchain system is established upon IP communication protocols and distributed networks. Each node in the peer network has equal rights which do not exist in any centre point or hierarchical structure.

2.3 | Blockchain smart contracts

With the complex design of smart contracts, it can be applied to many areas such as database systems, financial derivative services, etc. [42]. Generally speaking, a smart contract cannot be intervened by human activities once it is successfully

deployed. The Ethereum is a blockchain platform supporting smart contracts, and the advantages of smart contracts can be concluded as follows:

- Real-time updates: A smart contract supported system responds in almost real-time as it does not need an intermediary or third-party authentication, which largely increases transaction efficiency.
- Accuracy: The execution of each contract term is predefined and under the program's control, where all outputs are accurate and predictable [43].
- Low human intervention: Once a smart contract is deployed, the content of its contract cannot be revised by any parties so that any fraud or dishonest behaviour is punishable by the contract [44].
- Low operation cost: The system can achieve low-cost transactions by removing human involvement in transaction, enforcement and compliance costs [45].

Smart contracts are user-defined programs that determine the rules of writing on the ledger [46]. It is a computer protocol that is capable of self-executing and self-verifying without human intervention once it is deployed on the network [47]. In the technological aspect, smart contracts are executable programs that make changes on the ledger and are automatically triggered when being called or when a specific requirement needs to be met.

Before deploying a smart contract, the contract terms and logic flows are made with relevant standards. Then they are recorded in computer language encoding legal constraints and terms of agreements. A smart contract usually provides an interface for human–contract interaction which complies with the recorded logic and rules [48]. With the integration of cryptographic technology, the interaction activities can be authenticated to ensure that the contract is executed without any collisions or fraudulent activities in the process [49]. For example, the management of bank accounts can be viewed as a set of smart contract applications. In the traditional banking system, operations such as withdrawal and deposit need authentication from a centralized bank, and the system cannot run without the bank's supervision. With the aid of smart contracts, any operation can be programmed with strict logic flows and the system runs by calling the smart contract. In Figure 1, it depicts the logical workflow for the smart contracts on the Ethereum platform. Users can define the smart contracts using programming languages such as Solidity, Serpent and Lisp Like Language, which need to be translated into the EVM bytecodes [42]. Then the code is deployed on the Ethereum nodes with the cost of GAS using the Ethereum cryptocurrency for miners' confirmation. After it is successfully deployed, users can obtain an address for the contract and the interface. The Javascript API interface provided from web3.js can be used for calling contracts and making interactions [50].

As a complex combination of various technologies, blockchain is an elegant design of computer science, telecommunication, cryptography and economy. The core

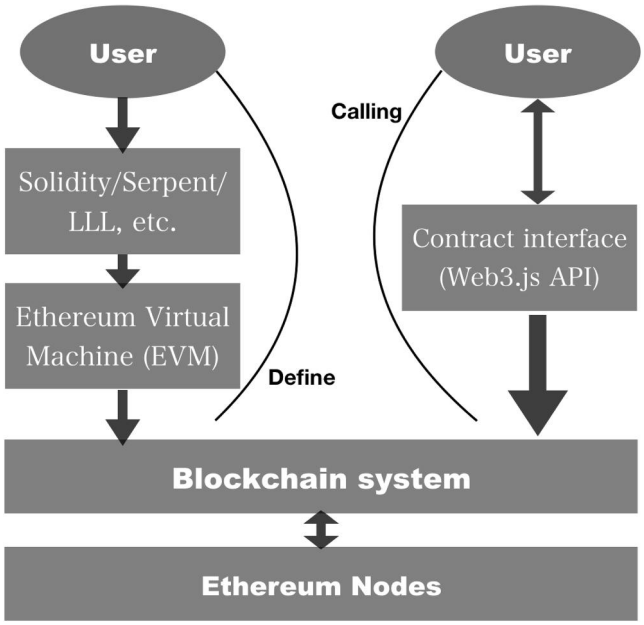

FIGURE 1 The process of smart contract deployment and calling on the Ethereum platform

technologies includes consensus mechanism, unlocking script [51], Merkel proof [52], transaction rules [38], Recursive Length Prefix [53], etc. In particular, this thesis focuses on the following technologies:

1. A smart contract that resides on blockchain and allows the automation of multi-step processes to self-execute the distributed heavy workflows is envisaged in the energy industry and the Internet of things [54]. The use of a smart contract in blockchain technology is driven by open-source agreements, which also provide the potential to balance supply and demand in the transactional energy market. A smart contract also provides insight into allowing the automation of multi-step processes to self-execute the distributed heavy workflows, which is envisaged in the energy industry and the Internet of things.
2. The consensus mechanism guarantees its robustness against misbehaviour and against malicious participants and incentivizes participants to validate transactions [36]. Hence, blockchain is a promising technology for broad business sectors where transparency, trust and efficiency are needed as it can help design and deploy a proper consensus mechanism.

2.4 | Consensus mechanisms

In a distributed system, multiple peers form a network cluster through asynchronous communication where states need to be replicated between different hosts to ensure consistency in all the peers [55]. However, if any of the peers in the cluster encounters attacks or failure, it might cause network congestion and broadcast tampered messages in the network. Hence, a fault-tolerant protocol is needed in the unreliable

asynchronous network to ensure a consistent consensus among all the peers.

As for the blockchain-based distributed ledger, the primary concern is to realize the correctness and consistency of the transaction data from different ledger nodes [56]. The consensus mechanisms in blockchain are the mechanisms or set of rules that enable all the full nodes to reach an agreement or consensus over the order of transactions [57]. There are many types of consensus mechanisms in different blockchain applications or scenarios such as Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS), RAFT, Proof of Authority (PoA), etc. After converging of the blockchain consensus process, the final confirmed block/order of transactions is referred to as the consensus finality [58]. It is worth noting that Directed Acyclic Graphs (DAG) could be an alternative to the traditional blockchain technology and can be categorized as a DLT [59]. It differs from blockchain in how transactions are added to a network, and it aims to improve the existing speed, scalability and cost issues of blockchain technology. Furthermore, by addressing the energy consumption issue generated from resource-intensive designed mining protocols, more studies have also explored the benefits of renewable resources to mitigate those negative environmental externalities [60].

2.4.1 | Proof of Work

Bitcoin is one of the most widely used blockchain systems that use PoW to solve the critical challenge of reaching consensus among participants [18]. PoW requires participants to dedicate computation time and energy towards work (mining), where the processes of initiating this consensus mechanism are called miners. Miners are required to solve a hash code crypto puzzle before encapsulating the transactions into a new block [61]. The miners repeatedly select a nonce, which is the difficulty in solving the puzzle to obtain a result lower than the threshold, whereas the network peers fight using their computation source. In this way, it is nearly impossible for a single attacker to jeopardize the system by modifying the block and solving the puzzle due to extensive computation. So the system can only be controlled or attacked if someone gains 51% of the total network hash power [62].

Undoubtedly, there is a huge waste of energy and it requires a constant global effort. It is claimed that Bitcoin and Ethereum burn over $1 million worth of electricity and hardware costs per day for running the consensus mechanisms [63]. Moreover, in order to reduce the number of forks in the chain, Bitcoin's PoW is designed to produce a new block in an average of 10 min and the difficulty of mining a new block is increasing. The PoW protocol has proved that it scales to a large number of users for public use. However, transaction rates and finality are comparatively low [64]. The recommended waiting frame is six blocks before accepting a transaction, which makes it impossible for many applications such as electricity trading [65].

2.4.2 | Byzantine Fault Tolerance

The origin of BFT algorithms is their work on Byzantine faults which deal with unpredictable actions in computer networks when encountering hardware breakdown, network congestion or malicious attacks [15]. The problem concerns a set of Byzantine generals to agree on a joint plan of action during the war. Generals need to perform a joint action in coordination with the different parts of an army to attack simultaneously; however, the message can only be delivered by senders due to the huge territory. The challenge is to ensure that loyal generals reach a consensus on the plan of attack such that traitors cannot disrupt the attack plan. It is proved that the attack plan can be guaranteed if there are no more than one-third traitors in the system [57].

In the blockchain system, the PBFT algorithm enables a system to reach consensus with a low overhead and proceed transaction within a few network information exchanges that work against up to one-third of the attacks from participants [66]. The PBFT algorithm uses primary and secondary replicas where the secondary replicas check the correctness and liveness of the primary ones so that the complexity decreases from exponential to polynomial [36]. PBFT enables instant consensus finality as blocks are globally verified. The problem of consensus is that participants of the distributed system must agree on and accept a single shared state [67]. It requires the network to have global knowledge of the participants and does not scale the number of participants.

2.4.3 | Proof of Stake

To address the energy consumption waste in the PoW consensus mechanism, various alternative consensus mechanisms have been proposed, such as the PoS mechanism [68]. The approach aims to replace the useless work of solving puzzles by selecting a leader for deciding the next block according to their stake shares. The probability of generating a block depends on the stake of the nodes in the system, which can result in less electricity consumption and a decreased 51% attack probability [17]. In the case of the few rich stake owners performing malicious attacks, PoS can make use of game theory mechanisms to prevent collusions and centralization by penalizing dishonest behaviours.

Moreover, the maximum transaction rate is a few hundred transactions per second, which is low compared with other consensus mechanisms or visa system [29]. The PoS protocol results in a lack of consensus finality and leads to frequent blockchain forks. Even though it is making energy consumption less wasteful, it still requires a fair amount of available computation resources. However, PoS-based algorithms can be used in public blockchains and the validators can be unknown when performing the consensus process without knowing the identity ahead of time compared with PBFT [57].

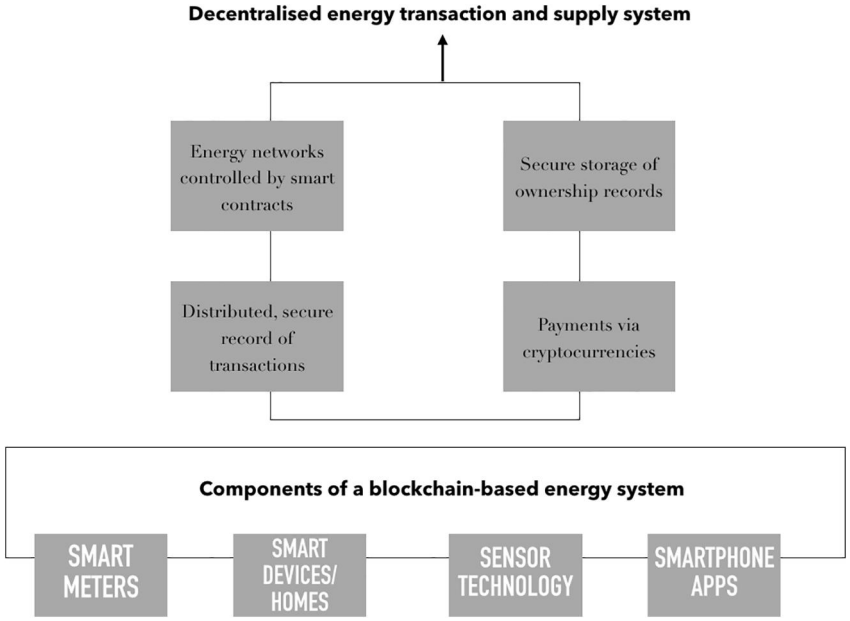

FIGURE 2 Cornerstones of a decentralized energy transaction and supply system

2.4.4 | Proof of Authority

The PoA is designed based on PoS, which is adopted for some private blockchains [69]. The protocol predetermines the authority parities in the network, and each authority is assigned to be the leader within a fixed time slot. Network members trust the authorities and a block is accepted if it receives a majority of approvals from authorized nodes. In this mechanism, it needs to perform KYC to identify the authority ID and background instead of the stake from PoS, where misconduct or manipulation will be publicly revealed [70]. As PoA relies on trusted authorities, it is only suitable for permissioned networks.

