Challenges of Blockchain in New Generation Energy Systems and Future Outlooks[★]

Tonghe Wang[a,1], Haochen Hua[b,2], Zhiqian Wei[c,3] and Junwei Cao[a,*,4]

[a]*Tsinghua University, Beijing, 100084, P.R. China*
[b]*Hohai University, Nanjing, Jiangsu, 211100, P.R. China*
[c]*Shandong University, Qingdao, Shandong, 266237, P.R. China*

ARTICLE INFO

Keywords:
blockchain
consensus
energy blockchain
energy internet
energy system

ABSTRACT

Recently, the blockchain technology has attracted widespread attention due to its advantageous features, e.g., decentralization, transparency, traceability, and immutability. To make full use of renewable energy resources, new generation energy systems advocate the deep integration of information technology in real-world energy projects, among which blockchain has become one of the most used technologies. However, with the continuous development of related studies and projects, blockchain has begun to expose more and more limitations. As a result, the application of energy blockchain, i.e., blockchain applied in energy systems, is facing various challenges caused by these limitations. This paper briefly reviews popular application scenarios of energy blockchain, analyzes generic limitations of blockchain and their impacts on energy systems, and summarizes several possible solutions to these limitations. As far as we know, this paper is one of the few works that deeply analyze the shortcomings of the blockchain technology and corresponding solutions in the energy field.

1. Introduction

Blockchain has been recognized as one of the most promising technologies since the advent of Bitcoin in 2008 [1]. As shown in Figure 1, a blockchain encapsulates data into blocks, and these blocks form a linked list in the order specified by a distributed **consensus** mechanism. The chain structure and the decentralized nature grant blockchain transparency, traceability, reliability, and immutability [2], which explains the widespread application of blockchain in various fields. In peer-to-peer (P2P) transactions, using blockchain can reduce transaction cost by getting rid of centralized trusted intermediaries [3, 4]. The traceability, transparency, and immutability makes blockchain very popular in commidity tracing [5, 6]. Blockchain can also establish trust and provide data security for cloud/edge computing [7], supply chains [8], and health care systems [9].

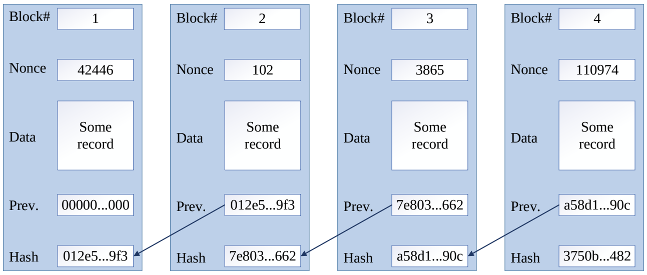


Figure 1: The chain structure of a blockchain [10]. Each block stores the hash value of its previous block, forming a chain structure.

With the proposal of "Blockchain 2.0" in 2014, the development of the blockchain technology embraces a new climax [11]. Compared with Blockchain 1.0, Blockchain 2.0 integrates smart contracts, a kind of programmable scripts that execute automatically when predefined conditions are met [12]. As a result, the application scope of blockchain has been further extended to automatic transaction settlement [13], system access control [14], content copyright protection [15], and many other services.

In the energy field, the full utilization of renewable energy resources for power generation has always been a hot topic. The deep integration of energy technology and information and communication technology (ICT) has become an inevitable trend of new generation energy systems since the concept of *Energy Internet* was brought about [16, 17]. As one of the most popular ICTs at the moment, blockchain is playing an important role in the revolution of modern energy systems. The blockchain applied in energy systems is also called **energy blockchain** [18]. In P2P energy trading scenarios where untrusted entities are involved, energy blockchain can guarantee trading transparency and privacy in the absence of trusted intermediaries [19, 20]. In electric vehicle (EV) charging systems, blockchain can provide secure energy exchange and efficient demand response [21, 22]. With the help of smart contracts, energy blockchain enable automation, decentralization, and flexibility in the control and management of energy systems [23, 24, 25].

However, as the number of practical blockchain-based projects increases, the limitations of blockchain have become

[★] This work is supported by National Key Research and Development Program of China (Grant No. 2017YFE0132100) and BNRist Program under Grant No. BNR2020TD01009.

[*] Corresponding author

tonghewang@tsinghua.edu.cn (T. Wang); huahc16@tsinghua.org.cn (H. Hua); wzqlen@163.com (Z. Wei); jcao@tsinghua.edu.cn (J. Cao)

http://www.mit.edu/~caoj/ (J. Cao)

ORCID(s): 0000-0002-8430-9755 (T. Wang); 0000-0002-3341-2947 (H. Hua); 0000-0003-3533-3756 (J. Cao)

[1] This author is with Department of Automation, Tsinghua University, Beijing, 100084, P.R. China.

[2] This author is with College of Energy and Electrical Engineering, Hohai University, Nanjing, Jiangsu, 211100, P.R. China.

[3] This author is with School of Cyberscience and Technology, Shandong University, Qingdao, Shandong, 266237, P.R. China.

[4] This author is with Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing, 100084, P.R. China.

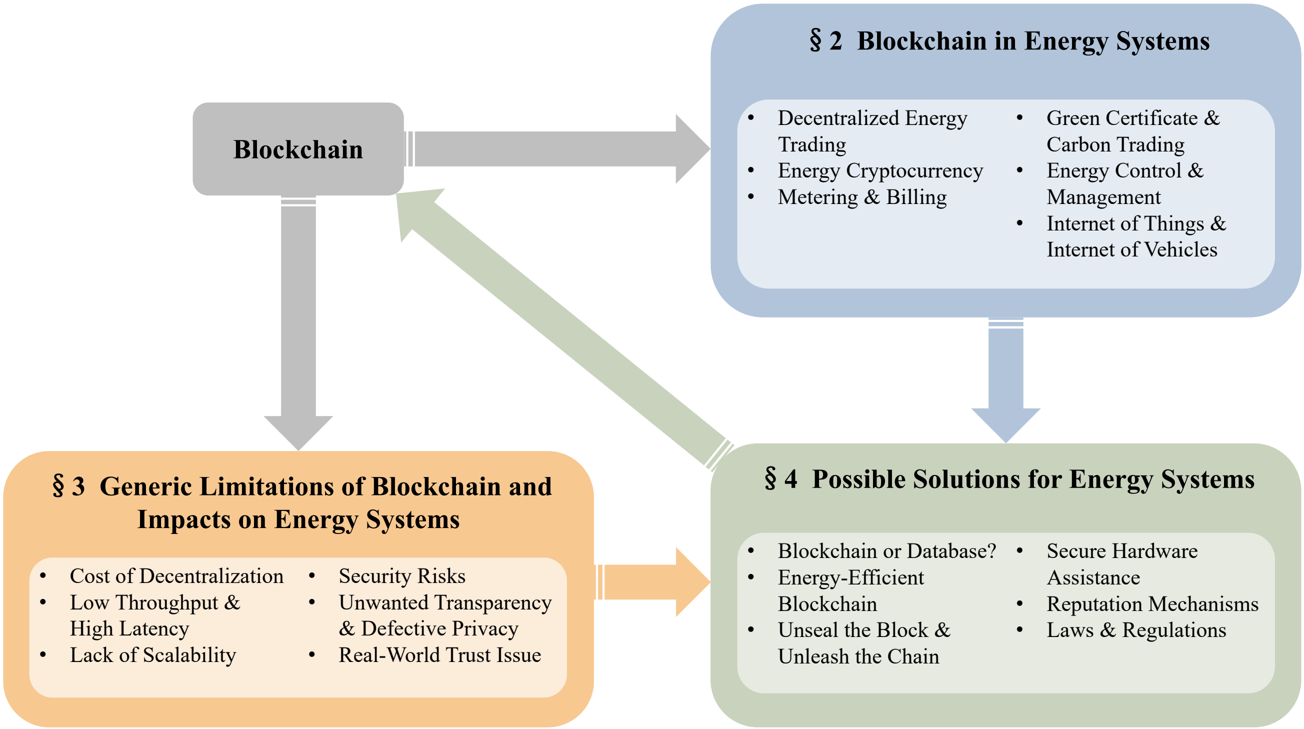

§ 2 Blockchain in Energy Systems
Decentralized Energy Trading
Energy Cryptocurrency
Metering & Billing
Green Certificate & Carbon Trading
Energy Control & Management
Internet of Things & Internet of Vehicles
Blockchain
§ 3 Generic Limitations of Blockchain and Impacts on Energy Systems
Cost of Decentralization
Low Throughput & High Latency
Lack of Scalability
Security Risks
Unwanted Transparency & Defective Privacy
Real-World Trust Issue
§ 4 Possible Solutions for Energy Systems
Blockchain or Database?
Energy-Efficient Blockchain
Unseal the Block & Unleash the Chain
Secure Hardware Assistance
Reputation Mechanisms
Laws & Regulations

Figure 2: The organization of this paper.

more acute. On the one hand, the blockchain technology is not a new technology, but a fusion of a variety of ICTs including P2P transmission, cryptography, distributed consensus, and smart contract. These technologies themselves may suffer from a series of generic issues (e.g., high power and storage costs, low throughput and high latency, and the lack of scalability [26, 27]), and combining them in a blockchain system does not mitigate these issues. On the other hand, due to the importance and particularity of energy industry, practical energy systems usually have high requirements for trustworthiness, security, and privacy [28, 29]. Unfortunately, these requirements are often compromised for decentralization, the most emphasized feature of blockchain [30]. This could make blockchain-based energy projects deviate from their expected results [31].

Existing works on energy blockchain tend to focus more on presenting the advantages of blockchain, but few of them fully evaluates the disadvantages. This paper will instead look deep into the limitations of the blockchain technology within the scope of the energy field. In more details, our contributions in this paper are as follows:

- We formally argue that the blockchain is not a panacea for energy systems. Blockchain's component technologies have their own generic issues and using blockchain could sometimes contradict the practical requirements of energy systems.
- We specially and systematically analyze the limitations of blockchain, and we also explore their potential impacts on energy systems.
- We summarize possible solutions for energy systems to deal with these impacts.

To the best of our knowledge, we are the first to make the above achievements.

The rest of this paper is organized as follows: Section 2 briefly reviews the applications of blockchain in energy systems; Section 3 analyzes the limitations of blockchain and their impacts on energy systems; Section 4 summarizes corresponding solutions for energy systems; Section 5 concludes this paper. A clear picture of the organization of this paper is provided in Figure 2.

2. Blockchain in Energy Systems

In this section, we will briefly introduce typical scenarios where energy blockchain is commonly applied. We will also explain the roles that blockchain palys in them. Table 1 enumerates some related works that use energy blockchain in different scenarios, and we will describe them one by one.

2.1. Decentralized Energy Trading

Decentralized energy trading is the most popular application of energy blockchain [20, 32, 34]. Traditional energy trading usually requires an intermediary utility provider in every transaction. When there exists direct physical power connections, prosumers (i.e., consumers with power generation devices such as photovoltaics or wind turbines) and consumers can perform P2P power trading without the need of a centralized provider (see Fig. 3). In more detail, prosumers and consumers communicate about transaction information

Scenario	Citation	Blockchain Choice	Goal of Using Blockchain
P2P energy trading	[32]	Hyperledger Fabric [33]	Provide transaction authetication and information transparency.
	[20]	Hyperledger Fabric	Establish trust; increase robustness against single point of failure.
	[34]	Ethereum [35]	Remove trusted third party; enhance data privacy.
Microgrid energy market	[36]	Ethereum	Remove intermediary; use smart contract to automate energy trading.
	[37]	Hyperledger Fabric	Implement a blockchain layer to protect data privacy; build trust in microgrid energy market.
Energy Cryptocurrency	[38]	Bitcoin	Avoid centralized failure in energy trading.
	[39]	Self-developed	Use smart contract to automate energy trading; serve as a payment currency.
	[40]	Self-developed	Reward for green production and sustainable use.
	[41]	Ethereum	Increase transparency and trust; attract investment in solar panels.
Metering & billing	[42]	Self-developed	Confirm metering data; achieve automatic billing; enable energy transaction through cryptocurrency.
	[43]	Self-developed	Provide immutability and reliability for metering services.
Green certificate	[44]	Corda [45]	Verify green certificate transactions.
	[46]	Self-developed	Authenticate green electricity generation and consumption data securely, transparently, and immutably.
Carbon trading	[47]	Ethereum & Hyperledger Fabric	Provide immutability, consistency, and transparency for database.
	[48]	Hyperledger Iroha [49]	Eliminate centralized entity in transactions.
	[50]	Ethereum & IPFS [51]	Use transparency to eliminate fraud; provide security for transaction and monitoring data.
Eenrgy control & management	[52]	Hyperledger Fabric	Verify all power management operations; provide transparency and immutability for the data.
	[53]	Ethereum	Implement automatic power flow optimization; ensure data security.
	[25]	Ethereum	Guarantee the privacy, security, and immutability of energy data; reach agreement on demand response events; increase the flexibility and reliability of demand response via smart contracts.
Internet of Things	[54]	Ethereum & Hyperledger Fabric	Verify transactions; confirm IoT device monitoring data; provide security for sharing economy service.
	[55]	Hyperledger Fabric	Guanrantee sensing data integrity; provide privacy and secutity for regulation.
Internet of Vehicles	[21]	Hyperledger Fabric	Enhance robustness against cyberattacks; ensure authentication, security, and privacy.
	[56]	Self-Developed	Provide traceability and authentication for EV electricity transactions; establish audit and transaction sharing in local aggregators without trusted third-party.

Table 1
Application scenarios of energy blockchain.

on a blockchain-based P2P platform run by the local community. Once transactions get approved, the corresponding amount of power will be transferred from prosumers to consumers through physical connections. This trading pattern has a prominent advantage that the local community has more flexibility in managing its own generation and utility demands [57].

In this scenario, blockchain helps to maintain a ledger by keeping a record of each transaction. Before stored into the ledger, each transaction record is authenticated by peers through distributed consensus. Data security of the ledger is guaranteed with cryptographic schemes of blockchain. The ledger is transparently shared by peers, making it easy to trace and difficult to tamper with any record. Moreover, au-

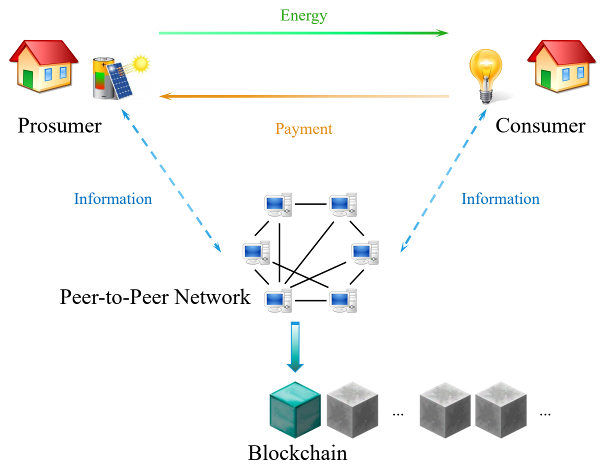


Figure 3: Peer-to-peer energy trading with a blockchain platform. Transactions are completed in a peer-to-peer network, with each peer implementing blockchain functions. All transactions authenticated by consensus will be recorded into the ledger maintained by all peers.

tomatic transactions can be accomplished once transaction rules are prescribed by peers in the form of smart contracts [58].

Decentralized energy trading can also take place between multiple microgrids operated by different groups. Unlike the local community setting, microgrids might not necessarily have direct physical connections. In this case, a microgrid energy market is needed to support the virtual community formed by participants [59]. Blockchain is also widely used to establish a trusted and secure microgrid energy market in the absence of a commonly trusted third-party [3, 36, 37].

2.2. Energy Cryptocurrency

Cryptocurrency is a form of digital asset that operates on the basis of blockchain technology, and it is the original purpose of inventing the blockchain technology. Without a centralized authority, P2P cryptocurrency transactions can eliminate additional transaction fees [60]. Thus, cryptocurrency is extremely popular in international trade since cryptocurrency is not affected by the exchange rate of any specific country [61]. The underlying blockchain technology also provides anonymity and privacy for transactions in cryptocurrency [62].

Energy cryptocurrency has been used as a means of payment in decentralized energy trading, either in Bitcoin or in self-developed cryptocurrency [38, 39]. Besides, energy cryptocurrency is more likely to play an incentive role in new generation energy systems. For one thing, producers can be rewarded for green energy production and consumers can be rewarded for sustainable use behavior with cryptocurrency [40]. For another, cryptocurrency is able to attract and encourage renewable energy investments (e.g., in solar panels) [41]. Therefore, energy cryptocurrency has both financial and social value.

2.3. Metering and Billing

Smart meters help users store, buy and, sell electrical energy. When blockchain is incorporated into smart meters, the electricity generated and consumed will be recorded into a distributed ledger. Any metering records in the ledger are authenticated, transparent, and traceable. The ledger can effectively ensure the integrity of metering data and billing record through its immutability, and it can also preserve the privacy of user identity through its anonymity [42, 43].

In practice, manual metering and billing often need additional management costs, and they may encounter mistakes or even frauds. With the support of smart contracts, metering and billing can also be automated. As a result, the administrative cost of metering and billing can be eliminated [63], and the probability of mistakes and frauds can also be reduced [64].

2.4. Green Certificate and Carbon Trading

Green certificates are a kind of products that authenticate the amount of renewable electricity generated by producers, and they can be traded between producers or between producers and customers [44]. In a green power pricing mechanism, green certificates can help producers avoid additional environmental protection and energy conservation expenditures [65]. The government will also grant subsidies to companies that produce green electricity based on their green certificates [66].

By integrating blockchain, extra expenses of issuing and auditing green certificates to central authorities can be eliminated [67]. Moreover, the transparency and immutability of blockchain can create a reliable setting for renewable energy power generation and transaction [46]. The automation provided by smart contracts also helps to avoid human mistakes or frauds during these processes [44].

On the other hand, carbon trading is an effective way to control carbon emissions. By imposing prices on carbon emission quotas or other carbon products, the financial expenditures caused by carbon emissions become more significant for businesses [68]. Large companies and institutions can purchase voluntary emission reduction targets to offset carbon emissions in daily operations and activities, and they can promote their corporate image and social responsibility in public at the same time [69].

There have been a lot of works that implement blockchain-based carbon trading systems [47, 48, 50]. Using energy blockchain in carbon trading can guarantee the integrity of emission monitoring data [47]. The decentralization of energy blockchain also encourages individuals and companies to participate in carbon trading and emission control [48]. In addition, like the trading of green certificates, carbon trading can also improve its reliability through the transparency and immutability provided by blockchain [70, 71].

2.5. Energy Control and Management

Control technology is an important basis for energy systems to maintain system stability and optimize energy management [72, 73]. It has been widely used to solve a variety of problems in energy scenarios, such as voltage control and frequency regulation [74, 75], reactive power optimization [76], active power sharing [77], social welfare maximization [78], demand response [79], and many other problems. With the wide deployment of a large number of devices in energy systems, control and management methods are implemented in more distributed ways [80]. Although distributed methods have higher flexibility, efficiency, scalability, and robustness against single point of failure, cybersecurity is always an urgent problem to be solved when private information is shared among multiple distributed agents [81].

Using blockchain as a secure database is a common practice in distributed energy control and management. Because of the tamper-proof nature of blockchain-based database, corresponding control operations become more reliable in the absence of centralized trust [25, 52]. In addition, autonomous energy management can be achieved by implementing controlling rules into smart contracts [53, 82].

2.6. Internet of Things and Internet of Vehicles

Internet of Things (IoT) is promoting the transformation of energy systems. With every device connected to the Internet, IoT technologies bring more intelligence and flexibility into new generation energy systems [83]. The development of IoT has spawned various research fields such as Internet of Vehicles (IoV), smart homes, smart cities, smart manufacturing and smart grids. Due to the involvement of massive heterogeneous smart devices, traditional IoTs face great challenges in data integrity, privacy, and reliability. Blockchain is a practical approach to solve these problems, providing decentralized, secure, and automatic system management [54, 55].

In particular, with the popularization of EVs, cybersecurity issues in the interaction between EVs and charging service providers have become more prominent [84]. Like P2P energy trading, trading that involves EVs can also use blockchain to establish secure transaction environment in terms of authentication, anonymity, and privacy in IoVs [21, 85]. Moreover, the smart contract technology can also serve as an incentive mechanism to encourage more EVs to participate in demand response [56].

3. Generic Limitations of Blockchain and Impacts on Energy Systems

In this section, we are going to systematically analyze the drawbacks of blockchain and their potential impacts on energy systems.

3.1. Cost of Decentralization

Decentralization is the most emphasized feature of blockchain in the energy field. Decentralization encourages every individual in the network, or node, to participate in the bookkeeping. In theory, this decentralization can mitigate the performance bottleneck caused by a centralized node, enhance robustness against single point of failure, and avoid intermediate transaction fees [86]. Unfortunately, many existing works neglect the energy and storage cost behind these benefits.

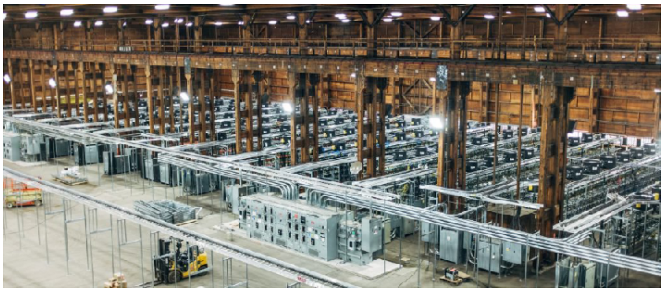


Figure 4: Some Bitcoin mining facility that uses a large number of energy-intensive processors for PoW mining [89].

3.1.1. Energy Cost

Bitcoin and Ethereum [35] are popular blockchain platforms in energy blockchain systems, and they both use Proof of Work (PoW) as their consensus mechanism. PoW requires nodes to solve computationally expensive hash puzzles. This process is called "mining" and nodes that participate in puzzle solving are called "miners" [87]. Then these miners will include answers in their blocks to prove their computational work. The first miner to provide a valid proof of work becomes the generator of the block.

The great burden of solving meaningless hash puzzles is regarded as a huge waste of resources [88]. Figure 4 shows a Bitcoin mining facility that uses hundreds of high energy-consumption processors for PoW mining [89]. It is estimated that Bitcoin's annual electricity consumption is between 60 and 150 TW·h. On average, the electricity required for each Bitcoin transaction is equivalent to the electricity consumption of a typical German household for weeks or months [90]. That is why Ethereum plans to launch Ethereum 2.0 [91] that will switch to Proof of Stake (PoS) consensus that comsumes monetary stakes instead of energy [92].

3.1.2. Storage Cost

Full decentralization requires redundant data storage, and each blockchain node needs to store a copy of the data. According to statistics, the volume of data stored on Bitcoin blockchain has reached 285.06 GB by June 2020 [93]. This means that in a system with 1,000 nodes, for instance, storing these blockchain data will consume up to 278.38 TB of storage in total. With the continuous expansion of blockchain networks and the increasing volume of blockchain data, this gigantic cost of storage resources will be a huge challenge for blockchain-based projects.

One possible way to solve the storage issue of decentralization is to deploy *lightweight nodes* that only store part of the blockchain data [94]. This breaks the (strong) consistency requirement of the consensus mechanism that all data should be synchronized within a limited time interval [95]. Since the information stored in lightweight nodes is incomplete, the completion of block verification relies on full nodes that store all blockchain information. This strategy reduces the pressure on data storage by consuming network resources, greatly enhancing the feasibility of blockchain-based projects. In return, involving lightweight nodes may nevertheless lead to vulnerabilities against many attacks, such as data availability attack [96], brute-force attacks [97], and Denial-of-Service attacks [98].