3 | ADVANCES IN BLOCKCHAIN-ENABLED SMART GRIDS

Along with use cases and pilot projects in various sectors, the potential of blockchain technology in the energy industry is enormous, which is why it is deemed as a game changer. Blockchain technology enables a trustless network to eliminate the operational cost of participation of the intermediary network and creates a means that is quicker, safer and cheaper in the transactional energy market. According to commercial reports from Deloitte [71] and PWC [72], blockchain has the capability to disrupt energy-related products and commodities which can be traded interoperably as digital assets.

3.1 | System upgrades overview

In Figure 2, it demonstrates the cornerstones of a blockchain-based energy system. Energy trading transactions are recorded on a blockchain in a tamper-proof way, and the energy is delivered via the network (power grid). In general design, transactions (consumer-producer matching) can be affected by smart contracts automatically or by operators in the system manually. With the integration of digital and communication technology, a full energy system with residential use can be achieved along with smart metres, smart devices, sensors and end interfaces. As depicted in the figure, there are some key points with respect to blockchain technology:

1. Energy networks: The supply and demand are balanced via smart contracts with the aid of balancing the market, microgrids, virtual power plants, storage and so on [73].
2. Energy transactions: Transactions data is stored on the blockchain using a decentralized mechanism, with parties identifying themselves through their digital identities, for example, in the context of energy storage, renewable energy, electric mobility and energy trading [32].
3. Record storage: The storage for the ownership records, including emission allowances, renewable energy certificates and asset management, can be securely stored on the blockchain [62].
4. Payment: The payment for transactional energy in the blockchain-enabled energy system does not limit to the fiat currency but also cryptocurrencies, which increases the efficiency and security of the trading process [14].

3.2 | Power sources

The energy system is undergoing a revolutionary reform which is advanced by the ICT and distributed energy resources. One of the main challenges is to decentralize and digitalize the current grid system, where the nature of decentralization in blockchain can be utilized in structures and operations of smart grids. In [74], the transactional energy system refers to a series of energy transactions for the delivery of a certain

amount of energy commodities within a specified time frame and location which can support the business of all parties including generators and distributed system operators.

The concept of transactional energy provides an insight into the treatment of electricity as a commodity in the market. In the market, control mechanism can be applied to achieve various objectives. Besides providing the wholesale market in the conventional grid system, transactional energy provides a vision to aid the coordination of retail customers by automating a large number of frequent batch transactions using a blockchain-enabled platform, therefore reducing the centralized features of the next-generation grid system [75]. The information exchange is the same for a large generator, distributed energy resource, renewable energy generators such as wind and solar energy resources, EV, microgrid, energy trader, broker, exchange, aggregator or system operator. Transactions can be executed between retail and wholesale markets, which equalizes the opportunity for all components. Furthermore, the transactions must also account for the transmission and distribution limits and other physical constraints on the grid. The power source is undergoing tremendous improvement to transition into a more decentralized one, where smart, local energy systems (SLES) are also well noted as forms of local energy projects to provide solutions to system integration and management [76]. The Prospering from the Energy Revolution (PFER) program seeks to develop, test and scale up SLES to deliver cleaner, cheaper and more resilient energy, and the four selection criteria for PFER demonstration projects could define SLES by outcomes rather than by constituent elements [77].

3.3 | Blockchain infrastructure

With increasing interactions between the power grid and electricity users, traditional blockchain infrastructure is no longer sufficient to support a large transaction throughput or a low response time. Consensus mechanism, one of the core parts in the blockchain system, is responsible for the coordination and connection of its stakeholders. In order to build an advanced smart grid application, it should be able to process the electricity and information distribution in order to be more efficient, decentralized, flexible, reliable and secure. In this regard, the consensus mechanism's advances in the blockchain infrastructure are presented in this subsection.

3.3.1 | Proof of Burn

In the Proof of Burn (PoBr) protocol, instead of providing proof of the work, the miner sends the coins to 'burn' in order to gain the right to mine a new block [78]. The miner which burns a larger amount of coin will get a greater chance of being selected by the random selection process. In this way, PoBr protocol does not require the huge hardware cost as PoW does; however, the validation process depends on the willingness to burn coins, which will cause unnecessary waste of resources [13].

3.3.2 | Proof of Elapsed Time

Proof of Elapsed Time (PoET) is designed to address the high power consumption (waste) and latency for transaction confirmation in PoW-based consensus mechanisms. It was first developed by Intel's Sawtooth project [79]. The protocol aims to replicate a random block generation process without spending valuable resources as PoBr or computation power as Bitcoin. By requesting a waiting time from a trusted function in a general-purpose processor, the miner node with the least waiting time is selected to mine the next block. It randomly distributes leadership election across the entire population of validators; however, this approach is dependent on the environment developed by Intel, where trust can only be guaranteed with a single authority [58].

3.3.3 | Enhanced Proof of Benefit

The Enhanced Proof of Benefit (ePoB) consensus mechanism is designed to choose the winning block leadership in the EV charging and discharging scenario [80]. The participants (EV) in the consensus process are a tuple of $\langle U, G, P, A \rangle$, where U is a set of public nodes to submit buy/sell electricity orders; G is a set of gateway nodes, and P is a set of decentralized network peers to execute the consensus process. All routines with charging and discharging requirements execute the verification algorithm of the ePoB consensus mechanism, which maintains and expands the blockchain. A benefit generating algorithm is proposed to calculate the maximum benefit number for the overall grid, where the benefit can be defined by the objective function.

Table 3 presents the comparison between some mainstream consensus mechanisms including PoW, BFT-based, PoS and ePoB. They are compared based on various characteristics such as consensus finality, computation cost, vulnerabilities and so on. As inferred from the table, all consensus mechanisms have their pros and cons. For example, the PoW consensus mechanism performs excellently in the aspects of security and fairness with high scalability; however, the energy consumption with increasing industrial-scale mining process is critical. It is also notable that the scalability of BFT-based consensus mechanisms is low because they require quite high communication overhead between permissioned nodes such as Hyperledger Fabric, which is based on PBFT [82]. On the other hand, the new consensus mechanism PoS is more environmentally friendly; however, it is less secure and fair compared with PoW. Furthermore, different consensus mechanisms adapt to different blockchain types, and the types of blockchain applications depend on use case scenarios. In order to adapt to the frequent trading demands and consider the global power network delivery quality in the energy sector, an adaptable consensus mechanism is required. The advances on consensus protocols support a more dynamic and robust energy grid infrastructure to further innovate the whole industry including electricity pricing, billing, planning and so on.

TABLE 3 Comparison between consensus mechanisms

	PoW	BFT-based	PoS	ePoB
Consensus finality	Probabilistic	Instant	Probabilistic	Instant
Computation cost	High	High (communication complexity/ overhead)	Low	Medium (Local + online)
Latency in Tx confirmation	High (6 blocks confirmation)	Low (high throughput)	Low (as compared with PoW)	Low (as compared with PoW)
Prone to forks	Yes	No	Yes	No
Scalability	High	Low (latency increases exponentially)	High	High
Vulnerability (n denotes the number of network peers)	Prone to 51% attack	Vulnerable to faulty nodes $> (n-1)/3$ ∗Vulnerable to DoS attack	Prone to 51% attack ∗Prone to collusion of rich stakeholders	vulnerable to faulty nodes $> n/2-1$
Type of blockchains	Permissionless	Permissioned	Permissionless and permissioned	Permissionless
Hardware requirement	No	No	No	Vehicle-embedded environment
Use cases	Bitcoin	Hyperledger	Cosmos, Bitshare (DPoS)	PEBT system [81]

Abbreviations: BFT, Byzantine Fault Tolerance; DoS, Denial of Service; ePoB, Enhanced Proof of Benefit; PBFT, Practical Byzantine Fault Tolerance; PoS, Power of Stake; PoW, Power of Work.

3.4 | Customer interface

Blockchain technology has the potential to be applied to various business processes and operations in the energy system, where it can bring novel business models or applications in the following areas:

- Tariff: A smart contract based energy system can enhance the automation process in billing for both consumers and distributed generators, where utility companies may change their tariff and billing plan according to the consumer energy profile, real-time cost or individual preferences [83, 84].
- Trading: A blockchain-enabled grid system can trade with distributed energy producers, which is completely different from traditional wholesale market management [85]. Commodity trading transactions, risk management and energy trading strategies are being explored to accommodate the new system [86, 87].
- Automation: By enabling P2P energy trading, blockchain technology can integrate locally produced energy, which increases energy self-production and self-consumption [88]. The automation process also significantly improves electricity trading and delivery efficiency, thus generating more revenues [89].
- Smart grid management: The integrated energy system in smart devices utilizes advanced communication and machine learning technologies to provide monitoring, controlling and management services. Grid management can not only offer additional services to end users but also improve network performance [83, 90, 91].
- Security and authentication: The protection of transactions and security is guaranteed via cryptographic techniques, which safeguard user privacy and data confidentiality and improves the auditing and regulatory compliance [92].

According to the features of transactional energy, blockchain technology matches the requirements of frequent and large-scale transactions, thus being widely adopted. By utilizing a distributed ledger with smart contracts, locally generated energy can be managed in a compliant way with PFER demonstrations. In [93], a novel energy trading mechanism based on blockchain technology is proposed to adopt the decentralized and competitive environment of locally generated electricity, but the blockchain here is only used as a database to record transactions. In [94], the authors further evaluate the economic features of market mechanism for local energy trading. A comprehensive Internet of thing business model is designed in [95] to enable P2P trade for paid data using blockchain and smart contract. However, the trading model does not perfectly adapt to energy sector trading to address frequent transaction needs and consider the overall system performance. In [96], a dynamic price incentive market mechanism is proposed to balance the local renewable energy production and support flexible demand. In [97], a blockchain-based trading platform is proposed to support the decentralized energy market with distributed optimization and control. In [98], a more sophisticated dynamic power network infrastructure is proposed, which can advance the performance of small-scale generators and the overall capacity resilience of grids.

A blockchain-based energy trading model is proposed to allow prosumers to trade energy in the grid, enabling production companies to achieve autonomy in the blockchain power trading platform, which can inject and draw energy into the smart grid public blockchain trading platform [51]. Henceforth, blockchain has generated broad interests in the

energy trading sector, where all energy traders are peers in the blockchain network.

4 | APPLICATIONS IN SMART GRIDS

Driven by the advances in blockchain technology, utility companies and blockchain teams have explored the feasibility of applying blockchain technology in the energy industry. The authors in [99] concluded eight types of use cases and wholesale, retail and P2P energy trading and cryptocurrencies, tokens and investment accounting take the largest shares among the eight types, accounting for 33% and 19% of the total share, respectively. Mature consensus mechanisms such as PoW and PoS have been applied in many blockchain projects; however, traditional consensus mechanisms might not meet the requirement of the system when combined with energy generation and trading [100]. So the choice of consensus mechanisms is highly correlated with use case which has different requirements for throughput, scalability, latency, security and so on. In this section, we focus on consensus mechanism uses in different energy grid projects and present them according to the types of blockchain-based applications for different purposes.

4.1 | PoW-based

PoW consensus mechanism has proven to be highly scalable for public blockchain, where it is the most commonly used consensus mechanism in applications [62]. The Bankymoon project works with banks to provide blockchain services for cryptocurrencies integrating into smart metres [101]. The project uses smart contracts to execute regulation or policy terms according to the application requirements, thereby effectively reducing transaction latency. A smart metre is used in water and electricity installation, where low-latency transaction is essential and the automated transaction process can achieve an approximate real-time settlement for payments. Bankymoon utilizes a smart contract feature on the Ethereum platform to ensure scalability and latency at the same time. Another PoW-based project named PowerLedger aims at trading P2P renewable energy resources with customers [102]. Blockchain is used to trace the authenticity of green energy, where the trading transparency on the origins can be promised. The solution eliminates the customers' concern about the energy sources, and all transactions are securely recorded on the blockchain. The Australian startup Divvi also focuses on renewable energy trading and ownership, which is also based up Ethereum's smart contracts [103]. However, P2P trading emphasizes more than the origin proof. Another important aspect is matching the customer with renewable energy suppliers or the commodity being traded in this process [87].

The Alliander group from the Netherlands uses a smart metre on the blockchain platform to enable real-time electricity exchange between energy markets (retail and wholesale) and residents [104]. Also, it is developing an EV charging and discharging platform to support dynamic customer contracts. In this way, the EV user can choose the energy supplier and trade with potential renewable energy providers whose electricity sources and prices are transparent to customers [88]. Due to the different application scenarios, Alliander uses multi-chain solutions in different use cases, such as a private blockchain solution which is used for P2P energy sharing platform, and a public blockchain which is adopted for smart metre transaction recordings. The e-mobility application is extremely popular as the EV is a highly dynamic energy source that can charge and discharge electricity to the grid network. PowerLedger and another startup named Everty are also working on the construction of an electric vehicle charging infrastructure. The purpose is to establish an electric vehicle charging platform, giving electric vehicle users more autonomy [102, 105]. As we can see from the PoW-based energy use cases, scalability and transaction settlement time are the two major considerations for accommodating more users. However, the incentive mechanisms in the project (used to promote users to contribute to and behave well in the project community) should also be considered equally as the aforementioned scalability and latency.

4.2 | PBFT-based

If a certain amount of signatures is collected from the network peers, a PBFT-based consensus mechanism can provide instant finality. However, the message overhead limits the scalability of the network; hence it is mostly applied in the consortium blockchain to deal with a limited number of participants. SunChain from France aims to build an energy management system to track, secure and certify energy exchanges on blockchain-based applications [106]. It uses consortium blockchain to eliminate the mining process and perform authentication between consumers and energy producers. The Dutch company TenneT and the German blockchain company Sonnen use residential battery to provide ancillary grid services [107]. It is implemented through Hyperledger, an open-source platform for enterprise-scale blockchain solutions [108], to provide information to the grid network operator regarding the current power availability and reservoir. TenneT is the first power grid operator to launch a blockchain project on the operator level, where the PBFT algorithm is suitable in an application with fewer stakeholders [109].

PONTON is dedicated to the whole energy market with blockchain technology [110]. PONTON works with energy trading companies and utilities to develop a P2P wholesale trading platform in the regional market's Tendermin platform. Moreover, it applies strategies to enable smart trading and provide additional energy services such as power load balancing [111]. The BFT-based blockchain project in BTL works with the largest utility company in Austria to trade energy on the blockchain platform, which approves a huge reduction in operation cost and improves the efficiency of the trading process [112]. The automation process executed by the blockchain contracts reduces the time in the wholesale

transaction, such as confirmation, authorization, audit, etc. [113]. Now, the projects mentioned here, that are based on the PBFT consensus mechanism, are working with large stakeholders where the number of participants is limited. Also, the identity of the network peers is known and visible to all participants, thus the system's security is ensured, whereas scalability is still the biggest drawback for PBFT-based consensus mechanism.

Ripple is an open-source payment PBT-based agreement on the Internet to achieve decentralized currency exchange, payment and liquidation [14]. In the Ripple network, the transaction is made by the application and broadcast via tracking nodes or validating nodes. The consensus process of Ripple is run between validating nodes where each node has a pre-configured copy of the Unique Node List (UNL), and only the nodes from the UNL are capable of voting for the approved transactions. The validating nodes will store the approved transaction with 80% votes from UNL nodes to the local ledger, which is referred to as the last closed ledger [114]. In the Ripple consensus algorithm, the identities of the voting nodes from the UNL are known, so the transaction confirmation time is around several seconds, which is more efficient than permissionless consensus mechanisms such as PoW. Hence, the Ripple consensus mechanism is only suitable for permissioned blockchain applications [28]. And the BFT capability is $\frac{n-1}{5}$, which guarantees a secure consensus process withstanding 20% nodes performing Byzantine faults [115] (n denotes the number of nodes in the network).

4.3 | PoA-based

A PoA-based consensus mechanism highly relies on KYC techniques, since identity is the authentication proof and participants only trust authorized nodes. The use case of PoA is usually characterized by a high security-oriented scenario where it cannot put integrity and security at risk [58]. Grid Singularity is a highly active member of a blockchain organization promoting green energy generation and certification [101]. It aims to provide smart grid management solutions to improve power load balancing, automated transaction and audition, and grid network reliability. Grid singularity is also a member of the Energy Web Foundation (EWF), an open-source platform, and works with large corporations to launch and accelerate blockchain use cases in the energy sector [116]. EWF is an Ethereum-based platform that uses a PoA consensus algorithm to generate blocks, where the finality can be generated by 51% of the validators' signatures. Another blockchain company named Wirepas works with the EWF and serves as an IoT provider to connect the IoT devices to the blockchain platform [117].

StromDAO is a German company that has established an investment platform for renewable projects, through which consumers can invest directly [118]. It focusses on energy grid stakeholders at all levels and provides blockchain solutions that conform to the traditional grid structure. The British startup Green Running is currently developing a decentralized platform to make P2P energy trading possible [119]. It proposes a market model to serve as a broker between the energy producers and local aggregators, and customers can conduct energy transactions on the platform. Artificial intelligence is used to predict power consumption and electricity price and then help the P2P market price for its participants. PoA-based blockchain applications have a clear tendency for large-scale corporation use cases. However, the authority judgement exposes the centralized governing body, which is opposed to the decentralized idea behind blockchain technology.

4.4 | Others

SolarCoin is an open community project, which was registered as a public benefit corporation in the USA in 2014 [120]. SolarCoin uses a reward mechanism for solar energy producers. Energy producer use blockchain-based digital tokens as rewards to produce one SunCoin per million watt-hours of solar energy. This project aims to enable verifiably produced solar energy with SolarCoin issued cryptocurrency and reduce carbon emission globally [121]. It uses a free economic incentive to increase the production and consumption of solar energy, and rewards the production of solar energy through additional electricity stimulus. SolarCoin's blockchain uses PoS consensus mechanism on the public blockchain platform to verify blocks which are claimed to be more environmentally friendly. As opposed to Bitcoin, SolarCoin is granted for the proof of energy production from the solar installation, rather than the mining reward for contributing to computation power. And the PoS in the SolarCoin project is designed to use less than 0.001% of the power of bitcoin on a similar scale [122]. Another PoS-based project is called Energo Labs, which works on decentralized autonomous energy exchange [123]. It utilizes the Quantum blockchain, a decentralized application platform, to integrate smart metres and EV charging stations, thus reducing energy waste compared to PoW [39].

Bouygues Immobilier & Stratumn developed a blockchain project, which is used for the direct exchange of electricity between renewable energy producers and customers, where renewable energy is authenticated and verified through a blockchain platform [124]. The proof of the process is the consensus mechanism for the verification process of zero-knowledge proof. Due to the hierarchical order of trust to be executed in this process, an obvious centralized organization is exposed [125]. Another startup named Pylon Network developed a decentralized electricity trading platform for distributed energy resources and customers, using Pylon coins to reward green energy generation. The consensus mechanism is the Proof of Capacity, which is based on LiteCoin that supports a lower energy cost than the PoW with a larger throughput [126].

We can see that majority of the applications are still based on traditional consensus mechanisms. The most common distributed ledger platforms include Ethereum, Quantum, Corda and Hyperledger Fabric, which feature in different functionalities that can be applied in more diverse scenarios.

However, more and more applications are adopting or designing novel consensus mechanisms to accommodate their application requirements. In summary, a general comparison of the consensus mechanisms used by applications in the recent times is shown in Table 4.

5 | SECURITY THREATS AND CHALLENGES

It is claimed that blockchain technology is capable of accelerating the smart grid transformation process for decentralized energy generation and trading [131]. The overall security of a smart grid in the context of a smart city covers multiple factors such as data, connectivity, physical hazards, etc., where a comprehensive security framework was proposed in [132]. As for the process of energy decentralization and digitalization, the main challenge is to explore the most suitable control paradigm and distributed technologies. In this subsection, it explores the challenges imposed by the aforementioned projects and use cases.

According to the interoperability standard of smart grids proposed by the National Institute of Standards and Technology (NIST) [133], a conceptual model of smart grids is shown in Figure 3. It is noticeable that the market domain and the operation domain have the highest interoperability, as these two domains can be connected to all the other six domains in Figure 3. Therefore, the security threats in the market domain may affect the normal operation of the smart grids and vice versa. When the stakeholders plan to build up the blockchain-enabled electricity trading market in the smart grids, they should consider the security threats in both the blockchain-enabled markets and the entire smart grids.

Hence, our analysis of the blockchain-enabled smart grids' security threats is twofold in this section. The first part shows the common security threats in smart grids. Then, the security threats in consensus mechanisms, EVM and smart contracts are analysed in the second part. Finally, in the last part of this section, we present the lessons learnt from our analysis as well as some suggestions for future blockchain-enabled smart grid security enhancements.

5.1 | Smart grids

Current smart grids are usually controlled and operated using ICT. Therefore, security is still one of the most important considerations to protect the devices, communications and services in smart grids. Next, we conclude eight prevalent security threats from [134–139] in smart grids.

5.1.1 | Central controller compromise

The central controller (the operations domain in Figure 3) usually has the most sound security safeguard in a smart grid since it is the brain that controls all the facilities and devices of the whole smart grid to provide varied services to the users. However, social engineering attacks can invade the central controller and make it vulnerable. Social engineering attacks

TABLE 4 Consensus mechanisms in energy projects

Company/project	Consensus mechanism	Platform
Bankymoon [101]	PoW	Ethereum
PowerLedger [102]	PoW	Ethereum
Alliander & Spectral Energy [104]	PoW, Round Robin-based	MultiChain
Divvi [103]	PoW	Ethereum
Everty [105]	PoW	Ethereum
SunChain [106]	PBFT	Hyperledger fabric
TenneT & Sonnen [107]	PBFT	Hyperledger fabric
PONTON [110]	PBFT	Tendermin
BTL [112]	BFT-based	Interbit
Wirepas [117]	PoA	Ethereum-based
StromDAO [118]	PoA	Fury Network [127]
GridSingularity [101]	PoA	Ethereum-based
GreenRunning [119]	PoA	Ethereum-based
Bouygues Immobilier & Stratumn [124]	Proof of Process [125]	Proprietary [128]
Pylon Network [129]	Proof of Capacity [126]	LiteCoin [130]
SolarCoin [120]	PoS	LiteCoin-based
Energo Labs [123]	PoS	Qtum [39]

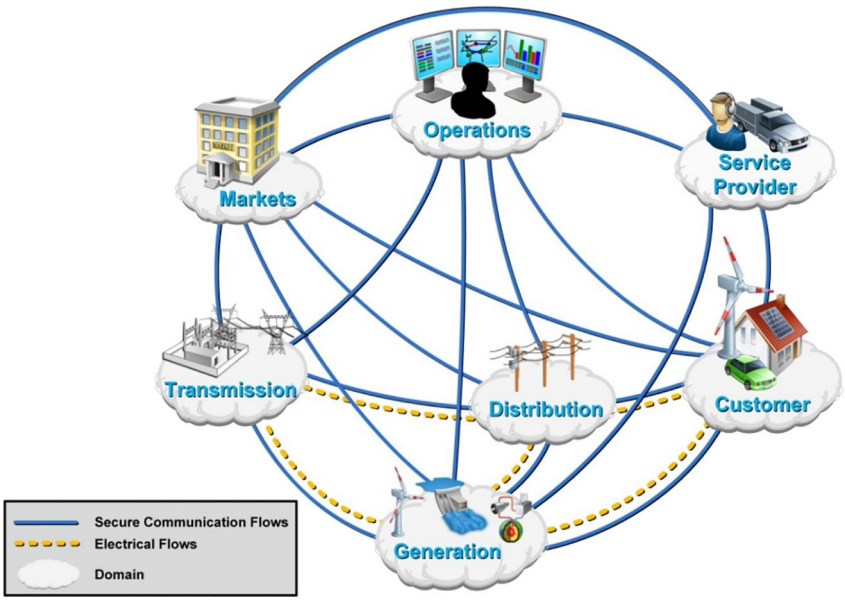

FIGURE 3 A conceptual model of smart grids defined in the smart grid standard of NIST [133]

can help an attacker obtain access to the central controller from certain nodes with weak security settings or from the staff. For instance, the central computers of the power grid in the United States and Ukrain were invaded and malwares were implanted by external attackers using social engineering attacks [140, 141]. These malwares can allow attackers to manipulate the servers, databases, billing systems and so on, resulting in severe corruption and privacy leakage.