3.1.3. Impacts

In the energy field, PoW-based Ethereum is the most used blockchain platform among academic studies and real-world projects [57]. The huge energy consumption of PoW consensus will impose unexpected burden on these energy blockchain projects, which contradicts the goal of using energy blockchain to improve the efficiency of energy utilization. The storage cost of decentralization could bring a series of troubles to blockchain-based energy systems in practice. For one thing, energy blockchain might not be a good choice if system devices only have limited storage and computing resources (e.g., in IoT or IoV). For another, additional security measures are required if lightweight nodes are deployed to reduce redundant storage. As a result, system designers are recommended to carefully choose the degree of decentralization according to practical requirements of the system.

3.2. Low Throughput and High Latency

Researchers often compare the performance of Bitcoin with VISA, the largest centralized payment system in the world. Bitcoin has a latency of 10 minutes to complete a transaction and a throughput of 7 transactions per second [99]. It seems that Bitcoin fails to show its advantage against VISA that achieves a much higher throughput up to 30,000 transactions per second [100].

There are many factors that may lead to the low throughput and high latency of blockchain systems, and we will analyze these factors in detail.

3.2.1. Slow Mining for Consensus

The contention of concurrent requests is a main cause of the inconsistency of consensus results because executing these contended requests in different orders may lead to different views of the system in different nodes. As described in Section 3.1.1, solving hash puzzles in PoW mining is also very time-consuming. This trading of time and computation resources for consistency is necessary to limit the speed of block generation and reduce the probability of contention caused by simultaneous block submission.

Although PoS and classical Byzantine fault tolerant (BFT) consensus algorithms do not need mining and can obtain better performance, PoW-based consensus is still the mainstream in practical blockchain systems, especially in energy systems [57]. The reasons are as follows:

- In PoS, the block generator stores monetary stakes in each block it generates as a deposit, and these stakes will be confiscated if some block submitted by the generator is detected as invalid. This reduces the time and energy wasted in the mining process of PoW, but introducing monetary concept could cause new security risks (to be discussed in Section 3.4).
- BFT consensus aims to reach consensus via message exchange between nodes [101]. However, BFT algorithms usually have strong theoretical assumptions (e.g., reliable transmission links, fully connected communication network, and partial synchrony). Consensus instances may fail if these assumptions cannot be guaranteed [102].

Therefore, PoW-based blockchains with higher energy consumption but more reliable consensus are still favorable for system designers.

3.2.2. Low Query Speed

The low efficiency of blockchain is also reflected in the low speed of information query. As shown in [103], the processing time of a single transaction of Ethereum is about 80 to 2,000 times longer than that of MySQL. This is caused by the orderly chained data structure of blockchain. In order to query records, the system requires all nodes to traverse all records in the block chain to generate the final query result, which is rather time consuming [104]. As the blockchain size grows larger and larger, this search strategy will be much slower.

3.2.3. Limited Block Size

By filling client requests into blocks of a fixed size, blockchain can process multiple transactions in one batch. Although this parallelism helps to increase the throughput in theory, the fixed block size could be a big hurdle if the system scale increases. When the request submission speed exceeds the block generation speed, unprocessed requests have to queue up in the server. It not only increases client-side responding latency, but also causes server congestion and, in worse cases, a denial of service [105].

On the contrary, Oversized blocks may also become a problem. Generating and propagating larger blocks take more time, thus increasing the latency in an analogous manner. It also requires additional space to store larger blocks. As a result, only a few devices with more resource can and are willing to participate in bookkeeping, making the system less decentralized and more vulnerable to single point of failure [106]. Therefore, how to carefully calibrate the size of blocks will be a great challenge to all blockchain systems.

3.2.4. Impacts

Decentralization alleviates the performance bottleneck caused by centralized nodes to a certain extent. With the increase of the decentralization degree, system performance may unexpectedly decrease. Reaching consensus, querying data and batching requests in a highly decentralized system are time and resource consuming. Therefore, blockchain-based energy systems sometimes may fail to satisfy the high real-time requirements of dynamic control [107], fault diagnosis [108], and EV charging [109], which require immediate response to an emergency.

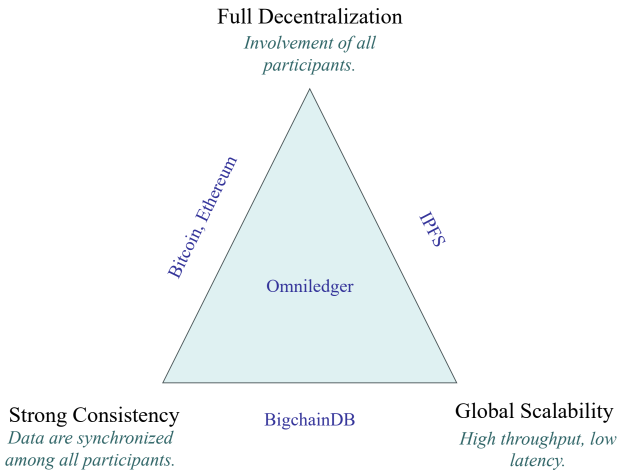

Full Decentralization
Involvement of all participants.
Bitcoin, Ethereum
IPFS
Omniledger
Strong Consistency
Data are synchronized among all participants.
BigchainDB
Global Scalability
High throughput, low latency.

Figure 5: The DCS Triangle [95, 110]. A distributed system that implements consensus can achieve two goals from full decentralization, strong consistency and global scalability at most. It is impossible to satisfy the three at the same time: Bitcoin and Ethereum cannot scale well, InterPlanetary File System (IPFS) [51] relaxes strong consistency requirement, and BigchainDB [111] involves a centralized voting federation. Omniledger [112] is able to find a balance between the three.

3.3. Lack of Scalability

Blockchain systems generally have scalability issues due to their underlying consensus mechanisms. **Scalability** reflects the ability of a system to handle workload increase as its scale expands [113]. The research on distributed consensus systems has been troubled by the problem of low scalability for the past few decades. PoW-, PoS- and BFT-based blockchains all have their own scalability issues [10]:

- PoW's low efficiency and high resource consumption make the operation and maintenance of a large system quite expensive;
- BFT algorithms require very strict theoretical assumptions and complicated subprotocols to resolve inconsistency, so the number of simultaneous clients the system can handle is rather small;
- PoS introduces monetary concepts and brings new security risks (to be discussed in Section 3.4), which could greatly increase the difficulty of preserving the security for a large-scale system.

The study of consensus algorithms encounters a trilemma called "the Decentralization-Consistency-Scalability (D-CS) triangle" (shown in Fig. 5). It has been theoretically proven that improving the scalability and consistency of a distributed consensus system comes at the expense of reducing its decentralization [110]. In essence, as the most core ingredient of the blockchain technology, consensus itself is a global synchronization problem that is generically difficult to solve in a decentralized manner.

Impacts. IoT technologies are important technical support of new generation energy systems. With the integration of IoT, the number of terminal devices deployed in an energy system is rapidly increasing. This puts forward higher requirements for the scalability of blockchain-based energy systems. However, the consensus algorithms of most existing blockchain systems are difficult to meet the scalability requirements of IoT [114]. To implement a practical blockchain-based energy system, choosing the most appropriate consensus mechanism and striking a balance between decentralization, consistency and scalability becomes a serious challenge to system designers.

3.4. Security Risks

The blockchain technology claims to provide many ideal security properties, such as anonymity, immutability, and robustness against single point of failures. Unfortunately, blockchain itself is still subject to various cyberattacks. There have been a lot of studies that analyze the cybersecurity risks of the blockchain in depth [144, 145, 146].

Table 2 enumerates these risks with detailed technical description, explanation about their causes, and corresponding cases, which covers: double spending [115], 51% attack [121], selfish mining [123], withholding attack [125], balance attack [128], nothing-at-stake attack [131], bribery attack [132], long-range attack [134]; eclipse attack [135], distributed Denial-of-Service (DDoS) attack [137], Sybil attack [140], and quantum computing attack [143].

Impacts. Although some of these attacks are only possible in theory and almost impossible to occur in reality (e.g., long-range attack), the particularity of energy industry itself might make them feasible. Take 51% attacks as an example. Controlling 51% of the computing resources of the whole network is not easy, so this kind of attack is rather difficult to take place in practice at present. However, the situation may change with the continuous implementation of real-world energy blockchain systems. Given the high centralization degree of energy industry, such an attack will become much more frequent and more prominent if a few industry giants assemble their resources to carry out 51% attacks for illegal profits. In addition, it cannot be ruled out that some power country is able to cause damage to another country by launching a 51% attack with its national power [121].

3.5. Unwanted Transparency and Defective Privacy

Supported by the decentralized blockchain system, information **transparency** is achievable by sharing the ledger between all participants. In the meanwhile, blockchain uses cryptography to protect the security of individual and corporate **privacy**. Many works implement energy blockchain for the purpose of increasing transparency and preserving privacy at the same time [147, 148, 149]. Unfortunately, the transparency and the privacy of blockchain are not impeccable, and they may even contradict each other.

In traditional transactions, user accounts are usually managed and protected by a third party. When users' accounts

Attack	Description	Cause	Case
Double spending [115]	The same asset is spent in multiple transactions, causing financial losses.	The long latency between initiation and verification of a blockchain transaction.	BitcoinGold [116], ZenCash [117], Zcash [118], and LitecoinCash [119] lost millions of dollars due to double spending attacks in 2018 [120].
51% attack [121]	Manipulate consensus results and persuade other miners to work on malicious forks by controlling 51% or more hashing power.	The consistency of PoW-based blockchains relies on hashing power.	Ethereum Classic suffered a 51% attack and over US$5.5 million were double spent in July 2020 [122].
Selfish mining [123]	Attackers also privately mine their own chains and publish these chains if they are longer than the main chain, causing other miners to abandon the main chain.	The lagging longest chain rule is used to choose the main chain.	The simulated selfish mining attack in [124] causes a fork rate of 1.51% in Bitcoin.
Withholding attack [125]	Discard complete solutions and only submit partial solutions to reduce the winning probability of pool mining.	Pool mining is widely used in PoW by having miners to solve hash puzzles togehter.	Eligius [126] lost up to 300 Bitcoins in the withholding attack in 2014 [127].
Balance attack [128]	Attackers choose a group of miners to delay and issue transactions with this group. Corresponding blocks may be removed by the GHOST protocol [129] when transactions take effects so that attackers can reissue these transactions.	The vulnerability of GHOST protocol to choose the main chain allows attackers to delay the network with only a little hashing power.	The test in [130] shows a 94% success rate of balance attack on Ethereum testnet within 4 minutes.
Nothing-at-stake attack [131]	Keep proposing blocks that cause forking.	The cost of building a chain is significantly low for PoS-based blockchains.	This attack only exists in theory at present.
Bribery attack [132]	Miners are bribed for more hashing power to create a fork, or for private keys to alter transaction records.	Carrying out bribery attacks is much cheaper in PoS-based blockchains.	The Goldfinger contract in [133] is able to bribe Ethereum for a block with only US$0.46.
Long-range attack [134]	Attackers creat forks from the beginning and overtake the main chain by building their own chains that are longer than the main chain.	The cost of building a chain is significantly less for PoS-based blockchains.	This attack only exists in theory at present.
Eclipse attack [135]	Compromise the links of victims so that victims only see information sent by attackers, causing inconsistent views of the ledger.	Nodes may not connect with each other simultaneously in a decentralized network.	An eclipse attack on Bitcoin is tested in [136] with a success rate of 85%.
DDoS attack [137]	Overwhelm the network and service by submitting large volume of requests.	The request processing of the blockchain is usually very slow.	The DDoS attack on BitMEX [138] in 2018 resulted in a US$300 drop in Bitcoin's price [139].
Sybil attack [140]	Use multiple identities to dominate the consensus results.	The blockchain enables anonymity and usually lacks an identity management mechanism.	A Sybil attack on Bitcoin was carried out by Chainalysis [141] in 2015 to collect information on the destination of transactions, threatening the privacy of Bitcoin users [142].
Quantum computing attack [143]	Break the cryptography and nullify system security with powerful quantum computing.	The security of many blockchain systems relies on computation workload.	This attack only exists in theory at present.

Table 2
Security risks of blockchain.

get lost or stolen, users can easily recover their accounts through some proof of real-world identity, such as ID card or passport. Unlike the traditional approach, blockchain accounts are protected by addresses and private keys and are usually not bound to real persons so as to provide a certain degree of privacy [150]. Once users forget their account information or lose their private keys, their accounts will never be recovered, and users will permanently lose their digital assets.

Moreover, the data stored on blockchain is transparently avaialble to all participants. Although private information will not be shared, it does not necessarily mean that the privacy will not get disclosed. What is worse, in order to achieve the more attactive goal of transparency, most blockchain systems only provide the lowest level of privacy protection [30]. In theory, side-channel analysis is shown to be quite proficient in breaking through blockchain privacy protection by correlating physical data (e.g., transmission time, power consumption, or electromagnetic radiation) [151, 152, 153]. It is also possible to locate and identify of some pivotal accounts by tracking transactions, analyzing transaction rules, and other anti-anonymity technologies [154, 155].

Impacts. Note that energy is the lifeblood of a country. It might put the country at risk if the unwanted transparency and defective privacy of energy blockchain are exploited. Once crucial data stored in energy blockchain are divulged, it could become possible to unscramble the energy trading rules, energy flow patterns, or even the energy policies [156].

3.6. Real-World Trust Issue

As we mentioned, blockchain has been widely used in commodity tracing due to its immutability and traceability. Although blockchain records the entire process of production, transportation, and distribution, it cannot completely eliminates the possibility of commodity fraud. Admittedly, blockchain data are difficult to tamper with, but the authenticity of these data before they are recorded into blockchains is not guaranteed. Moreover, the signators of smart contracts are usually represented by virtual accounts rather than real persons [157]. Consequently, real-world contract execution and accountability may be difficult to enforce.

To solve this problem, a specialized area of research has been put forward to explore "law is code", i.e., legal enforcement in the form of smart contracts [158, 159]. It yet violates the decentralization requirement of blockchain when the legislature is involved. Moreover, real-world trust can also be accomplished by binding virtual accounts with real persons, which again contradicts the privacy and anonymity of blockchain.

Impacts. The requirements for real-world trust of some energy systems may contradict the lightspots of blockchain. In strategic energy systems such as infrastructure construction, transportation, and offshore wind power, real-world trust is indispensable. To establish real-world trust, energy blockchain, as well as blockchain in other fields, might need to involve the certification from authorities, trusted measuring instruments, or legal restrictions [160].

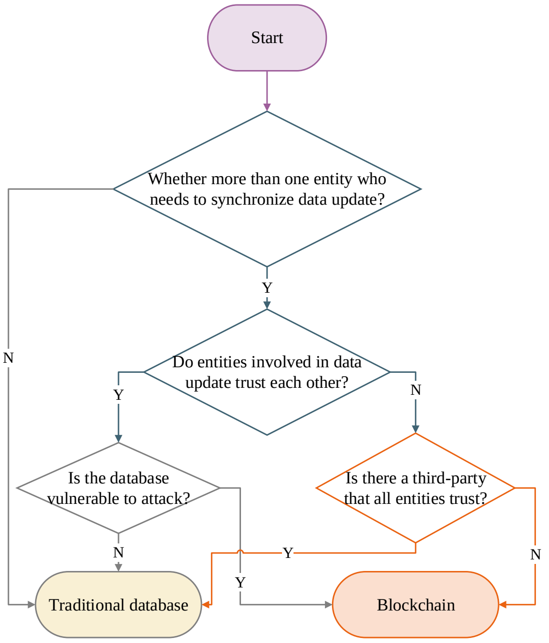

Start
Whether more than one entity who needs to synchronize data update?
Y
N
Do entities involved in data update trust each other?
Y
N
Is the database vulnerable to attack?
Is there a third-party that all entities trust?
N
Y
Y
N
Traditional database
Blockchain

Figure 6: A decision tree to choose between a traditional database and blockchain considering the establishment of mutual trust [161].

4. Possible Solutions for Energy Systems

In view of the limitations of blockchain, the challenges faced by energy blockchain are therefore nonnegligible. This section will summarize possible solutions in related studies that could deal with these challenges.

4.1. Blockchain or Database?

In view of the impacts of the defects of blockchain mentioned in Section 3, it is not a wise choice to follow the trend and use energy blockchain without careful consideration. The first question that every energy system designer must answer is whether it is necessary to deploy energy blockchain.

The real application of blockchain should conform to cost reduction, efficiency improvement, and many other practical requirements, instead of indulging in the vague words of "decentralization", "traceability", or "immutability". Unfortunately, many existing works fail to give full play to the advantages of blockchain and merely use energy blockchain as a secure database [162, 163, 164]. In fact, the blockchain systems in these works can as well be replaced by traditional databases with secure measures, which could greatly reduce the difficulty of system development.

Note that the core and irreplaceable value of blockchain lies in the establishment of mutual trust in decentralized and autonomous systems [161]. The authors of [161] provide a decision tree to choose between a traditional databases and blockchain (see Fig. 6). Since the implementation and maintenance of an entire blockchain system is complicated and expensive, energy blockchain is not recommended if a traditional database with security insurance suffices to complete the tasks.

4.2. Energy-Efficient Blockchain

Seeing the huge power consumption of existing energy blockchain systems (as described in Section 3.1.1), energy-efficient consensus algorithms for blockchain are needed to optimize the overall energy efficiency of energy systems.

Accordingly, some recent works choose PoS as a substitute for PoW [165, 166]. However, PoS brings new security risks (as described in Section 3.4). Besides, Proof of Elapsed Time (PoET) [167], Proof of Authority (PoAuth) [168], and Proof of Reputation (PoRep) [169] are also great energy-efficient consensus algorithms that could circumvent the issues faced by PoS-based consensus.

Other works choose to use PBFT-based Hyperledger Fabric as their blockchain platform [20, 21, 52]. However, classical BFT algorithms usually require more redundant nodes to tolerate Byzantine failures. They can work correctly in the presence of Byzantine faults unless the proportion of faulty nodes exceeds 33% (compared to the 50% of PoW and PoS) [170]. In other words, classical BFT algorithms need to spend the computation and storage resource of more participants to achieve the same robustness as PoW and PoS.

Another possible approach is to use renewable energy microgrid to power blockchain systems, thereby reducing the consumption of nonrenewable energy. Unlike most related works that use blockchain to support distributed energy trading in microgrids, blockchain miners are conversely recommended to purchase renewable energy from microgrids [171]. This strategy not only increases revenue by making full use of renewable energy, but also encourages deeper reciprocity between microgrids and blockchain.

4.3. Unseal the Block and Unleash the Chain

As we have explained in Section 3.2, a fixed block size could cause the degradation of system performance, and the chain structure could result in a slow query speed. Some recent works on distributed ledger technology (DLT) choose to abandon the block unit and chain structure of the blockchain. These ideas have great potentials in energy systems.

4.3.1. Block-Free Ledgers

Many works in energy blockchain have been using "blockchain" and "DLT" interchangeably. This phenomenon was broken since the emergence of block-free ledger technologies [172]. Implementing a block-free ledger could ingeniously circumvent the performance degradation caused by fixed block sizes [173].

Since the deployment of a blockchain system is very complicated, some works try to achieve the decentralized, traceable, and immutable nature of blockchain through block-free ledgers based only on cryptography, consensus, and smart contracts [174, 175]. By simplifying and improving the blockchain technology, block-free ledgers can not only meet the demands of energy systems for the ideal properties of blockchain, but also reduce the complexity of the system, thereby enhancing the feasibility of practical projects.

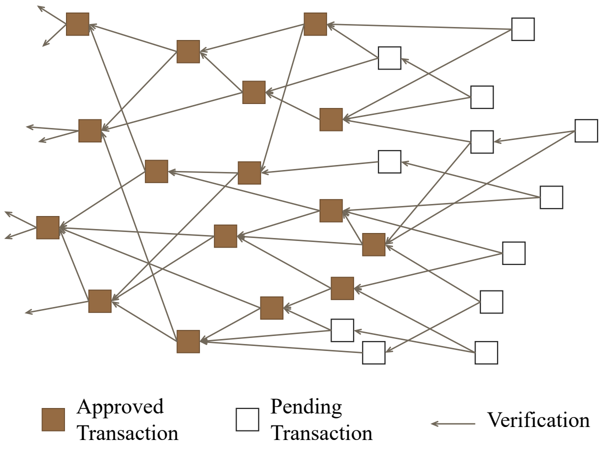


Figure 7: The directed acyclic structure of an IOTA ledger [183]. In IOTA, transactions referenced by two new transactions are seen as approved.

4.3.2. Directed Acyclic Graphs

In order to achieve better efficiency to meet the real-time requirements of energy systems, people start to add various pipelining mechanisms to blockchain to improve efficiency. As a result, the original chain structure of blockchain has begun to transform to a tree or a directed acyclic graph (DAG) [176]. The idea of DAG-based ledger technology recommends to avoid establishing a strict total order by a complete consensus mechanism in transaction approval. Each new transaction needs to verify at least two old transaction records as references, and a transaction verified by sufficient different transactions is seen as approved [177]. Fig. 7 shows the directed acyclic graph formed by the transactions in an IOTA ledger [172].

The emergence of DAG-based ledger technologies has greatly promoted the diversified development of DLTs, bringing up the era of "Blockchain 3.0" [178]. Compared to blockchain, DAG-based ledgers are more efficient and scalable, and they are more friendly to IoT systems (and therefore IoT-based energy systems) [179]. Charging piles that integrate IOTA functions have come into being in real-world communities to enable automatic and reliable energy transactions and data exchange with EVs [180]. Fantom [181], the first DAG-based platform, cooperates with IoT energy corporations in the hope of improving the energy efficiency of microgrids and constructing new infrastructure for reliable real-time transactions and data sharing [182]. Although there are not many related works on DAG-based energy systems, this is a direction worthy of in-depth excavation.

4.4. Secure Hardware Assistance

In related works about energy blockchain, hardware assistance has been rarely studied. In theory, hardware is considered to be more reliable than software in mitigating vulnerabilities and preserving security. By hardcoding programs in chips, the security guarantee provided by hardware cannot be nullified by any remote attacks unless these chips are physically shut down [184]. Moreover, hardware-based random numbers are more reliable than software-based pseudorandom numbers, thus providing more powerful cryptography [185]. In fact, secure hardware has been applied to enable trusted cryptography for blockchain-based energy transactions [186].

Secure hardware can also help to improve the scalability of energy blockchain. This can be achieved by improving the decentralization and scalability of blockchain consensus algorithms while acquiring consistency from secure hardware at the same time. Take PoET (mentioned in Section 4.2) as an example. Instead of solving hash puzzles, PoET only require a miner to wait for a time period randomly drawn from a predetermined probability distribution. To succeed in generating a block, the miner need to include a valid proof of the waiting time, generated by Software Guard Extensions (SGX) hardware [187], in the new block. Apart from SGX, the following hardware devices or services have also been applied to guarantee consensus security in similar ways [188, 189, 190, 191, 192]:

- Unique Sequential Identifier Generator (USIG) [193]
- Trusted Platform Module (TPM) [194];
- Field Programmable Gate Array (FPGA) [195];
- Trusted Execution Environments (TEE) [196];
- Remote Direct Memory Access (RDMA) [197];
- etc..

At present, there are not many research works on hardware-based energy blockchain. In view of the high security requirements of energy systems, secure hardware-based energy blockchain will become a promising choice.

4.5. Reputation Mechanisms

Energy blockchain helps to establish trust without any centralized authority in a distributed energy system. In most cases, participants have to reach consensus for each instance of participation, which is rather inefficient. In practice, real-world trust is cumulative and can be used as a reference in different scenarios.

Based on this, recent studies have begun to introduce reputation (or credit) mechanisms into blockchain systems. The reputation mechanism is mainly used to enable *delegated consensus*, which significantly reduce message complexity (i.e., the number of message transmissions to achieve consensus) and resource consumption by cutting down the number of consensus participants [198].

In delegated consensus, the credibility of each participant can be evaluated by a reputation score, either maintained locally or shared in public. The reputation score will be dynamically updated according to the historical record of consensus results and the behavior of the participant during consensus. The corresponding delegated consensus only needs to reach an agreement in a committee composed of high-reputation participants [199]. Take PBFT as an example. The delegated version of PBFT algorithm provided in [200] reduces its message complexity from quadratic to subquadratic, which is a great relief from the heavy communication overload of the original PBFT (see Fig. 8 for the comparison). Although entrusting consensus to a committee reduces the decentralization and security of the system, this compromise for efficiency and scalability is usually considered acceptable.