5.1.2 | Intermediation compromise

In smart grids, all the communication between different devices needs to pass through multiple intermediate nodes (multi-hop communications), for example, a user uploads the bills to the central controller via several collector nodes. Meanwhile, some service facilities (e.g. charging piles) should use router nodes to communicate with their controllers. If the intermediate nodes are compromised in a smart grid, plenty of sensitive information can be leaked, including control commands, event and device identifiers, users' power consumption (usage) and so on, which will infringe user privacy and even support other potential attacks indirectly. For example, users' behaviours and life patterns can be analysed from their power usage [142]. Malicious code can be injected into metres through modified software update by attackers [143]. In addition, legal identifiers can be utilized to forge authorized devices or even credentials but smart grid networks cannot discover them.

Another example is a weak backhaul network. Backhaul network is an IP-based intermediate component for data (e.g. bills and bidding price) aggregation and collection. In a backhaul network, misconfigurations may lead to weak authentication. Furthermore, IP packets can be easily eavesdropped and even tampered, since packet encryption is not mandatory in the configuration. Therefore, the attacker can use methods like sniffing, replaying, spoofing and tampering to gather sensitive information and interfere users' actions [136]. For example, the attacker can modify the packet destination to make the user send bills to him/her. On the other hand, the attacker can change the packet sequence to delay the user's bidding [144, 145]. It is clear that a weak backhaul network may lead to fatal service failure, financial loss and cause harm to users' privacy.

5.1.3 | Intrusion by unknown nodes

This attack means that an attacker can implant several nodes (e.g. forwarding nodes) in the multi-hop network where the smart grid is constructed. If the multi-hop network lacks access authentication, these unknown nodes can be invisible and utilized to perform the following three kinds of man-in-the-middle (MITM) attacks:

- Packet analysis: The attacker can use the implanted nodes to intercept the transported data and perform an attack similar to the compromise analysis of the multi-hop network.
- Service disorder: The attacker can block the connections between nodes or publish fake commands (to ending nodes) to disrupt the normal services in the smart grid.
- Operational failure: The attacker intercepts electronic infrastructure commands and then deliberately sends (tampered) incorrect commands to these infrastructures to trigger their fault alarms and even shut them down [146]. Such threats may lead to severe damage to the smart grid's availability.

Compared with the threat of intermediation compromise, this threat is much more practical (lower cost) and concealed, and if there is no well-structured authentication strategy in the smart grid, the attacker does not need to attack the nodes.

5.1.4 | Denial of Service

Denial of Service (DoS) threat means that the attacker can exploit vulnerabilities in different network layers to generate a tremendous number of fake connections in a short period of time, thereby reducing the operating performance of the entire smart grid. DoS can be further categorized as follows:

- Processor or memory exhaust: The attacker can utilize buffer overflow or malicious resource-exhausted applications to crash the device's operating system, thus causing a DoS in the device [147].
- Ending device compromise: If certain legal ending devices are compromised, the attacker can exploit these devices to repeatedly send useless packets (e.g. fake control signals) to other nodes (like zombie network) in the smart grid, thus realizing flooding attacks. This kind of DoS can decrease communication performance and drain the devices' energy in the smart grid [146].
- Forwarding and routing compromise: This attack is kind of a further exploitation of the intermediation compromise. When an attacker controls some forwarding nodes, he/she can continuously forward the same packets to degrade the data transmitting capability of the smart grid or clogg packet confirmation through a large number of trash packets, causing the data transmission to lose synchronization. For example, if the attacker manipulates certain routing nodes, he/she can find a non-existent address by broadcasting an address lookup message, thus crashing the routing service and clogging the network [148]. On the other hand, if the trusted third party that the smart grid relies on is attacked, it may cause a DoS in the smart grid since certain essential security functions such as key distribution, identity validation, etc. can be clogged. It implies that reliance on a fully trusted third party in a smart grid environment reduces the robustness of the smart grid and increases the maintenance cost [149].

5.1.5 | Weak credential

Weak credential is a threat not only to the smart grid but also to most of the information systems. In smart grids, weak credentials involve not only fake or weak credentials and weak passwords but also vulnerable authentications (e.g. unsafe PPTP VPN links), lose authorization policies and so on that can be used to enter devices and facility systems. Weak credentials enable the attacker to learn the network structure, collect information, find the vulnerabilities of different nodes, and plan the attack targets in the smart grid when they are compromised. For example, in the attack on the Ukrainian power grids, the perpetrators broke the weak VPN credentials to access the industrial control system and then remotely shut down the partial power plants via human machine interface [141].

5.1.6 | Eavesdropping

Eavesdropping is the most common threat to an individuals' privacy and the system security in smart grids. As discussed in *Intermediation compromise* and *Intrusion by unknown nodes*, the attacker can intercept communication channels to gather power usage, household power load, peak time period, geolocation and other personal sensitive information, and analyse users' daily routine and behaviours [150]. On the other hand, eavesdropping is an effective approach for an attacker to obtain useful information from the target smart grid. Moreover, the attacker can exploit the information to learn about the smart grid, and find potential vulnerabilities to organize targeted and perilous attacks.

5.1.7 | Privacy analysis

When we consider privacy leakage and analysis, one type of privacy analysis is conducted by the external attacker, which is what we discussed in the intermediation compromise. However, there is another potential threat of privacy analysis from the internal nodes. Even though a user's power usage and bills are aggregated with certain privacy-preserving aggregation schemes before they are transmitted to the power supplier (central controller), the aggregation nodes can still reveal the user's private data to the power supplier and other stakeholders such as electric companies [151] because these aggregation nodes are essentially managed by the central controller [143]. For example, a user's private data can be utilized for repair, maintenance, price adjustment or even precise advertisement, but the user actually knows nothing.

5.2 | Blockchain

Since blockchain and different consensus mechanisms were proposed, the security discussions about blockchain and consensus mechanisms have never stopped. Meanwhile, more and more consensus mechanisms are being implemented based on Ethereum; thus the security of EVM is being considered to ensure that consensus mechanisms and smart contracts can be executed correctly. Furthermore, as the carrier of trade strategy and the applied consensus mechanism, a smart contract has security vulnerabilities that may lead to transaction chaos or even real-world economic loss (manipulated by attackers).

5.2.1 | Consensus mechanism

Collusion attack

The collision attack is the most common method which can be used by attackers to attack different consensus mechanisms. To be specific, if the attacker has more than 50% of the computing power in the PoW-based context, the attacker can manipulate all the results of the consensus requests, thereby causing fatal problems to the PoW network (e.g. selfish mining, cancelled

transactions and double-spending) [152]. On the other hand, if the attacker can control over 50% of the validation nodes selected by the consensus leader, the collusion attack may occur in the PBFT-related context. Compared with the PoW-based context, the PBFT-based context can be more easily affected by the collusion attack because the quantity of the used validation nodes defined by different consensus mechanisms that process each consensus request is much less than 50% of all the nodes in the PBFT-based context. The simulation result is shown in Figure 4, which is consistent with this view as the consensus mechanisms PBFT and Ripple cannot reach 100% consensus accuracy in handling a different number of concurrent transactions. Note that we utilize OPNET to conduct our simulations based on the idea and source code from [153]. The number of the consensus nodes for validation increases from 2000 to 18,000 with a step of 4000. In the PoW (ePoB) network and the PBFT (Ripple) network, the proportion of the unfaithful nodes is $\frac{1}{3}$ and $\frac{1}{5}$, respectively. Meanwhile, incorrect concurrent transactions are generated randomly during the simulation.

Sybil attack

Sybil attack means that one attacker claims a large number of fake identities (nodes) and then attempts to influence the voting result of the consensus mechanism in the consensus network. If the identity authentication is not robust enough, the Sybil attack will be widespread in peer-to-peer networks. For the PoW consensus mechanism operating in the anonymous network, the method used to ensure whether each node is valid involves checking whether the node owns a considerable amount of computing power. Meanwhile, PoW consensus mechanism provides miners with an incentive to work honestly but not to work in a way that will help avoid a Sybil attack. However, if enough fake nodes are selected in the validator group, the PBFT-related consensus mechanism may be affected by a Sybil attack, resulting in a higher probability.

Eclipse attack

In an eclipse attack, the attacker monopolizes all incoming and outgoing connections of the victim, thus isolating the victim from the rest of his or her peers in the network [154]. To be specific, a node depends on n number of nodes selected by the peer selection strategy to view its distributed ledger in a decentralized network. However, if an attacker can force this victim node to choose all the n number of nodes from the malicious nodes manipulated by him, the attacker can eclipse the original ledger of the victim node and replace the original ledger with a tampered ledger. Figure 5 shows an example of the eclipse attack, where the victim node cannot send/receive correct ledgers to the decentralized network since the victim can only choose the malicious nodes as peers. Compared with a Sybil attack that affects the entire blockchain network, an eclipse attack only attacks certain nodes more precisely, so the attack cost of an eclipse attack is much lower. It indicates that an eclipse attack is much easier to be performed in real-world blockchain-enabled systems [155]. In order to detect an eclipse attack, Xu et al. [156] proposed to utilize random forest classification algorithms to separate the attack data packets in terms of certain packet features (e.g. packet size, access frequency, access time and so on). Furthermore, two major countermeasures are proposed to mitigate an eclipse attack. The first countermeasure is partial randomness, giving priority to the old nodes with fresh outgoing connections in the peer selection. The other countermeasure is to establish some known and verified nodes' outgoing connections to test the neighbour nodes before they are selected as peers [154].

5.2.2 | EVM

EVM is a transaction-based state machine that runs on a 256-bit stack to execute all the functions in a smart contract and then implements the consensus mechanism [48]. Compared with the VMs used for general computation like Java Virtual Machine (JVM), Dalvik and ART in Android, the complexity of EVM is relatively low as it only needs to execute smart contracts deterministically and supports certain cryptographic primitives [157]. Nevertheless, security is still a primary concern in EVM since it is the last barrier to prevent malicious smart contracts and flaw consensus mechanisms. On the other hand, Ethereum is the most mainstream platform (or framework) serving numerous cryptocurrency and non-cryptocurrency applications. If EVM itself has severe vulnerabilities, attackers may endanger all Ethereum-based platforms to cause irreversible financial loss. Meanwhile, there are four versions of EVM that are used base on different programming languages: py-evm (Python), js-evm (JavaScript), geth (Golang) and aleth (C++). This diversity increases the potential attack range for attackers and the workload of security analysis for security researchers. In the current research, the major methods for discovering EVM vulnerabilities are symbolic execution and fuzzing [158], and the explored vulnerabilities in EVM are mainly related to memory management (e.g. stack overflow and illegal memory access) and opcode [48, 159].