Apart from enhancing the underlying consensus, reputation mechanisms also show great potential in many energy scenarios. A credit risk management system can be developed for distributed energy transactions supported by the blockchain [202]. To prevent refusal to fulfill contracts, the system can take the credit score of the participant as an important attribute of the transaction account. Smart contracts will automatically raise the difficulty of transactions for participants with poor credit scores. In addition, reputation values can also be used to model the credibility of transactions from vehicles to ensure the safety of roadside units [203]. By integrating a reputation-based consensus algorithm, the efficiency of the energy sharing system will be further improved.

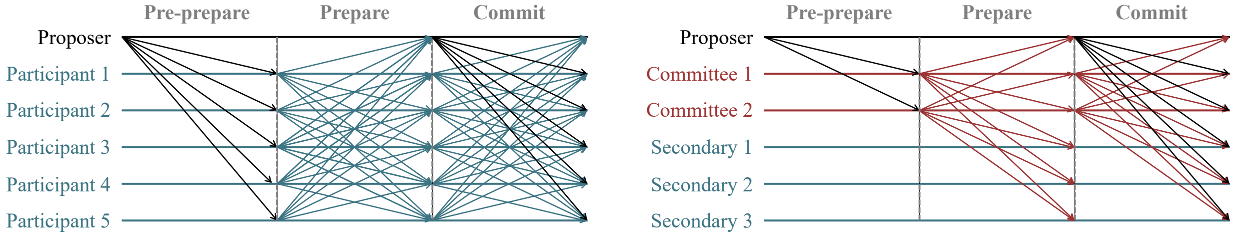
4.6. Laws and Regulations

“*Technology is a double-edged sword.*” This saying has never been outdated since the prosperity of information technology. If some blockchain user has ulterior motives, then the advantages of blockchain may also turn into disadvantages.

There is no lack of news about the blockchain technology being misused or abused. For instance, during the 2017 WannaCry ransomware attack, around 200,000 computers across 150 countries were hijacked until a ransom was paid in Bitcoin [204]. It caused a total of US$8 billion in losses, and the anonymity provided by the blockchain made it more difficult to locate and track the attacker’s account. In 2018, German researchers discovered that hundreds of links to child abuse images were hidden on the Bitcoin platform [205]. The immutability of the blockchain greatly increased the workload of removing inappropriate content.

In view of these potential blockchain abuses (especially crimes based on cryptocurrencies), many countries have successively introduced regulations on the use of the blockchain technology. In 2019, the U.S. government formulated detailed policies that stipulate how to use blockchain within the current regulatory framework [206]. While China encourages the development of the blockchain technology in practical projects, domestic transactions in any form of cryptocurrency are prohibited [207].

In the field of energy, related norms and rules also need to be improved, because the consequences of blockchain abuses in energy systems are not only financial but also social. The design of energy blockchain-based projects should in-



(a) Original PBFT [201]

(b) Delegated PBFT [200]

Figure 8: Communication patterns of original PBFT and delegated PBFT. By avoiding the participation of secondary members (i.e., members that are excluded from the committee), delegated PBFT greatly reduces its message complexity and improves its efficiency.

clude a clear definition of related privacy protection, auditing, and regulatory standards. During the construction of the Brooklyn Microgrid project described in [208], for example, representatives spent a lot of time in negotiating detailed rules with regulatory agencies. Although this may limit the scope of the project's business, it ensures that the project would be steadily promoted within the scope of the law. Incorporating rule-makers in blockchain systems breaks blockchain's pursuit of decentralization. However, compromising decentralization for the survival of blockchain might be reasonable and fair.

5. Conclusion

There are a wide range of energy scenarios in which blockchain has been applied. While people enjoy its theoretical benefits, blockchain has begun to expose its limitations to people in practice. It is undeniable that many advantages of blockchain are promoting the energy industry in a more digitalization, informatization, and modernization direction. However, it is worth noting that the energy industry is special. The consequences caused by the limitations of energy blockchain are not only technical, but also social, national, and international.

In essence, blockchain itself is not a new technology, but a fusion of various technologies. While integrating the advantages of multiple technologies, blockchain also inherits their generic disadvantages, and the fusion fails to mitigate these disadvantages. In addition, due to the particularity of the energy field, practical requirements of energy systems may conflict with the characteristics of blockchain. Based on these facts, this paper systematically review the limitations of blockchain and specially analyzes their impacts on energy systems. Besides, this paper also provides possible solutions to tackle with the challenges brought about by energy blockchain.

Decentralization is the most favorable feature of blockchain in energy systems. By removing centralized authorities, decentralization reduces intermediate expenses and increases system flexiblity. It also results in a transparent and tamper-resistant ledger. However, the huge cost of energy and storage resources caused by decentralization may contradicts the goal to make full use of resources. The low efficiency of decentralization can also make it impractical to develop blockchain-based energy systems. What is more, some critical and strategic energy projects may need centralization, which is incompatible with the decetralization of blockchain.

Since energy is related to the sustainable development of a country, the priority of security requirements in energy projects is often much higher than other requirements. In order to protect systems from potential cyberattacks, system designers who want to take advantage of blockchain security must implement additional security mechanisms. On the contrary, blockchain puts decentralization before security. The security of the vast majority of existing energy blockchain systems merely depends on blockchain itself and hardly implements additional security protection to deal with the security flaws in blockchain, which could be very dangerous.

The value of this paper includes two aspects. On the one hand, this paper recommends that future work need to carry out more in-depth research on the limitations of blockchain in energy systems. On the other hand, this paper emphasizes that energy system designers should fully consider whether it is necessary to deploy a complete blockchain system. This is not to criticize or deny the blockchain technology, but to provide an instruction for blockchain-based energy systems to develop in a more realistic and pragmatic direction.

References

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008, [accessed 9 October 2020].

[2] U. Tariq, A. Ibrahim, T. Ahmad, Y. Bouteraa, A. Elmogy, Blockchain in internet-of-things: a necessity framework for security, reliability, transparency, immutability and liability, IET Communications, 2019; 13:3187–3192.

[3] W. Tushar, T. K. Saha, C. Yuen, T. Morstyn, M. D. McCulloch, H. V. Poor, K. L. Wood, A motivational game-theoretic approach for peer-to-peer energy trading in the smart grid, Applied Energy, 2019; 243:10–20. doi:10.1016/j.apenergy.2019.03.111.

[4] J. J. Hunhevicz, D. M. Hall, Do you need a blockchain in construction? Use case categories and decision framework for DLT design options, Advanced Engineering Informatics, 2020; 45:101094. doi:10.1016/j.aei.2020.101094.

[5] Y.-B. Son, J.-H. Im, H.-Y. Kwon, S.-Y. Jeon, M.-K. Lee, Privacy-preserving peer-to-peer energy trading in blockchain-enabled smart grids using functional encryption, Energies, 2020; 13:1321.

[6] A. Kamilaris, A. Fonts, F. X. Prenafeta-Boldu, The rise of block-

chain technology in agriculture and food supply chains, Trends in Food Science & Technology, 2019; 91:640–652.

[7] H. Liu, Y. Zhang, T. Yang, Blockchain-enabled security in electric vehicles cloud and edge computing, IEEE Network, 2018; 32:78–83.

[8] M. Tieman, M. R. Darun, Leveraging blockchain technology for halal supply chains, Islam and Civilisational Renewal, 2017; 274:1–4.

[9] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, in: 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), IEEE, 2017, pp. 1–5.

[10] M. Salimitari, M. Chatterjee, A survey on consensus protocols in blockchain for IoT networks, 2018; arXiv preprint arXiv:1809.05613.

[11] T. Swanson, Blockchain 2.0—let a thousand chains blossom. https://letstalkbitcoin.com/blockchain-2-0-let-a-thousand-chains-blossom, 2014, [accessed 27 September 2020].

[12] S. Dekhane, K. Mhalgi, K. Vishwanath, S. Singh, N. Giri, GreenCoin: Empowering smart cities using blockchain 2.0, in: 2019 International Conference on Nascent Technologies in Engineering (ICNTE), 2019.

[13] Y. Li, W. Yang, P. He, C. Chen, X. Wang, Design and management of a distributed hybrid energy system through smart contract and blockchain, Applied Energy, 2019; 248:390–405. doi:10.1016/j.apenergy.2019.04.132.

[14] D. R. Putra, B. Anggorojati, A. P. P. Hartono, Blockchain and smart-contract for scalable access control in internet of things, in: 2019 International Conference on ICT for Smart Society (ICISS), 2019.

[15] S. Zhao, D. O'Mahony, Bmcprotector: A blockchain and smart contract based application for music copyright protection, in: Proceedings of the 2018 International Conference on Blockchain Technology and Application, 2018, pp. 1–5.

[16] J. Cao, H. Hua, , G. Ren, The SAGE Encyclopedia of the Internet, SAGE Publications, 2018, pp. 344–350.

[17] H. Hua, C. Hao, Y. Qin, Energy Internet: Systems and Applications, Springer, 2020, pp. 421–437.

[18] B. Teufel, A. Sentic, M. Barmet, Blockchain energy: Blockchain in future energy systems, Journal of Electronic Science and Technology, 2019; 17:317–331. doi:10.1016/j.jnlest.2020.100011.

[19] O. Jogunola, M. Hammoudeh, B. Adebisi, K. Anoh, Demonstrating blockchain-enabled peer-to-peer energy trading and sharing, in: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), IEEE, 2019, pp. 1–4.

[20] S. Saxena, H. Farag, A. Brookson, H. Turesson, H. Kim, Design and field implementation of blockchain based renewable energy trading in residential communities, in: 2019 2nd International Conference on Smart Grid and Renewable Energy (SGRE), IEEE, 2019, pp. 1–6.

[21] M. Kim, K. Park, S. Yu, J. Lee, Y. Park, S.-W. Lee, B. Chung, A secure charging system for electric vehicles based on blockchain, Sensors, 2019; 19:3028. doi:10.3390/s19133028.

[22] M. B. Ryssdal, Blockchain Technology Implementation for Electric Vehicle Charging within the Smart Grid Architecture Model, Master's thesis, NTNU, 2019.

[23] P. Claudia, C. Tudor, A. Marcel, A. Ionut, S. Ioan, B. Massimo, Blockchain based decentralized management of demand response programs in smart energy grids, Sensors, 2018; 18:162.

[24] V. Deshpande, L. George, H. Badis, A. A. Desta, Blockchain based decentralized framework for energy demand response marketplace, in: IEEE/IFIP Network Operations and Management Symposium, 2020.

[25] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, M. Bertoncini, Blockchain based decentralized management of demand response programs in smart energy grids, Sensors, 2018; 18:162.

[26] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaria, To blockchain or not to blockchain: That is the question, IT Professional, 2018; 20:62–74. doi:10.1109/mitp.2018.021921652.

[27] J. Golosova, A. Romanovs, The advantages and disadvantages of the blockchain technology, in: 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018.

[28] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, Z. Y. Dong, Cyber security framework for internet of things-based energy internet, Future Generation Computer Systems, 2019; 93:849–859. doi:10.1016/j.future.2018.01.029.

[29] B. Wen, N. Tian, X. Feng, E. Lu, Q. Guo, Research on the privacy-preserving energy management in power grid based on information masking, in: 2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2), 2019.

[30] Privacy for blockchains: An introduction. https://blog.coinmarketcap.com/2018/10/09/privacy-for-blockchains-an-introduction/, 2018, [accessed 15 September 2020].

[31] U. W. Chohan, The limits to blockchain? Scaling vs. decentralization, SSRN Electronic Journal, 2019; doi:10.2139/ssrn.3338560.

[32] Z. Che, Y. Wang, J. Zhao, Y. Qiang, Y. Ma, J. Liu, A distributed energy trading authentication mechanism based on a consortium blockchain, Energies, 2019; 12:2878. doi:10.3390/en12152878.

[33] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in: Proceedings of the thirteenth EuroSys conference, 2018, pp. 1–15.

[34] A. Dorri, A. Hill, S. S. Kanhere, R. Jurdak, F. Luo, Z. Y. Dong, Peer-to-peer energy trade: A distributed private energy trading platform, 2018; arXiv preprint arXiv:1812.08315v1.

[35] N. Schneider, Code your own utopia: Meet ethereum, bitcoin's most ambitious successor. http://america.aljazeera.com/articles/2014/4/7/code-your-own-utopiameetethereumbitcoinasmostambitioussuccessor.html, 2014, [accessed 4 August 2020].

[36] M. Faizan, T. Brenner, F. Foerster, C. Wittwer, B. Koch, Decentralized bottom-up energy trading using Ethereum as a platform, Journal of Energy Markets, 2019; 12:19–48. doi:10.21314/jem.2019.193.

[37] Y. Yu, Y. Guo, W. Min, F. Zeng, Trusted transactions in micro-grid based on blockchain, Energies, 2019; 12:1952.

[38] M. U. Gurmani, T. Sultana, A. Ghaffar, M. Azeem, Z. Abubaker, H. Farooq, N. Javaid, Energy trading between prosumer and consumer in p2p network using blockchain, in: Advances on P2P, Parallel, Grid, Cloud and Internet Computing, Springer International Publishing, 2019, pp. 875–886. doi:10.1007/978-3-030-33509-0_82.

[39] M. Mihaylov, I. Razo-Zapata, A. Nowé, NRGcoin—a blockchain-based reward mechanism for both production and consumption of renewable energy, in: Transforming Climate Finance and Green Investment with Blockchains, Elsevier, 2018, pp. 111–131. doi:10.1016/B978-0-12-814447-3.00009-4.

[40] The ECO coin. https://uploads-ssl.webflow.com/5c1b58255c613376879c2558/5c4970105b4d237571564f43_ECOcoin_white_paper_v1.0.pdf, [accessed 6 October 2020].

[41] ImpactPPA. https://www.impactppa.com/wp-content/uploads/2018/03/ImpactPPA_WP_v1.2WEB.pdf, 2018, [accessed 6 October 2020].

[42] V. Peter, J. Paredes, M. R. Rivial, E. S. Sepúlveda, D. A. H. Astorga, Blockchain meets energy: digital solutions for a decentralized and decarbonized sector, German-Mexican Energy Partnership (EP) and Florence School of Regulation (FSR), 2019.

[43] G. Wang, Z. J. Shi, M. Nixon, S. Han, SMChain: A scalable blockchain protocol for secure metering systems in distributed industrial plants, in: Proceedings of the International Conference on Internet of Things Design and Implementation, ACM, 2019.

[44] F. Imbault, M. Swiatek, R. De Beaufort, R. Plana, 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), IEEE, 2017, pp. 1–5.

[45] M. Hearn, Corda: A distributed ledger. https://www.corda.net/content/corda-technical-whitepaper.pdf, 2016, [accessed 9 October 2020].

[46] F. Zhao, X. Guo, W. K. Chan, Individual green certificates on blockchain: A simulation approach, Sustainability, 2020; 12:3942.

[47] L. Franke, M. Schletz, S. Salomo, Designing a blockchain model for the paris agreement's carbon market mechanism, Sustainability, 2020; 12:1068. doi:10.3390/su12031068.

[48] J. Eckert, D. López, C. L. Azevedo, B. Farooq, A blockchain-based user-centric emission monitoring and trading system for multi-modal mobility, 2019; arXiv preprint arXiv:1908.05629.

[49] Hyperledger Iroha documentation. https://iroha.readthedocs.io/en/master/#hyperledger-iroha-documentation, [accessed 27 September 2020].

[50] F. Liss, Blockchain and the EU ETS: An architecture and a prototype of a decentralized emission trading system based on smart contracts, Ph.D. thesis, Technical University of Munich, 2018.

[51] Delivering innovative financial and technology solutions for insurance premium financing. https://www.ipfs.com/, [accessed 12 September 2020].

[52] G. Suciu, M.-A. Sachian, M. Dobrea, C.-I. Istrate, A. L. Petrache, A. Vulpe, M. Vochin, Securing the smart grid: A blockchain-based secure smart energy system, in: 2019 54th International Universities Power Engineering Conference (UPEC), IEEE, 2019, pp. 1–5.

[53] E. Münsing, J. Mather, S. Moura, Blockchains for decentralized optimization of energy resources in microgrid networks, in: 2017 IEEE conference on control technology and applications (CCTA), IEEE, 2017, pp. 2164–2171.

[54] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, M. Guizani, Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city, IEEE Access, 2019; 7:18611–18621. doi:10.1109/access.2019.2896065.

[55] L. Hang, D.-H. Kim, Design and implementation of an integrated IoT blockchain platform for sensing data integrity, Sensors, 2019; 19:2228. doi:10.3390/s19102228.

[56] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, E. Hossain, Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains, IEEE Transactions on Industrial Informatics, 2017; 13:3154–3164.

[57] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews, 2019; 100:143–174. doi:10.1016/j.rser.2018.10.014.

[58] M. Giancaspro, Is a 'smart contract' really a smart idea? Insights from a legal perspective, Computer law & security review, 2017; 33:825–835.

[59] N.-U.-R. Chowdhury, K. Islam, F. Hasan, An efficient algorithm for peer-to-peer energy trading using blockchain in microgrid energy markets, European Journal of Electrical Engineering and Computer Science, 2019; 3:. doi:10.24018/ejece.2019.3.3.80.

[60] B. Shanmugam, S. Azam, K. C. Yeo, J. Jose, K. Kannoorpatti, A critical review of Bitcoins usage by cybercriminals, in: 2017 International Conference on Computer Communication and Informatics (ICCCI), 2017.

[61] B. Scott, How can cryptocurrency and blockchaintechnology play a role in building social and solidarity finance. https://www.weusecoins.com/assets/pdf/library/Cryptocurrency%20and%20Blockchain%20-%20Role%20in%20Building%20Social%20and%20Solidarity%20Finance.pdf, 2016, [accessed 6 October 2020].

[62] N. Amarasinghe, X. Boyen, M. Mckague, A survey of anonymity of cryptocurrencies, in: the Australasian Computer Science Week Multiconference, 2019.

[63] A. Fagkra, Blockchain in Energy Markets The case of Electricity Sector, Ph.D. thesis, International Hellenic University, 2019.

[64] J. C. Olivares-Rojas, E. Reyes-Archundia, J. A. Gutiérrez-Gnecchi, I. Molina-Moreno, A survey on smart metering systems using blockchain for E-mobility, 2020; arXiv preprint arXiv:2009.09075.

[65] Y. L. Wang, Y. H. Zhou, H. F. Gu, A new market mode based on pricing mechanism of green power, in: China International Conference on Electricity Distribution, 2009.

[66] Green insurance. https://www.nationalbanken.dk/en/governmentdebt/IR/Pages/Model-for-sovereign-green-bonds.aspx, 2020, [accessed 29 September 2020].

[67] H. Wang, L. Wang, S. Shi, C. Gao, Research on US green certificate trading mechanism experience and domestic implementation prospects, IOP Conference Series: Earth and Environmental Science, 2019; 237:052035. doi:10.1088/1755-1315/237/5/052035.

[68] Q. Weng, H. Xu, A review of China's carbon trading market, Renewable and Sustainable Energy Reviews, 2018; 91:613–619. doi:10.1016/j.rser.2018.04.026.

[69] Carbon footprinting. https://prod-drupal-files.storage.googleapis.com/documents/resource/restricted/carbon-footprinting-guide.pdf, 2018, [accessed 29 September 2020].

[70] W. Hua, J. Jiang, H. Sun, J. Wu, A blockchain based peer-to-peer trading framework integrating energy and carbon markets, Applied Energy, 2020; 279:115539. doi:10.1016/j.apenergy.2020.115539.

[71] A. Richardson, J. Xu, Carbon trading with blockchain, 2020; arXiv preprint arXiv:2005.02474.

[72] H. Hua, Y. Qin, H. Xu, C. Hao, J. Cao, Robust control method for DC microgrids and energy routers to improve voltage stability in energy internet, Energies, 2019; 12:1622. doi:10.3390/en12091622.

[73] H. Hua, Y. Qin, C. Hao, J. Cao, Optimal energy management strategies for energy internet via deep reinforcement learning approach, Applied Energy, 2019; 239:598–609. doi:10.1016/j.apenergy.2019.01.145.

[74] H. Hua, J. Cao, G. Yang, G. Ren, Voltage control for uncertain stochastic nonlinear system with application to energy internet: Non-fragile robust H_∞ approach, Journal of Mathematical Analysis and Applications, 2018; 463:93–110. doi:10.1016/j.jmaa.2018.03.002.

[75] M. Bauer, T. T. Nguyen, A. Jossen, J. Lygeros, Evaluating frequency regulation operated on two stationary energy systems with batteries from electric vehicles, Energy Procedia, 2018; 155:32–43. doi:10.1016/j.egypro.2018.11.068.

[76] J. M. Lujano-Rojas, G. Zubi, R. Dufo-López, J. L. Bernal-Agustín, J. L. Atencio-Guerra, J. P. S. Catalão, Embedding quasi-static time series within a genetic algorithm for stochastic optimization: the case of reactive power compensation on distribution systems, Journal of Computational Design and Engineering, 2020; 7:177–194.

[77] H. Hua, Y. Qin, Z. He, L. Li, J. Cao, Energy sharing and frequency regulation in energy internet via mixed H_2/H_∞ control with Markovian jump, CSEE Journal of Power and Energy Systems, 2020; doi:10.17775/CSEEJPES.2019.01900.

[78] B. Singh, R. Mahanty, S. P. Singh, Social welfare maximization for congestion management in multiutility market using improved PSO incorporating transmission loss cost allocation, International Transactions on Electrical Energy Systems, 2018; 28:e2593.

[79] P. Gope, B. Sikdar, An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids, IEEE Internet of Things Journal, 2018; 5:3126–3135. doi:10.1109/jiot.2018.2833863.

[80] M. Bahramipanah, D. Torregrossa, R. Cherkaoui, M. Paolone, A decentralized adaptive model-based real-time control for active distribution networks using battery energy storage systems, IEEE Transactions on Smart Grid, 2018; 9:3406–3418. doi:10.1109/TSG.2016.2631569.

[81] H. Pourbabak, J. Luo, T. Chen, W. Su, A novel consensus-based distributed algorithm for economic dispatch based on local estimation of power mismatch, IEEE Transactions on Smart Grid, 2018; 9:5930–5942. doi:10.1109/tsg.2017.2699084.

[82] M. Fan, X. Zhang, Consortium blockchain based data aggregation and regulation mechanism for smart grid, IEEE Access, 2019; 7:35929–35940. doi:10.1109/access.2019.2905298.

[83] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, K.-C. Wang, Review of internet of things (IoT) in electric power and energy systems, IEEE Internet of Things Journal, 2018; 5:847–870.

[84] C. Luo, Y.-F. Huang, V. Gupta, Dynamic pricing and energy management strategy for EV charging stations under uncertainties, in: Proceedings of the International Conference on Vehicle Technology and Intelligent Transport Systems, SCITEPRESS - Science and and Technology Publications, 2016. doi:10.5220/0005797100490059.

[85] T. Zhang, H. Pota, C.-C. Chu, R. Gadh, Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency, Applied Energy, 2018; 226:582–594. doi:10.1016/j.apenergy.2018.06.025.

[86] M. Atzori, Blockchain technology and decentralized governance: Is the state still necessary, Journal of Governance and Regulation, 2017; 6:45–62. doi:10.22495/jgr_v6_i1_p5.

[87] H. Albrecher, P.-O. Goffard, On the profitability of selfish blockchain mining under consideration of ruin. https://eprint.iacr.org/2020/094.pdf, 2020, [accessed 9 October 2020].

[88] A. Lihu, J. Du, I. Barjaktarevic, P. Gerzanics, M. Harvilla, A proof of useful work for artificial intelligence on the blockchain, 2020; arXiv preprint arXiv:2001.09244v1.