Apart from detecting vulnerabilities in EVM, some researchers try to reinforce EVM via bytecode verification and semantics analysis [44, 50, 160, 161]. The target of these two methods is to eliminate unsafe bytecodes generated in different smart contracts. Since EVM is now continuously maintained and updated, new vulnerabilities in EVM may threaten all consensus mechanisms and smart contracts implemented on Ethereum. Therefore, the blockchain community should pay close attention to EVM security. In addition, many other studies are discussing the use of cryptographic methods (e.g. zero-knowledge proof, ring signature and multi-party computation) to design more secure consensus mechanisms running in EVM [51, 162].

5.2.3 | Smart contracts

A smart contract is an entity to carry the implemented consensus mechanism and transaction strategy. Therefore, the security of consensus mechanism is tightly linked to the

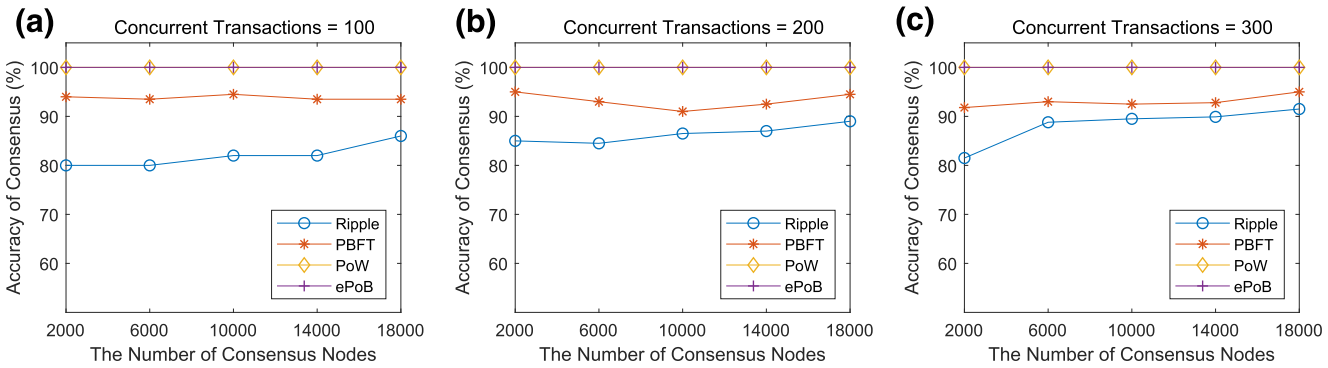

FIGURE 4 The accuracy comparison of different consensus mechanisms under collusion attacks

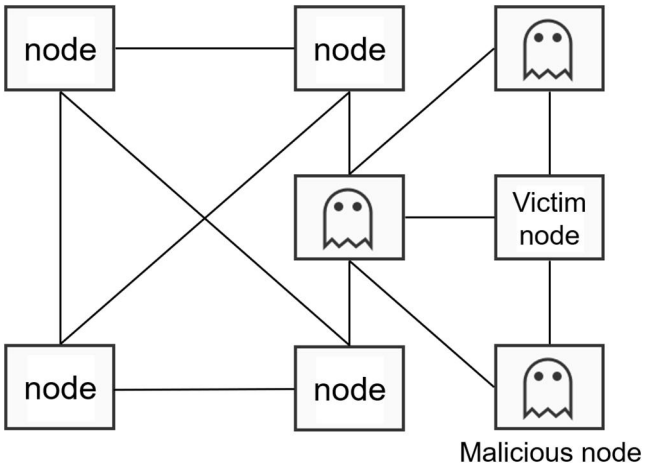

FIGURE 5 An example of the eclipse attack

security of smart contracts. In order to explore the potential vulnerabilities in smart contracts, several projects have proposed the construction of fuzzing tools based on heuristic search, symbolic execution, control flow graph and data stream analysis [46, 163–166]. The common vulnerabilities found in thousands of real-world smart contracts are summarized as follows.

Leaking and suicidal

A smart contract is considered to have a leak vulnerability if it leaks ether to attackers. Similarly, a smart contract is considered suicidal if it can be killed by attackers [167]. Both of these vulnerabilities are caused by inappropriate permission settings (especially in some smart contract tests), which allow attackers to invoke *send()* or *selfdestruct()* functions without any restrictions.

Block status dependency

If the transaction of sending ether (or other critical operations) relies on certain block status variables (e.g. timestamp, difficulty, gas limit and so on), the smart contract can be vulnerable since an attacker can construct transactions to achieve malicious behaviours by analysing the block status. Timestamp dependency is an example. Every block has a timestamp in the blockchain to record the time of the transaction. When the trigger conditions of some critical operations in a smart contract depend on timestamps, the timestamp can be exploited as a vulnerability. If an attacker can manipulate the timestamps (e.g. change the local system time), the timestamp-dependent smart contracts may be vulnerable.

Exception disorder

The reason for exception disorder is the inconsistency during exception handling. When a smart contract A tries to invoke a function f in another smart contract B, the function call may fail and generate different exceptions. Normally, all the transactions will be reverted in terms of the chain of nested calls for $f \in B$. However, if there is at least one low-level function call (e.g. *address.call()* and *address.send()*) in the chain, the transaction rollback will be terminated at the last low-level function call. Therefore, the rest of the transactions cannot be reverted, and the exceptions cannot be propagated to the caller A.

Re-entrancy

In general, the status of the contract's account can be changed after the invocation of some re-entrant functions in a smart contract is completed. However, many functions in smart contracts are not designed to be re-entrant functions. Therefore, if a malicious smart contract invokes these functions in a re-entrant manner repeatedly, it may lead to ether theft. The famous 'DAO' attack takes advantage of the re-entrancy vulnerability through the fallback function *withdraw()* to steal about 60 million USD [168].

Gasless send

When the sender tries to send ether >0 to the recipient, the fallback function in the recipient smart contract will be invoked with a fixed gas stipend (2300) determined by the EVM. However, if the gas consumption of the fallback function is designed to be higher than the current gas balance of the sender in the recipient contract, the sender will receive the exception 'out of gas'. Therefore, if the exception 'out of gas' is not handled and broadcast appropriately, a malicious sender can send ether to the recipient without costing gas.

Frozen ether (locking)

Some smart contracts are designed to invoke the functions of other smart contracts to operate ether via *delegatecall()*. It means that these smart contracts entirely depend on the related functions of other smart contracts to manipulate ether, as there is no actual ether manipulating function in these smart contracts. When the smart contracts that provide ether manipulating functions execute self-destructive (suicide) operation, the smart contracts with only delegated calls cannot send the ether to others, so that all the ether is frozen. In November 2017, a frozen ether bug resulted in the Parity Wallet users to permanently lose an estimated $150 million in funds [169].

Dangerous delegatecall

The *delegatecall* opcode is designed for a caller smart contract to invoke other library contracts. Specifically, the caller contract can load the library contract's code and execute it in the context of the caller contract. Since the parameter of *delegatecall* is the address of a library contract, an attacker can execute an arbitrary code in the caller contract by manipulating the parameter (i.e. the library contract's address) of *delegatecall*. This vulnerability has been exploited to result in $30 million loss in a multi-signature wallet.[1]

5.3 | Lessons learnt

- Improving the administration of staff and facilities is an important step to enhance the security of the smart grid. There should be widespread awareness of information security and it should be learnt by every staff working for smart grids because these staff are the actual operators of all the facilities in a smart grid. If the staff are compromised by social engineering or activate certain malicious applications unconsciously, any smart grid can be broken easily, even if they are flawless. On the other hand, the physical access control of the facilities and the firmware security of the electronic devices should also be considered carefully. This is because some attackers may barge into some smart grid facilities to implant malicious devices for eavesdropping, jamming, data collection and so on. Meanwhile, the vulnerabilities in the electronic devices' firmware can be exploited by some attackers to interfere the running of these devices or execute other attacks, thereby destroying the entire smart grid.
- Pragmatic testbeds should be built for a study to evaluate different security approaches with unified standards. Table 5 presents diverse countermeasures to address the threats discussed in the smart grids (Section 5.1). It is noticeable that each kind of solution has its own security goals and features. However, they have a common drawback: lack of practical evaluation. Because smart grids are critical and valuable fundamental infrastructures, it is unrealistic to test new security countermeasures (including solutions, schemes, etc.) in real smart grids. Such tests (or evaluations) may incur fatal errors, causing the smart grid to be in an unstable state (even out of service). Therefore, a realistic testbed is a wise choice, which is jointly constructed and used by researchers and stakeholders.
- Code security should be strongly concerned in all blockchain-related systems. Apart from studying the security of consensus mechanisms and smart contract, researchers and software engineers should also study code security because vulnerable codes can be utilized by attackers, resulting in financial loss (e.g. DAO attack). More validating and simulating tools should be developed to test the codes in different smart contracts and can be applied to different test techniques for software security (e.g. fault injection, fuzzing, symbolic execution, sandbox, static analysis, etc). As a result, more and more severe vulnerabilities in smart contracts can be avoided before such smart contracts are released to the public.

In a nutshell, when discussing the security of consensus mechanism, we should not only consider the threats to consensus mechanisms themselves but also the threats to both the carrier (smart contract) and the running environment (EVM). In the smart grid sector and many other non-cryptocurrency sectors, there are no standards (or any best practice) to guide companies to deploy secure blockchain-based systems. Even in the cryptocurrency area, the related standards and standard operation procedures (SOPs) are still unclear (in developing). Otherwise, there would not be this many cases of cryptocurrencies being stolen on different cryptocurrency trading platforms [200]. In our view, in non-cryptocurrency areas, building up security standards (e.g., PKI) and normalizing code writing (smart contracts) for blockchain-based applications should be considered as the top priority.

6 | CONCLUSIONS AND FUTURE WORKS

Here, we comprehensively study the consensus mechanism of blockchain technology applied in the energy sector. We first introduce the basic terms related to blockchain technology and its general applications. We pay special attention to the application of a blockchain-enabled system in the energy sector, where the overall structure and principals are presented. Next, state-of-the-art consensus mechanisms are reviewed and the corresponding use cases are presented. We can see the obvious trend of the consensus protocol design in the blockchain system, where the use case with a large number of participants chooses a consensus mechanism with high scalability, such as PoW. Moreover, the use cases that use stricter user access prefer PBFT or PoA because the user's identity is easy to be checked. The choice of consensus mechanism relies on the trade-off between transaction cost and throughput, scalability and latency, privacy and decentralization, energy waste and security. A security analysis demonstrates that collusion attack and sybil attack can influence the consensus accuracy of

[1] https://blog.openzeppelin.com/on-the-parity-wallet-multisig-hack-405a8c12e8f7/

TABLE 5 Countermeasures to the discussed threats in smart grids

Threat	Countermeasure	Description
Central controller compromise	Probabilistic distribution: [170]	Pros: This early warning system can detect DoS attacks in the network stream before the stream arrives at the central controller. Therefore, this method allows the central controller of the smart grid to react to DoS attacks in advance.
		Cons: The study only considers DoS attacks; only simulations.
	Black list: [171]	Pros: Black and white list to monitor all log-in actions.
		Cons: Only framework, no concrete algorithm or solution.
Intermediation compromise	Authentication: [145, 172, 173]	Pros: Authenticate devices with methods of public key cryptography; good scalability for multicast network; resistance of different attacks (e.g. man-in-the-middle and DoS).
		Cons: Significant message delay; high communication cost; no practical test in smart grids.
	Encrypted aggregation: [174, 175]	Pros: Homomorphic encryption to provide confidentiality and integrity for transmitted data.
		Cons: Very high computational cost; feasibility and scalability are not tested.
Intrusion by unknown nodes	Improved route protocol: [176, 177]	Pros: Scalable and efficient; resilient multicast; safeguard to spoofing, DoS and many others attacks.
		Cons: Communication overhead is not validated; lack of detailed security analysis and test in real smart grids.
	Authentication: [177, 178]	Pros: Direct and efficient approach to prevent unknown nodes; confidentiality and integrity of data packets; identification management.
		Cons: Lack of real use cases to evaluate actual security of these schemes.
	Neural network: [179]	Pros: The statistical method is quite efficient after completed training; intrusion prediction and detection.
		Cons: Training is time-consuming for real use; no real application to evaluate the actual false positive rate (FPR).
DoS	Routing strategy: [180, 181]	Pros: Dynamic routing; neighbour supervision; malicious routing detection.
		Cons: Larger packet size; delay of establishing connections; lack of evaluation on testbeds.
	Transport layer security: [182–184]	Pros: Secure communication channels; confidentiality and integrity of data; resist replay attack and tampering simultaneously.
		Cons: High cost for deploying such protocols; high time consumption for establishing secure channels; lack of security test in real systems.
	Dynamic status control: [185, 186]	Pros: High-efficient optimization methods; reduce the magnitude and duration of service disruption caused by DoS; earlier DoS prediction; enhanced stability and resiliency of smart grids.
		Cons: High grid fluctuation; high communication overhead in central controllers; FPR should be considered in real use cases.
Weak credential	Authentication with encryption: [187–189]	Pros: Hybrid security methods are secure against tampering and forgery; identity validation; data confidentiality.
		Cons: Incremental cost for computation and communication in smart grids; weak security analysis; lack of practical evaluations.
Eavesdropping	Encryption: [190–192]	Pros: Data confidentiality; tampering detection; friendly data aggregation.
		Cons: Homomorphic encryption for data aggregation is not practical as it is quite time-costing in computation; DoS and replay attack is not fully considered; performance and security analysis are not conducted on testbeds (or in real use).
	Access control: [193–196]	Pros: Data integrity; identity management; protect against eavesdropping, DoS attack, manipulation, replay attack, etc.; can be combined with encryption methods to form holistic security solution.
		Cons: High computational complexity and communication cost; lack of concrete security analysis or privacy policies; practical performance is not examined.

(Continues)

TABLE 5 (Continued)

Threat	Countermeasure	Description
Privacy analysis	Trust computing: [197–199]	Pros: protect data in all data processing and transmitting phases; secure multi-party computation; prevent privacy leakage, and side channel and man-in-the-middle attacks. Cons: Complicated configuration; slow system initialization; cannot safeguard to DoS attack; no practical test.

different consensus mechanisms, especially the consensus accuracy of Ripple. On the other hand, the numerous vulnerabilities due to man-made faults in the blockchain environment can lead to vulnerable consensus mechanisms.

This work focusses on a deeper understanding of the consensus mechanism in the energy sector to boost the development of smart grid management systems. However, the current consensus mechanism might not be able to fully implement all the requirements from its use case. A customized consensus mechanism should be designed to better adapt to more complicated and efficient energy grid operations in the future. And the customized consensus mechanism can be deployed and tested on the platform with a governance structure by giving special permissions. For blockchain-based platforms in smart grids, the development of security standards and the normalization of the smart contract's code should be given priority. Besides, the security of the system relies on secure data transmission and management, which can improve data encryption in the network layer and the authentication mechanisms for user identity validation. Combining with user identification and access priorities will further improve system security and flexibility.

ORCID

Chao Liu https://orcid.org/0000-0001-6473-2292

REFERENCES

1. Adye, K., Pearre, N., Swan, L.: Contrasting distributed and centralized photovoltaic system performance using regionally distributed pyranometers. Solar Energy. 160(15), 1–9 (2018)
2. Jing, Q., Venkatram, A.: The relative impacts of distributed and centralized generation of electricity on local air quality in the south coast air basin of California. Energy Policy. 39(9), 4999–5007 (2011)
3. Maher, G., Anan, M.: Smart grid opportunities and challenges of integrating renewable sources: a survey. In: Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International, pp. 1098–1105. IEEE (2014)
4. Fadaeenejad, M., et al.: The present and future of smart power grid in developing countries. Renew. Sustain. Energy Rev. 29, 828–834 (2014)
5. Bahga, A., Madisetti, V.K.: Blockchain platform for industrial internet of things. J. Softw. Eng. Appl. 09(10), 533–546 (2016)
6. Vukolić, M.: The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: Open Problems in Network Security, pp. 112–125. Springer International Publishing, Cham (2016)
7. Marzband, M., et al.: Smart transactive energy framework in grid-connected multiple home microgrids under independent and coalition operations. Renew. Energy. 126, 95–106 (2018)
8. Kakran, S., Chanana, S.: Smart operations of smart grids integrated with distributed generation: a review. Renew. Sustain. Energy Rev. 81, 524–535 (2018)
9. Agung, A.A.G., Handayani, R.: Blockchain for smart grid. J. King Saud Univ. Comput. Info. Sci. 01.002, 1–10 (2020)
10. Musleh, A.S, Yao, G., Muyeen, S.M.: Blockchain applications in smart grid – review and frameworks. IEEE Access. 7, 86746–86757 (2019)
11. Sayeed, S., Marco-Gisbert, H., Caira, T.: Smart contract: attacks and protections. IEEE Access. 8, 24416–24427 (2020)
12. Mollah, M.B., et al.: Blockchain for future smart grid: a comprehensive survey. IEEE Internet Things J. 8(1), 18–43 (2020)
13. Kiayias, A., et al.: Blockchain mining games. In: Proceedings of the 2016 ACM Conference on Economics and Computation, pp. 365–382. ACM (2016)
14. Zheng, Z., et al.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. 14(4), 352–375 (2018)
15. Sukhwani, H., et al.: Performance modelling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). In: 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), pp. 253–255. IEEE (2017)
16. Woos, D., et al.: Planning for change in a formal verification of the RAFT consensus protocol. In: Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs, pp. 154–165. ACM (2016)
17. Abraham, I., Malkhi, D.: The blockchain consensus layer and BFT. Bull. EATCS. 3(123) (2017)
18. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
19. Yli-Huumo, J., et al.: Where is current research on blockchain technology?—a systematic review. PloS One. 11(10), e0163477 (2016)
20. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Fut. Gener. Comput. Syst. 82, 395–411 (2018)
21. Beck, R., et al.: Blockchain technology in business and information systems research. Bus. Inf. Syst. Eng. 59(6), 381–384 (2017)
22. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc. (2015)
23. Matzutt, R., et al.: A quantitative analysis of the impact of arbitrary blockchain content on Bitcoin. In: Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer (2018)
24. Tian, F.: An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: 2016 13th International Conference on Service Systems and Service Management (ICSSSM), pp. 1–6. IEEE (2016)
25. Aste, T., Tasca, P., Di Matteo, T.: Blockchain technologies: The foreseeable impact on society and industry. Computer. 50(9), 18–28 (2017)
26. Böhme, R., et al.: Bitcoin: economics, technology, and governance. J. Econ. Perspect. 29(2), 213–238 (2015)
27. Gramoli, V.: From blockchain consensus back to byzantine consensus. Fut. Gener. Comput. Syst. 107, 760–769 (2017)
28. Pilkington, M.: 11 blockchain technology: principles and applications. Research Handbook on Digital Transformations, pp. 225-253. Elgar-Online (2016). https://www.elgaronline.com/view/edcoll/9781784717759/9781784717759.00019.xml
29. Jaag, C., Bach, C.: Blockchain technology and cryptocurrencies: opportunities for postal financial services. In: The Changing Postal and Delivery Sector, pp. 205–221. Springer (2017)
30. Iansiti, M., Lakhani, K.R.: The truth about blockchain. Harv. Bus. Rev. 95(1), 118–127 (2017)