[89] O. Serpell, Energy and the blockchain. https://kleinmanenergy.upenn.edu/sites/default/files/policydigest/Energy%20and%20the%20Blockchain.pdf, 2018, [accessed 7 October 2020].

[90] J. Sedlmeir, H. U. Buhl, G. Fridgen, R. Keller, The energy consumption of blockchain technology: Beyond myth, Business & Information Systems Engineering, 2020; doi:10.1007/s12599-020-00656-x.

[91] Ethereum 2.0 - what is Proof of Stake. https://our.status.im/ethereum-2-0-what-is-proof-of-stake/, 2020, [accessed 7 October 2020].

[92] S. King, S. Nadal, PPCoin: Peer-to-peer crypto-currency with proof-of-stake. https://decred.org/research/king2012.pdf, 2012, [accessed 8 April 2020].

[93] S. Liu, Bitcoin blockchain size 2010-2020, by quarter. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/, 2020, [accessed 31 August 2020].

[94] R. Abe, Blockchain storage load balancing among DHT clustered nodes, 2019; arXiv preprint arXiv:1902.02174.

[95] T. McConaghy, The DCS triangle. https://blog.bigchaindb.com/the-dcs-triangle-5ce0e9e0f1dc, 2016, [accessed 4 August 2020].

[96] M. Yu, S. Sahraei, S. Li, S. Avestimehr, S. Kannan, P. Viswanath, Coded Merkle tree: Solving data availability attacks in blockchains, in: Financial Cryptography and Data Security, Springer International Publishing, 2020, pp. 114–134. doi:10.1007/978-3-030-51280-4_8.

[97] A. Dorri, R. Jurdak, Tree-Chain: A fast lightweight consensus algorithm for IoT applications, 2020; arXiv preprint arXiv:2005.09443.

[98] S. Brotsis, N. Kolokotronis, K. Limniotis, S. Shiaeles, D. Kavallieros, E. Bellini, C. Pavue, Blockchain solutions for forensic evidence preservation in IoT environments, in: 2019 IEEE Conference on Network Softwarization (NetSoft), IEEE, 2019. doi:10.1109/netsoft.2019.8806675.

[99] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, R. Wattenhofer, On scaling decentralized blockchains, in: Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2016, pp. 106–125.

[100] M. Trillo, Stress test prepares VisaNet for the most wonderful time of the year. https://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html, 2013, [accessed 4 August 2020].

[101] M. Z. Abid, A Multi-leader Approach to Byzantine Fault Tolerance, Master's thesis, KTH Royal Institute of Technology, 2015.

[102] S. Duan, M. K. Reiter, H. Zhang, BEAT: Asynchronous BFT made practical, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2018.

[103] S. Chen, J. Zhang, R. Shi, J. Yan, Q. Ke, A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems, in: Distributed, Ambient and Pervasive Interactions: Understanding Humans, Springer International Publishing, 2018, pp. 21–34.

[104] Z. Peng, H. Wu, B. Xiao, S. Guo, VQL: Providing query efficiency and data authenticity in blockchain systems, in: 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW), IEEE, 2019. doi:10.1109/icdew.2019.00-44.

[105] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, A. Mohaisen, Exploring the attack surface of blockchain: A systematic overview, 2019; arXiv preprint arXiv:1904.03487v1.

[106] M. Scherer, Performance and Scalability of Blockchain Networks and Smart Contracts, Master's thesis, Umeå University, 2017.

[107] M. Bell, F. Berkel, S. Liu, Real-time distributed control of low-voltage grids with dynamic optimal power dispatch of renewable energy sources, IEEE Transactions on Sustainable Energy, 2019; 10:417–425. doi:10.1109/tste.2018.2800108.

[108] M. Shahbazi, P. Poure, S. Saadate, Real-time power switch fault diagnosis and fault-tolerant operation in a DFIG-based wind energy system, Renewable energy, 2018; 116:209–218.

[109] W. Jiang, Y. Zhen, A real-time EV charging scheduling for parking lots with PV system and energy store system, IEEE Access, 2019; 7:86184–86193. doi:10.1109/access.2019.2925559.

[110] G. Slepak, A. Petrova, The DCS theorem, 2018; arXiv preprint arXiv:1801.04335v1.

[111] Meet BigchainDB. https://www.bigchaindb.com/, [accessed 16 September 2020].

[112] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, B. Ford, Omniledger: A secure, scale-out, decentralized ledger via sharding, in: 2018 IEEE Symposium on Security and Privacy (SP), IEEE, 2018, pp. 583–598.

[113] C. B. Weinstock, J. B. Goodenough, On System Scalability, Technical Report CMU/SEI-2006-TN-012, Carnegie Mellon University, 2006.

[114] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, Y. Yang, A survey of IoT applications in blockchain systems, ACM Computing Surveys, 2020; 53:1–32. doi:10.1145/3372136.

[115] A. Begum, A. Tareq, M. Sultana, M. Sohel, T. Rahman, A. Sarwar, Blockchain attacks, analysis and a model to solve double spending attack, International Journal of Machine Learning and Computing, 2020; 10:.

[116] BITCOIN GOLD. https://bitcoingold.org/, [accessed 15 September 2020].

[117] HORIZEN FAUCET. https://getzen.cash/?_lang=en, [accessed 15 September 2020].

[118] Mining Zcash. https://z.cash/mining/, [accessed 15 September 2020].

[119] LitecoinCash. https://litecoinca.sh/, [accessed 15 September 2020].

[120] J. Jang, H.-N. Lee, Profitable double-spending attacks, 2019; arXiv preprint arXiv:1903.01711.

[121] S. Sayeed, H. Marco-Gisbert, Assessing blockchain consensus and security mechanisms against the 51% attack, Applied Sciences, 2019; 9:1788.

[122] A. Behrens, Hacker nets over $5 million in Ethereum Classic 51% attack. https://decrypt.co/37721/hacker-nets-over-5-million-ethereum-classic-51-attack, 2020, [accessed 16 September 2020].

[123] Q. Bai, X. Zhou, X. Wang, Y. Xu, X. Wang, Q. Kong, A deep dive into blockchain selfish mining, 2018; arXiv preprint arXiv:1811.08263.

[124] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016.

[125] R. Qin, Y. Yuan, F.-Y. Wang, Optimal block withholding strategies for blockchain mining pools, IEEE Transactions on Computational Social Systems, 2020; 7:709–717. doi:10.1109/tcss.2020.2991097.

[126] ELIGIUS. http://eligius.st/, [accessed 12 June 2020].

[127] S.-Y. Chang, Share withholding attack in blockchain mining: Technical report, 2020; arXiv preprint arXiv:2008.13317.

[128] C. Natoli, V. Gramoli, The balance attack against proof-of-work blockchains: The R3 testbed as an example, 2016; arXiv preprint arXiv:1612.09426.

[129] L. Kovalchuk, D. Kaidalov, O. Shevtsov, A. Nastenko, R. Oliynykov, Analysis of splitting attacks on Bitcoin and GHOST consensus protocols, in: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017.

[130] C. Natoli, V. Gramoli, The balance attack or why forkable blockchains are ill-suited for consortium, in: 2017 47th Annual IEEE/IFIP

International Conference on Dependable Systems and Networks (D-SN), IEEE, 2017. doi:10.1109/dsn.2017.44.

[131] F. Saleh, Blockchain without waste: Proof-of-stake, SSRN Electronic Journal, 2018; doi:10.2139/ssrn.3183935.

[132] J. Bonneau, Why buy when you can rent, in: International Conference on Financial Cryptography and Data Security, Springer, 2016, pp. 19–26.

[133] P. McCorry, A. Hicks, S. Meiklejohn, Smart contracts for bribing miners, in: Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2019, pp. 3–18.

[134] E. Deirmentzoglou, G. Papakyriakopoulos, C. Patsakis, A survey on long-range attacks for proof of stake protocols, IEEE Access, 2019; 7:28712–28725. doi:10.1109/access.2019.2901858.

[135] G. Xu, B. Guo, C. Su, X. Zheng, K. Liang, D. S. Wong, H. Wang, Am I eclipsed? A smart detector of eclipse attacks for Ethereum, Computers & Security, 2020; 88:101604. doi:10.1016/j.cose.2019.101604.

[136] E. Heilman, A. Kendler, A. Zohar, S. Goldberg, Eclipse attacks on Bitcoin's peer-to-peer network, in: Proceedings of the 24th USENIX Conference on Security Symposium, SEC'15, USENIX Association, USA, 2015, p. 129–144.

[137] A. Feder, N. Gandal, J. Hamrick, T. Moore, The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox, Journal of Cybersecurity, 2017; 3:137–144.

[138] BitMEX | Bitcoin mercantile exchange. https://www.bitmex.com/, [accessed 14 September 2020].

[139] K. Sedgwick, Bitcoin history: When DDoS attacks made BTC's price drop. https://news.bitcoin.com/bitcoin-history-25/, 2020, [accessed 15 September 2020].

[140] P. Swathi, C. Modi, D. Patel, Preventing sybil attack in blockchain using distributed behavior monitoring of miners, in: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2019, pp. 1–6.

[141] Building trust in blockchains. https://www.chainalysis.com/, [accessed 15 September 2020].

[142] G. Caffyn, Chainalysis CEO denies 'Sybil attack' on Bitcoin's network. https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network, 2015, [accessed 15 September 2020].

[143] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, W. J. Knottenbelt, Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack, Royal Society Open Science, 2018; 5:180410. doi:10.1098/rsos.180410.

[144] J. Moubarak, E. Filiol, M. Chamoun, On blockchain security and relevant attacks, in: 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), 2018.

[145] M. Iqbal, R. Matulevicius, Blockchain-based application security risks: A systematic literature review, in: International Conference on Advanced Information Systems Engineering (CAiSE): Advanced Information Systems Engineering Workshops, 2019, pp. 176–188.

[146] E. Zamani, Y. He, M. Phillips, On the security risks of the blockchain, Journal of Computer Information Systems, 2018; 0:1–12.

[147] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, M. Rahman, Blockchain-based privacy-preserving charging coordination mechanism for energy storage units, 2018; arXiv preprint arXiv:1811.02001.

[148] E. M. Radi, N. Lasla, S. Bakiras, M. Mahmoud, Privacy-preserving electric vehicle charging for peer-to-peer energy trading ecosystems, in: ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019.

[149] W. A. Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, K. Akkaya, Privacy-preserving smart parking system using blockchain and private information retrieval, 2019; arXiv preprint arXiv:1904.09703.

[150] F. Béres, I. A. Seres, A. A. Benczúr, M. Quintyne-Collins, Blockchain is watching you: Profiling and deanonymizing Ethereum users, 2020; arXiv preprint arXiv:2005.14051.

[151] A. Miller, Y. Xia, K. Croman, E. Shi, D. Song, The honey badger of BFT protocols, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 31–42.

[152] N. Courtois, G. Song, R. Castellucci, Speed optimizations in bitcoin key recovery attacks, Nephron Clinical Practice, 2016; 67:55–68.

[153] M. Ma, X. Yang, G. Shi, F. Li, Enhanced blockchain based key management scheme against key exposure attack, in: Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing - AIIPCC '19, ACM Press, 2019.

[154] J. Appelbaum, M. Ray, K. Koscher, I. Finder, vpwns: Virtual pwned networks, in: 2nd USENIX Workshop on Free and Open Communications on the Internet. USENIX Association, 2012.

[155] N. Krawetz, Anti-honeypot technology, IEEE Security & Privacy, 2004; 2:76–79.

[156] C. Bowe, Can blockchain power the energy business. https://www.brinknews.com/can-blockchain-power-the-energy-business/, 2018, [accessed 12 Octover 2020].

[157] H. X. Son, M. H. Nguyen, N. N. Phien, H. T. Le, Q. N. Nguyen, V. Dinh, P. Tru, P. Nguyen, Towards a mechanism for protecting seller's interest of cash on delivery by using smart contract in hyperledger, International Journal of Advanced Computer Science and Applications, 2019; 10:45–50.

[158] J. S. Notland, J. S. Notland, D. Morrison, The minimum hybrid contract (mhc): Combining legal and blockchain smart contracts, 2020; arXiv preprint arXiv:2002.06850.