31. Ouaddah, A., Abou El Kalam, A., Ouahman, A.A.: Harnessing the power of blockchain technology to solve IoT security & privacy issues. In: ICC, pp. 7–1. (2017)
32. Liu, B., et al.: Blockchain based data integrity service framework for IoT data. In: 2017 IEEE International Conference on Web Services (ICWS), pp. 468–475. IEEE (2017)
33. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. 5(2), 1184–1195 (2018)
34. Zamyatin, A., et al.: A wild velvet fork appears! Inclusive blockchain protocol changes in practice. In: International Conference on Financial Cryptography and Data Security, pp. 31–42. Springer (2018)
35. Truby, J.: Decarbonizing bitcoin: law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies. Energy Res. Soc. Sci. 44, 399–410 (2018)
36. Zheng, Z., et al.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. IEEE (2017)
37. Delgado-Segura, S., et al.: Analysis of the bitcoin UTXO set. In: International Conference on Financial Cryptography and Data Security, pp. 78–91. Springer (2018)
38. Guy, Z., et al.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops, pp. 180–184. IEEE (2015)
39. Kiktenko, E.O., et al.: Quantum-secured blockchain. Quantum Sci. Technol. 3(3), 035004 (2018)
40. Karame, G.: On the security and scalability of bitcoin's blockchain. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1861–1862. ACM (2016)
41. Hari, A., Lakshman, T.V.: The internet blockchain: a distributed, tamper-resistant transaction framework for the internet. In: Proceedings of the 15th ACM Workshop on Hot Topics in Networks, pp. 204–210. ACM (2016)
42. Dannen, C.: Introducing Ethereum and Solidity. Springer (2017)
43. Grishchenko, I., Maffei, M., Schneidewind, C.: A semantic framework for the security analysis of ethereum smart contracts. In: International Conference on Principles of Security and Trust, pp. 243–269. Springer (2018)
44. Hildenbrandt, E., et al.: Kevm: A complete semantics of the Ethereum Virtual Machine, Technical Report 2142/97207 (2017)
45. Wohrer, M., Uwe, Z.: Smart contracts: security patterns in the ethereum ecosystem and solidity. In: 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pp. 2–8. IEEE (2018)
46. Luu, L., et al.: Making smart contracts smarter. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS 16, pp. 254–269. ACM, New York (2016)
47. Wood, G., et al.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 151(2014), 1–32 (2014)
48. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (sok). In: International Conference on Principles of Security and Trust, pp. 164–186. Springer (2017)
49. Bartoletti, M., et al.: Dissecting Ponzi schemes on ethereum: identification, analysis, and impact arXiv preprint arXiv:1703.03779 (2017)
50. Hirai, Y.: Defining the ethereum virtual machine for interactive theorem provers. In: International Conference on Financial Cryptography and Data Security, pp. 520–535. Springer (2017)
51. Aitzhan, N.Z., Svetinovic, D.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secure Comput. 15(5), 840–852 (2016)
52. Zeng, Q., et al.: Storage optimization algorithm for publication blockchain. In: International Conference on Computer Engineering and Networks, pp. 828–835. Springer (2018)
53. Faccia, A., Mosteanu, N.R.: Accounting and blockchain technology: from double-entry to triple-entry. Bus. Manag. Rev. 10(2), 108–116 (2019)
54. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access. 4, 2292–2303 (2016)
55. Lamport, L.: Time, clocks, and the ordering of events in a distributed system. Commun. ACM. 21(7), 558–565 (1978)
56. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. 5(9), 1–10 (2016)
57. Du, M., et al.: A review on consensus algorithm of blockchain. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 2567–2572. IEEE (2017)
58. Baliga, A.: Understanding Blockchain Consensus Models. Persistent (2017)
59. Benčić, F.M., Žarko, I.P.: Distributed ledger technology: blockchain compared to directed acyclic graph. In: IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 1569–1570. IEEE (2018)
60. Li, J., et al.: Energy consumption of cryptocurrency mining: a study of electricity consumption in mining cryptocurrencies. Energy. 168, 160–168 (2019)
61. Adam, B.: Hashcash – A Denial of Service Counter-Measure. (2002)
62. Cachin, C., Vukolić, M.: Blockchains consensus protocols in the wild. arXiv preprint arXiv:1707.01873 (2017)
63. Vukolić, M.: The quest for scalable blockchain fabric: proof-of-work vs. Bft replication. In: International Workshop on Open Problems in Network Security, pp. 112–125. Springer (2015)
64. Wang, W., et al.: A survey on consensus mechanisms and mining management in blockchain networks, 1–33 arXiv preprint arXiv:1805.02707 (2018)
65. Rosenfeld, M.: Analysis of hashrate-based double spending arXiv preprint arXiv:1402.2009 (2014)
66. Castro, M., et al.: Practical byzantine fault tolerance. In: OSDI, vol. 99, pp. 173–186. (1999)
67. Milutinovic, M., et al.: Proof of luck: an efficient blockchain consensus protocol. In: Proceedings of the 1st Workshop on System Software for Trusted Execution, vol. 2. ACM (2016)
68. King, S., Scott, N.: Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. (2018)
69. De Angelis, S., et al.: Pbft vs Proof-Of-Authority: Applying the Cap Theorem to Permissioned Blockchain (2018)
70. Dinh, T.T.A., et al.: Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. 30(7), 1366–1385 (2018)
71. Lou, C.: What is blockchain? J. Account. 224(1), 29 (2017)
72. Imbault, F., et al.: The green blockchain: managing decentralized energy production and consumption. In: 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), pp. 1–5. IEEE (2017)
73. Liu, C., et al.: Blockchain based energy trading model for electric vehicle charging schemes. In: Seet, B.-C., Chai, M. (eds.) Smart Grid and Innovative Frontiers in Telecommunications, pp. 64–72. Springer International Publishing, Cham (2018)
74. Oh, S.C., et al.: Assessment of energy demand response options in smart grid utilizing the stochastic programming approach. In: 2011 IEEE Power and Energy Society General Meeting, pp. 1–5. (July 2011)
75. Patterson, B.T., Geary, D.E.: Real-time transactional power management in a microgrid mesh network: The enernet. IEEE Int. Telecommun. Energy Conf. 1–7 (2016)
76. Wilson, C., et al.: Common Types of Local Energy System Projects in the UK (2020)
77. Fell, M.J., et al.: Post-Pandemic Recovery: How Smart Local Energy Systems Can Contribute (2020)
78. Nguyen, G.-T., Kim, K.: A survey about consensus algorithms used in blockchain. J. Infor. Proc. Syst. 14(1) (2018)
79. Chen, L., et al.: On security analysis of proof-of-elapsed-time (poet). In: International Symposium on Stabilization, Safety, and Security of Distributed Systems, pp. 282–297. Springer (2017)
80. Liu, C., et al.: Proof-of-benefit: a blockchain-enabled ev charging scheme. In: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), pp. 1–6. (2019)
81. Liu, C., et al.: Peer-to-peer electricity trading system: smart contracts based proof-of-benefit consensus protocol. Wirel. Netw. 1, 1–12 (2019)

82. Chacko, J.A., Mayer, R., Jacobsen, H.-A.: Why do my blockchain transactions fail? A study of hyperledger fabric (extended version) arXiv preprint arXiv:2103.04681 (2021)
83. Pop, C., et al.: Blockchain based decentralized management of demand response programs in smart energy grids. Sensors. 18(1), 162 (2018)
84. Mannaro, K., Pinna, A., Marchesi, M.: Crypto-trading: blockchain-oriented energy market. In: 2017 AEIT International Annual Conference, pp. 1–5. IEEE (2017)
85. Zhang, Y., et al.: Distributed electrical energy systems: needs, concepts, approaches and vision. Acta Autom. Sin. 43(NREL/JA-5D00-70646) (2017)
86. Zhang, C., et al.: Review of existing peer-to-peer energy trading projects. Energy Procedia. 105, 2563–2568 (2017)
87. Mengelkamp, E., et al.: Designing microgrid energy markets: a case study: The brooklyn microgrid. Appl Energy, 870–880 210(2018)
88. Chitchyan, R., Jordan, M.: Review of blockchain technology and its expectations: Case of the energy sector arXiv preprint arXiv:1803.03567 (2018)
89. Dispenza, J., Garcia, C., Ryan, M.: Energy Efficiency Coin (EECoin): A Blockchain Asset Class Pegged to Renewable Energy Markets. (2017) https://www.enledger.io/Energy_Efficiency_Coin_Whitepaper_v1_0.pdf Accessed 1 June 2017 [Online]
90. Dong, Z., Luo, F., Liang, G.: Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. J. Mod. Power Syst. Clean Energy. 6(5), 958–967 (2018)
91. Noor, S., et al.: Energy demand side management within micro-grid networks enhanced by blockchain. Applied energy. 228, 1385–1398 (2018)
92. Xue, T., Sun, H., Guo, Q.: Electricity transactions and congestion management based on blockchain in energy internet. Power Syst. Technol. 40, 3630–3638 (2016)
93. Mihaylov, M., et al.: Nrg-x-change a novel mechanism for trading of renewable energy in smart grids. 101–106 (2014)
94. Mengelkamp, E., et al.: A blockchain-based smart grid: towards sustainable local energy markets. Comput. Sci. Res. Dev. 33(1), 207–214 (2017)
95. Zhang, Y., Wen, J.: The IoT electric business model: using blockchain technology for the internet of things. Peer-to-Peer Netw. Appl. 10(4), 983–994 (2017)
96. Horta, J., et al.: Novel market approach for locally balancing renewable energy production and flexible demand. (2017). arXiv preprint arXiv:1711.09565
97. Münsing, E., Mather, J., Moura, S.: Blockchains for decentralized optimization of energy resources in microgrid networks. In: 2017 IEEE Conference on Control Technology and Applications (CCTA), pp. 2164–2171. (2017)
98. Ilic, D., et al.: An energy market for trading electricity in smart grid neighbourhoods. In: 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 1–6. (2012)
99. Andoni, M., et al.: Blockchain technology in the energy sector: a systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 100, 143–174 (2019)
100. Watanabe, H., et al.: Blockchain contract: a complete consensus using blockchain. In: 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), pp. 577–578. IEEE (2015)
101. Goranović, A., et al.: Blockchain applications in microgrids: an overview of current projects and concepts. In: IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, pp. 6153–6158. IEEE (2017)
102. Carson, B., et al.: Blockchain Beyond the Hype: What Is the Strategic Business Value. McKinsey & Company (2018)
103. Divvi Energy. https://divvi.xyz/ Accessed 13 August 2019 [Online]
104. Alliander Spectral Enegy. http://blockchain.alliander.com/map/ Accessed 12 August 2019 [Online]
105. Everty EV Charging Station. https://everty.com.au/ Accessed 13 August 2019 [Online]
106. Stephant, M., et al.: A survey on energy management and blockchain for collective self-consumption. In: 2018 7th International Conference on Systems and Control (ICSC), pp. 237–243. IEEE (2018)
107. Jonas, S., Ammon, L., German, R.: Ethome: open-source blockchain based energy community controller. In: Proceedings of the Ninth International Conference on Future Energy Systems, pp. 319–323. ACM (2018)
108. Cachin, C.: Architecture of the hyperledger blockchain fabric. Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310, p. 4. (2016)
109. Albrecht, S., et al.: Dynamics of blockchain implementation-a case study from the energy sector. In: Proceedings of the 51st Hawaii International Conference on System Sciences (2018)
110. Lee, T., et al.: Automation of the supplier role in the GB power system using blockchain-based smart contracts. CIRED Open Access Proc. J. 2017(1), 2619–2623 (2017)
111. Fu, B., Shu, Z., Liu, X.: Blockchain enhanced emission trading framework in fashion apparel manufacturing industry. Sustainability. 10(4), 1105 (2018)
112. Karajovic, M., Kim, H.M., Laskowski, M.: Thinking outside the block: projected phases of blockchain integration in the accounting industry. Aust. Account Rev. 29(2), 319–330 (2019)
113. Kamboj, D., Yang, T.: An exploratory analysis of blockchain: applications, security, and related issues. In: Proceedings of the International Conference on Scientific Computing (CSC), pp. 67–73. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) (2018)
114. Moreno-Sanchez, P., et al.: Listening to whispers of ripple: linking wallets and deanonymizing transactions in the ripple network. Proc. Privacy Enhancing Technol. 2016(4), 436–453 (2016)
115. Bach, L.M., Mihaljevic, B., Zagar, M.: Comparative analysis of blockchain consensus algorithms. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1545–1550. IEEE (2018)
116. Livingston, D., et al.: Applying block chain technology to electric power systems, Technical Report, Discussion Paper. Council on Foreign Relations (2018)
117. Wirepas Mesh – IoT network. https://wirepas.com/ Accessed 17 August 2019 [Online]
118. Stromdao, Hybridstrom von Stromdao. https://stromdao.de/de Accessed 17 August 2019 [Online]
119. Green, R.: Energy trading. https://www.greenrunning.com/about-us/ Accessed 17 August 2019 [Online]
120. SolarCoin Official Website. https://solarcoin.org/ Accessed 10 August 2019 [Online]
121. Gogerty, N., Johnson, P.: Network Capital: Value of Currency Protocols Bitcoin & SolarCoin Cases in Context. SSRN (2018)
122. Wang, N., et al.: When energy trading meets blockchain in electrical power system: The state of the art. Appl. Sci. 9(8), 1561 (2019)
123. Energo Labs: Decentralized autonomous energy system. https://www.energolabs.com/static/env1.1.3.4062bc1d.pdf Accessed 17 August 2019 [Online]
124. Hampikian, Z.: Positive energy and networks: local energy autonomy as a vector for controlling flows. Local Energy Auton. Spaces Scales Politics. 1, 141–161 (2019)
125. Lemieux, V.L.: Trusting records: is blockchain technology the answer? Record Manag. J. 26(2), 110–139 (2016)
126. Yang, Z., et al.: A blockchain-based reputation system for data credibility assessment in vehicular networks. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5. IEEE. (2017)
127. Utz, M., et al.: Blockchain-based management of shared energy assets using a smart contract ecosystem. In: International Conference on Business Information Systems, pp. 217–222. Springer (2018)
128. Rennock, M.J.W, Cohn, A., Butcher, J.R.: Blockchain technology. Journal. 1(7) (2018)
129. Pylon Network PylonCoin. https://pylon-network.org/ Accessed 15 August 2019 [Online]
130. Martin, H., Diaz, J.M.Q.: Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of bitcoin, litecoin and