[159] P. D. Filippi, S. Hassan, Blockchain technology as a regulatory technology: From code is law to law is code, First Monday, 2016; .

[160] S. McNew, Privacy & regulatory considerations in enterprise blockchain. https://www.darkreading.com/risk/privacy-and-regulatory-considerations-in-enterprise-blockchain-/a/d-id/1334277, 2019, [accessed 12 October 2020].

[161] S. Chen, H. Wang, Z. Yan, Z. Shen, J. Ping, N. Zhang, C. Kang, Rethinking the value of blockchain: Direction and boundary of blockchain applications, Proceedings of the Chinese Society for Electrical Engineering, 2020; 40:2123–2132. (in Chinese).

[162] R. Casado-Vara, J. Prieto, J. M. Corchado, How blockchain could improve fraud detection in power distribution grid, in: Advances in Intelligent Systems and Computing, Springer International Publishing, 2018, pp. 67–76. doi:10.1007/978-3-319-94120-2_7.

[163] J. Mattila, T. Seppälä, C. Naucler, R. Stahl, M. Tikkanen, A. Bådenlid, J. Seppälä, Industrial blockchain platforms: An exercise in use case development in the energy industry. https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-43.pdf, 2016, [accessed 5 August 2020].

[164] J. Hwang, M. in Choi, T. Lee, S. Jeon, S. Kim, S. Park, S. Park, Energy prosumer business model using blockchain system to ensure transparency and safety, Energy Procedia, 2017; 141:194–198.

[165] A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: A provably secure proof-of-stake blockchain protocol, in: Annual International Cryptology Conference, 2017.

[166] Z. Jaroucheh, B. Ghaleb, W. J. Buchanan, SklCoin: Toward a scalable proof-of-stake and collective signature based consensus protocol for strong consistency in blockchain, in: 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), 2020.

[167] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, W. Shi, On security analysis of proof-of-elapsed-time (PoET), in: International Symposium on Stabilization, Safety, and Security of Distributed Systems, Springer, 2017, pp. 282–297.

[168] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone, PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain, in: Italian Conference on Cyber Security, 2018.

[169] Q. Zhuang, Y. Liu, L. Chen, Z. Ai, Proof of reputation: A reputation-based consensus protocol for blockchain based systems, in: Proceedings of the 2019 International Electronics Communication Conference, 2019, pp. 131–138.

[170] Y. Amoussou-Guenou, A. D. Pozzo, M. Potop-Butucaru, S. Tucci-Piergiovanni, Correctness and fairness of Tendermint-core blockchains, 2018; arXiv preprint arXiv:1805.08429.

[171] J. Li, Z. Zhou, J. Wu, J. Li, S. Mumtaz, X. Lin, H. Gacanin, S. Alotaibi, Decentralized on-demand energy supply for blockchain in internet of things: A microgrids approach, IEEE Transactions on Computational Social Systems, 2019; 6:1395–1406.

[172] J. Park, R. Chitchyan, A. Angelopoulou, J. Murkin, A block-free distributed ledger for P2P energy trading: Case with IOTA, in: International Conference on Advanced Information Systems Engineering, 2019, pp. 111–125.

[173] K. Jannes, B. Lagaisse, W. Joosen, You don't need a ledger: Lightweight decentralized consensus between mobile web clients, in: Proceedings of the 3rd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, 2019, pp. 3–8.

[174] M. Bottone, F. Raimondi, G. Primiero, Multi-agent based simulations of block-free distributed ledgers, in: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, 2018, pp. 585–590.

[175] R. Rahmani, Y. Li, A scalable digital infrastructure for sustainable energy grid enabled by distributed ledger technology, Journal of Ubiquitous Systems & Pervasive Networks, 2020; 12:17–24.

[176] H. Pervez, M. Muneeb, M. U. Irfan, I. U. Haq, A comparative analysis of DAG-based blockchain architectures, in: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), IEEE, 2018. doi:10.1109/icosst.2018.8632193.

[177] Y. Sompolinsky, S. Wyborski, A. Zohar, PHANTOM and GHOSTDAG. https://eprint.iacr.org/2018/104.pdf, 2020, [accessed 7 October 2020].

[178] C. Comben, What is blockchain 3.0. https://nulltx.com/what-is-blockchain-3-0/, 2018, [accessed 7 October 2020].

[179] Z. Zhang, V. Vasavada, X. Ma, L. Zhang, DLedger: An IoT-friendly private distributed ledger system based on DAG, 2019; arXiv preprint arXiv:1902.09031v2.

[180] H. van den Brink, World's first IOTA smart charging station. https://blog.iota.org/worlds-first-iota-smart-charging-station-52f9024db788, 2018, [accessed 5 August 2020].

[181] S.-M. Choi, J. Park, Q. Nguyen, A. Cronje, Fantom: A scalable framework for asynchronous distributed systems, 2018; arXiv preprint arXiv:1810.10360.

[182] DAG smart contract platform Fantom partners with IOT energy giant, Danfoss. https://bitcoinexchangeguide.com/fantom-blockchain-project-partners-with-multi-billion-dollar-danfoss-iot-energy-giant/, 2018, [accessed 2 September 2020].

[183] S. Popov, The tangle. http://www.descryptions.com/Iota.pdf, 2018, [accessed 17 August 2020].

[184] M. Nickolova, E. Nickolov, Verification and application of conceptual model and security requirements on practical DRM systems in E-learning, Information Technologies and Knowledge, 2007; 1:163–168.

[185] E. Syta, I. Tamas, D. Visher, D. I. Wolinsky, P. Jovanovic, L. Gasser, N. Gailly, I. Khoffi, B. Ford, Keeping authorities "honest or bust" with decentralized witness Cosigning, in: 2016 IEEE Symposium on Security and Privacy (SP), IEEE, 2016. doi:10.1109/sp.2016.38.

[186] S. S. Saha, C. Gorog, A. Moser, A. Scaglione, N. G. Johnson, Integrating hardware security into a blockchain-based transactive energy platform, 2020; arXiv preprint arXiv:2008.10705.

[187] Intel®software guard extensions. https://software.intel.com/content/www/us/en/develop/topics/software-guard-extensions.html, [accessed 16 September 2020].

[188] G. S. Veronese, M. Correia, A. N. Bessani, L. C. L. L. C. Lung, EBAWA: Efficient byzantine agreement for wide-area networks, in: 2010 IEEE 12th International Symposium on High Assurance Systems Engineering, 2010.

[189] G. S. Veronese, M. Correia, A. N. Bessani, L. C. Lung, P. Verissimo, Efficient byzantine fault-tolerance, IEEE Transactions on Computers, 2013; 62:16–30. doi:10.1109/tc.2011.221.

[190] R. Kapitza, J. Behl, C. Cachin, T. Distler, K. Stengel, CheapBFT: Resource-efficient byzantine fault tolerance, in: ACM EuroSys conference on computer systems, 2012.

[191] J. Liu, W. Li, G. O. Karame, N. Asokan, Scalable byzantine consensus via hardware-assisted secret sharing, 2016; arXiv preprint arXiv:1612.04997.

[192] M. K. Aguilera, N. Ben-David, R. Guerraoui, V. Marathe, I. Zablotchi, The impact of RDMA on agreement, 2019; arXiv preprint arXiv:1905.12143.

[193] G. S. Veronese, M. Correia, A. N. Bessani, L. C. Lung, Highly-resilient services for critical infrastructures.

[194] L. F. G. Sarmenta, M. van Dijk, C. W. O'Donnell, J. Rhodes, S. Devadas, Virtual monotonic counters and count-limited objects using a TPM without a trusted OS, in: Proceedings of the first ACM workshop on Scalable trusted computing - STC'06, ACM Press, 2006.

[195] Intel®FPGAs resource center. https://www.intel.com/content/www/us/en/products/programmable/fpga/new-to-fpgas/resource-center/overview.html, [accessed 16 September 2020].

[196] Trusted execution environments and arm trustzone. https://azeria-labs.com/trusted-execution-environments-tee-and-trustzone/, 2020.

[197] Introduction to RDMA (remote direct memory access) [minitool wiki]. https://www.minitool.com/lib/rdma.html, [accessed 16 September 2020].

[198] T. Do, T. Nguyen, H. Pham, Delegated proof of reputation: a novel blockchain consensus, in: Proceedings of the 2019 International Electronics Communication Conference, ACM, 2019.

[199] A. Biryukov, D. Feher, ReCon: Sybil-resistant consensus from reputation, Pervasive and Mobile Computing, 2020; 61:101109. doi:10.1016/j.pmcj.2019.101109.

[200] W. Cai, W. Jiang, K. Xie, Y. Zhu, Y. Liu, T. Shen, Dynamic reputation-based consensus mechanism: Real-time transactions for energy blockchain, International Journal of Distributed Sensor Networks, 2020; 16:1–13.

[201] M. Castro, B. Liskov, Practical Byzantine fault tolerance and proactive recovery, ACM Transactions on Computer Systems (TOCS), 2002; 20:398–461.

[202] J. Ping, Z. Yan, S. Chen, Z. Shen, S. Yang, J. Li, H. Qu, Credit risk management in distributed energy resource transactions based on blockchain, Proceeding of the Chinese Society for Electrical Engineering, 2019; 39:7137–7145. (in Chinese).

[203] H. Chai, S. Leng, K. Zhang, S. Mao, Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles, IEEE Access, 2019; 7:175744–175757.

[204] M. Reynolds, Ransomware attack hits 200,000 computers across the globe. https://www.newscientist.com/article/2130983-ransomware-attack-hits-200000-computers-across-the-globe/, 2017, [accessed 17 August 2020].

[205] S. Gibbs, Child abuse imagery found within bitcoin's blockchain. https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content, 2018, [accessed 5 August 2020].

[206] Blockchain regulations: Recent key developments. https://www.e-zigurat.com/innovation-school/blog/blockchain-regulations-recent-key-developments/, [accessed 5 August 2020].

[207] Cryptocurrency regulations around the world. https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/, [accessed 17 August 2020].

[208] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, C. Weinhardt, Designing microgrid energy markets: A case study: The Brooklyn microgrid, Applied Energy, 2018; 210:870–880. doi:10.1016/j.apenergy.2017.06.054.

Tonghe Wang received his Ph.D. degree in computer science from Georgetown University, Washington, DC, USA, in 2017. He received his bachelor's degree in mathematics and applied mathematics from University of Science and Technology of China, Hefei, Anhui, China. He is currently a Postdoctoral Researcher in the Department of Automation of Tsinghua University, Beijing, China.

His current research interests include distributed computing, energy blockchain and artificial intelligence.

Haochen Hua received his Ph.D. degree in mathmatical sciences in 2016 and Bachelor's degree in mathematics with finance in 2011, both from University of Liverpool, Liverpool, UK. From 2016 to 2019, he was a postdoctoral fellow in the Research Institute of Information Technology, Tsinghua University, Beijing, China. Since 2020, he has been a professor in the College of Energy and Electrical Engineering, Hohai University, Nanjing, China. His current research interests include optimal and robust control theories and their applications in power systems, smart grids, and Energy Internet.

Zhiqian Wei is currently pursuing his Bachelor's degrees in Cyberspace Security and Financial Mathematics, in Shandong University, Qingdao, Shandong, China. His current research interests include blockchain technology and computer system security.

Junwei Cao received his Ph.D. degree in Computer Science from University of Warwick, Coventry, UK, in 2001. He received his Bachelor's and Master's degrees in Control Theories and Engineering in 1996 and 1998, respectively, both from Tsinghua University, Beijing, China.

He is currently a Research Professor of Intelligence Science and Technology Division, Beijing National Research Center for Information Science and Technology, Tsinghua University, P.R. China. He is also an Adjunct Professor of College of Energy and Electrical Engineering, Hohai University, P.R. China. Before joining Tsinghua University in 2006, he had worked as a Research Scientist at MIT LIGO Laboratory and NEC Laboratories Europe for about 5 years. He has published over 200 papers and cited by international scholars for over 18,000 times. He has authored or edited 8 books. His research focuses on distributed computing technologies and energy/power applications.

Prof. Cao is a Senior Member of the IEEE Computer Society and a Member of the ACM and China Computer Federation (CCF).