namecoin. In: International Workshop on Enterprise Applications and Services in the Finance Industry, pp. 106–120. Springer (2014)
131. James, B., Cottrell, M.: How utilities are using blockchain to modernize the grid. Harv. Bus. Rev. 23 (2017)
132. Toh, C.K.: Security for smart cities. IET Smart Cities. 2(2), 95–104 (2020)
133. Greer, C., et al.: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, Technical Report (NIST SP)-1108r3. NIST, Gaithersburg (2014)
134. Khurana, H., et al.: Smart-grid security issues. IEEE Secur. Privacy Mag. 8(1), 81–85 (2010)
135. Lu, Z., et al.: Review and evaluation of security threats on the communication networks in the smart grid. In: 2010-Milcom 2010 Military Communications Conference, pp. 1830–1835. IEEE (2010)
136. Baig, Z.A., Amoudi, A.-R.: An analysis of smart grid attacks and countermeasures. J. Commun. 8(8), 473–479 (2013)
137. Kim, S.-K., Huh, J.-H.: A study on the improvement of smart grid security performance and blockchain smart grid perspective. Energies. 11(8), 1973 (2018)
138. Kumar, P., et al.: Smart grid metering networks: a survey on security, privacy and open research issues. IEEE Commun. Surv. Tutorials. 21(3), 2886–2927 (2019)
139. Komninos, N., Philippou, E., Pitsillides, A.: Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun. Surv. Tutorials. 16(4), 1933–1954 (2014)
140. Gorman, S.: Electricity Grid in U.S. Penetrated By Spies. https://www.wsj.com/articles/SB123914805204099085 Accessed 08 April 2009 [Online]
141. Defense Use Case: Analysis of the Cyberattack on the Ukrainian Power Grid, vol. 388. Electricity Information Sharing and Analysis Center (E-ISAC) (2016)
142. Hafez, O., Bhattacharya, K.: Queuing analysis based Pev load modelling considering battery charging behaviour and their impact on distribution system operation. IEEE Trans. Smart Grid. 9(1), 261–273 (2016)
143. Ali, M., Mohammed, O.A., Zonouzsaman, S.: Empirical development of a trusted sensing base for power system infrastructures. IEEE Trans. Smart Grid. 6(5), 2454–2463 (2015)
144. Mahmoud, M.M.E.A., et al.: Privacy-preserving power injection over a hybrid AMI/LTE smart grid network. IEEE Internet Things J. 4(4), 870–880 (2016)
145. Kim, Y., Kolesnikov, V., Thottan, M.: Resilient end-to-end message protection for cyber-physical system communications. IEEE Trans. Smart Grid. 9(4), 2478–2487 (2016)
146. Yi, P., et al.: Puppet attack: a denial of service attack in advanced metering infrastructure network. J. Netw. Comput. Appl. 59, 325–332 (2016)
147. Abbasinezhad-Mood, D., Ostad-Sharif, A., Nikooghadam, M.: Design of an anonymous lightweight communication protocol for smart grid and its implementation on 8-bit AVR and 32-bit arm. Int. J. Netw. Secur. 21(4), 607–617 (2019)
148. Lin, J., et al.: On false data injection attacks against distributed energy routing in smart grid. In: 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, pp. 183–192. IEEE (2012)
149. Wang, X., Liu, Y., Choo, K.R.: Fault tolerant, ULTI-subset aggregation scheme for smart grid. IEEE Trans. Ind. Infor. (2020)
150. Werner, S., Lundén, J.: Smart load tracking and reporting for real-time metering in electric power grids. IEEE Trans. Smart Grid. 7(3), 1723–1731 (2015)
151. Paverd, A., Martin, A., Brown, I.: Security and privacy in smart grid demand response systems. In: International Workshop on Smart Grid Security, pp. 1–15. Springer (2014)
152. He, Y., et al.: A blockchain based truthful incentive mechanism for distributed P2P applications. IEEE Access. 6, 27324–27335 (2018)
153. Gervais, A., et al.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 3–16. (2016)
154. Heilman, E., et al.: Eclipse attacks on bitcoin's peer-to-peer network. In: 24th {USENIX} Security Symposium ({USENIX}Security 15), pp. 129–144. (2015)
155. Zhang, S., Lee, J.-H.: Eclipse-based stake-bleeding attacks in PoS blockchain systems. In: Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, pp. 67–72. (2019)
156. Xu, G., et al.: Am I eclipsed? A smart detector of eclipse attacks for ethereum. Comput. Secur. 88, 101604 (2020)
157. Tikhomirov, S., et al.: Smartcheck: static analysis of ethereum smart contracts. In: 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), pp. 9–16. IEEE (2018)
158. He, J., et al.: Learning to fuzz from symbolic execution with application to smart contracts. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 531–548. (2019)
159. Fu, Y., et al.: EvmFuzzer: detect EVM vulnerabilities via fuzz testing. In: Proceedings of the 2019 27th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, pp. 1110–1114. ACM (2019)
160. Park, D., et al.: A formal verification tool for ethereum VM bytecode. In: Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, pp. 912–915. ACM (2018)
161. Ma, F., et al.: EVM*: from offline detection to online reinforcement for ethereum virtual machine. In: 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER), pp. 554–558. IEEE (2019)
162. Ali, D., et al.: A secure private blockchain-based solution for distributed energy trading. IEEE Commun. Mag. 57(7), 120–126 (2019)
163. Jiang, B., Liu, Y., Chan, W.K.: ContractFuzzer: fuzzing smart contracts for vulnerability detection. In: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, pp. 259–269. ACM (2018)
164. Kalra, S., et al.: Zeus: analyzing safety of smart contracts. NDSS (2018)
165. Liu, C., et al.: ReGuard: finding reentrancy bugs in smart contracts. In: Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings, pp. 65–68. ACM (2018)
166. Di Angelo, M., Salzer, G.: A survey of tools for analyzing ethereum smart contracts. In: 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). IEEE (2019)
167. Nikolić, I., et al.: Finding the greedy, prodigal, and suicidal contracts at scale. In: Proceedings of the 34th Annual Computer Security Applications Conference, pp. 653–663. (2018)
168. Zhao, X., et al.: The dao attack paradoxes in propositional logic. In: 2017 4th International Conference on Systems and Informatics (ICSAI), pp. 1743–1746. IEEE (2017)
169. Parity Technologies: Security Alert. https://www.parity.io/security-alert-2/ Accessed 08 November 2017 [Online]
170. Fadlullah, Z., et al.: An early warning system against malicious activities for smart grid communications. IEEE Netw. 25(5), 50–55 (2011)
171. Khan, R., et al.: Threat analysis of blackEnergy malware for synchrophasor based real-time control and monitoring in smart grid. In: 4th International Symposium for ICS & SCADA Cyber Security Research, vol. 4, pp. 53–63. (2016)
172. He, D., Chan, S., Guizani, M.: Cyber security analysis and protection of wireless sensor networks for smart grid monitoring. IEEE Wirel. Commun. 24(6), 98–103 (2017)
173. Hussain, S., et al.: A lightweight and formally secure certificate based signcryption with proxy re-encryption (cbsre) for internet of things enabled smart grid. IEEE Access. 8, 93230–93248 (2020)
174. Guo, C., et al.: Lightweight privacy preserving data aggregation with batch verification for smart grid. Fut. Gener. Comput. Syst. (2020)
175. Kamil, I.A., Ogundoyin, S.O.: Lightweight privacy-preserving power injection and communication over vehicular networks and 5G smart grid slice with provable security. Internet Things. 8, 100–116 (2019)
176. Jin, W., Kundur, D.: Goalie: goal-seeking obstacle and collision evasion for resilient multicast routing in smart grid. IEEE Trans. Smart Grid. 7(2), 567–579 (2015)
177. Taylor, C., Johnson, T.: Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid

networks. In: 2015 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1835–1840. IEEE (2015)
178. Wan, M., et al.: SRDA: a secure routing and data aggregation approach for wireless smart metre. J. Commun. 11(1) (2016)
179. Haghnegahdar, L., Wang, Y.: A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection. Neural Comput. Appl. 32(13), 9427–9441 (2020)
180. Hu, B., Gharavi, H.: Smart grid mesh network security using dynamic key distribution with Merkle tree 4-way handshaking. IEEE Trans. Smart Grid. 5(2), 550–558 (2013)
181. Lee, G., Kim, Y.-S., Kang, J.: An adaptive dos attack mitigation measure for field networks in smart grids. In: International Conference on Broadband and Wireless Computing, Communication and Applications, pp. 419–428. Springer (2016)
182. Hoefling, M., et al.: jOSEF: a Java-based open-source smart metre gateway experimentation framework. In: DA-CH Conference on Energy Informatics, pp. 165–176. Springer (2015)
183. Khaled, O., et al.: Analysis of secure TCP/IP profile in 61850 based substation automation system for smart grids. Int. J. Distrib. Sens. Netw. 12(4), 5793183 (2016)
184. Afianti, F., Wirawan, T., Suryani, T.: Lightweight and dos resistant multiuser authentication in wireless sensor networks for smart grid environments. IEEE Access. 7, 67107–67122 (2019)
185. Wang, Z., Wang, J.: A novel finite-time control scheme for enhancing smart grid frequency stability and resilience. IEEE Trans. Smart Grid. 10(6), 6538–6551 (2019)
186. Hasnat, M.A., Rahnamay-Naeini, M.: A data-driven dynamic state estimation for smart grids under DoS attack using state correlations. In: 2019 North American Power Symposium (NAPS), pp. 1–6. IEEE (2019)
187. Kumar, N., et al.: ECCAuth: a secure authentication protocol for demand response management in a smart grid system. IEEE Trans. Ind. Inf. 15(12), 6572–6582 (2019)
188. Hasan, M.M., Hussein, T.M.: Cloud-centric collaborative security service placement for advanced metering infrastructures. IEEE Trans. Smart Grid. 10(2), 1339–1348 (2017)
189. Garg, S., et al.: Secure and lightweight authentication scheme for smart metering infrastructure in smart grid. IEEE Trans. Ind. Inf. 16(5), 3548–3557 (2019)
190. Guan, Z., et al.: Effect: an efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid. Sci. China Inf. Sci. 62(3), 32103 (2019)
191. Ahene, E., et al.: Efficient signcryption with proxy re-encryption and its application in smart grid. IEEE Internet Things J. 6(6), 9722–9737 (2019)
192. Ding, Y., et al.: Secure metering data aggregation with batch verification in industrial smart grid. IEEE Trans. Ind. Inf. 16(10), 6607–6616 (2020)
193. Gope, P.: Pmake: privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid. Comput. Commun. 152, 338–344 (2020)
194. Mahmood, K., et al.: An enhanced anonymous identity-based key agreement protocol for smart grid advanced metering infrastructure. Int. J. Commun. Syst. 32(16), e4137 (2019)
195. Odelu, V., et al.: Provably secure authenticated key agreement scheme for smart grid. IEEE Trans. Smart Grid. 9(3), 1900–1910 (2016)
196. Saxena, N., Choi, B.J., Lu, R.: Authentication and authorization scheme for various user roles and devices in smart grid. IEEE Trans. Inf. Forensics Secur. 11(5), 907–921 (2015)
197. Jia, Z., et al.: Privacy protection scheme based on remote anonymous attestation for trusted smart metres. IEEE Trans. Smart Grid. 9(4), 3313–3320 (2016)
198. Velusamy, D., Pugalendhi, G., Ramasamy, K.: A cross-layer trust evaluation protocol for secured routing in communication network of smart grid. IEEE J. Sel. Area Commun. 38(1), 193–204 (2019)
199. Li, H., et al.: Trust-enhanced content delivery in blockchain-based information-centric networking. IEEE Netw. 33(5), 183–189 (2019)
200. Wikipedia: Cryptocurrency and Security. https://en.wikipedia.org/wiki/Cryptocurrency_and_security Accessed 17 September 2019 [Online]

How to cite this article: Liu C, Zhang X, Chai KK, Loo J, Chen Y. A survey on blockchain-enabled smart grids: Advances, applications and challenges. *IET Smart Cities*. 2021;3:56–78. https://doi.org/10.1049/smc2.12010