

Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems

Zhaoyang DONG¹, Fengji LUO², Gaoqi LIANG³



Abstract Modern power systems are rapidly evolving into complex cyber-physical systems. The increasingly complex interaction among different energy entities calls for a secure, efficient, and robust cyber infrastructure. As an emerging distributed computing technology, Blockchain provides a secure environment to support such interactions. This paper gives a prospective on using Blockchain as a secure, distributed cyber infrastructure for the future grid. Firstly, the basic principles of Blockchain and its state-of-the-art are introduced. Then, a Blockchain based smart grid cyber-physical infrastructure model is proposed. Afterwards, some promising application domains of Blockchain in future grids are presented. Following this, some potential challenges are discussed.

Keywords Blockchain, Smart grid, Distributed computing, Energy internet

CrossCheck date: 4 April 2018

Received: 26 March 2018 / Accepted: 4 April 2018 / Published online: 6 July 2018

© The Author(s) 2018

✉ Zhaoyang DONG
zydong@ieee.org

Fengji LUO
fengji.luo@sydney.edu.au

Gaoqi LIANG
lianggaoqi@cuhk.edu.cn

¹ School of Electrical Engineering and Telecommunications, The University of NSW, Sydney, NSW 2052, Australia

² School of Civil Engineering, The University of Sydney, Sydney, NSW 2006, Australia

³ School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen 518172, China

1 Introduction

Human society is facing the critical challenges of climate change, more frequent extreme weathers, energy shortage, and ever-increasing energy demand. These challenges drive the re-construction of the aging energy structure. Since the proposal of “Smart Grid” in the early of 21st Century [1], modern power systems have been revolving towards being more environmentally friendly, efficient, and fault-tolerant. In the last several years, the proposal of “Energy Internet” [2] further drives the integration of different kinds of energy systems and plug-in distributed energy resources. In the authors’ recent work [3], we described an “Energy Ecosystem” vision in the active distribution system side, which is characterized by the intercommunication, interaction, and interoperability of autonomous, heterogeneous energy prosumers.

Ongoing transformation from centralized to distributed generation pattern naturally calls for robust, effective, and secure cyber infrastructures to support the complex communications interactions of the large number of distributed energy entities. A recent technology in the distributed computing paradigm, i.e. Blockchain [4], provides a new promising solution for the cyber infrastructure of next-generation grids. As a distributed computing technology for establishing a reliable, shared ledger through cryptography, consensus mechanism, and smart contract, Blockchain has gained huge successes in the finance field, i.e. the BitCoin system [4]. Its notable features, including decentralized, scalable, non-temperability and security, make it be promising to act as an information and communication backbone of many application domains in future energy systems.

This paper aims to give forward-looking discussions on the potential role of Blockchain in future energy systems.

In this paper, firstly the basic principles and state-of-the-art of Blockchain are introduced (Section 2); then, a conceptual cyber-physical infrastructure model for future grids is proposed (Section 3). Based on it, this paper discusses several promising application domains of Blockchain in future energy systems (Section 4). These conceptual model and application scenarios are likely to provide references to relevant engineers and researchers, and can be used as a road-map for future researches. Potential challenges on the practical deployment of Blockchain in future energy systems are also discussed (Section 5). Finally, conclusion and future work are drawn (Section 6).

2 State of the art of Blockchain

Blockchain, first proposed by Satoshi Nakamoto [4], is designed to achieve peer-to-peer electronic payments directly, without participation of a trusted third party. During the past 10 years, it has been explosively discussed and has shown huge potential in many domains. Essentially, Blockchain is a distributed, redundant, chain-connected, ledger sharing database, in which each node in the network is fault-tolerant and can achieve point-to-point communications. The Blockchain can be categorized into two classes: public chain and generalized private chain. Public chain represents a fully opened network, in which every individual or institution can join and leave freely, and every participant is able to send transactions to others and is scramble for the accounting right. The generalized private chain imposes restrictions on the participant, and it can be further categorized into two types: consortium chain and fully private chain. Consortium chain usually refers to a network that is composed of a few institution-consortiums, and consortiums can cooperate with others but are not fully trusted; the fully private chain is more computationally efficient because it has strict access, read and write permissions.

2.1 Key features of Blockchain

Blockchain is characterized by multiple key features, which are introduced as below.

1) Decentralized

The decentralized structure of Blockchain weakens some functions of traditional centralized organizations. In financial field, a traditional centralized organization usually verifies both buyers' and sellers' information, takes the right to authorize customers to sign terms & conditions, and stores all transaction information. Such centralized operation pattern would lead to some hazards, such as disclosure of user privacy, manipulation of trading

information by cyber attackers, etc. Blockchain provides a new approach to transform such centralized operation pattern to be a decentralized and fully autonomous pattern. In Blockchain, information is verified by all nodes in the network through a certain consensus mechanism, and it is replicated at each node. This process is completely decentralized without a centralized organization.

2) Distributed nodes and storages

Blockchain improves the autonomous and self-management of nodes. The nodes in a Blockchain network are independent individuals or institutions which are often geographically distributed. Based on the networked structure, Blockchain provides a distributed data storage mechanism, in which every node in the network has a copy of ledger. When a new block is generated (which contains one or more data items), it is verified by all nodes, inserted into the ledger, and synchronized among all nodes.

3) Consensus and smart contract

A Blockchain system requires the participation and coordination of distributed nodes to build a trusted fault-tolerant chain-connected network, in which every decision is made based on the agreement of majority nodes, referred to as consensus. Nowadays, different consensus algorithms have been developed, where the most widely-used ones include Proof of Work (PoW) [4] and Proof of Stake (PoS) [5].

The concept of smart contract refers to a set of software codes, which specify the pre-determined execution conditions. The smart contract is often organized as the "if...then..." conditional form. Once the execution conditions are satisfied, the execution of the contract will be automatically triggered without human intervention and third party's supervision.

4) Asymmetric encryption

Since the distributed system is highly autonomous, it is important to use trusted encryption technology to ensure the network security. Asymmetric encryption technology is an integrated part of Blockchain networks. By applying asymmetric encryption, each node is assigned with two keys: ① a public key, which is broadcasted to all nodes in the network and is also used as the owner's ID address; ② a private key, which is kept secret and is also used as the owner's identification.

Applications of asymmetric encryption in Blockchain systems mainly include information encryption and digital signature. In information encryption, the sender node uses the receiver node's public key to encrypt the information, and broadcasts the information to the network; only nodes which hold the receiver's private key can decrypt the information. In digital signature, the sender encrypts a



STATE GRID

STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

message using its private key, and broadcasts the message to the network. The receiver decrypts the message with the sender's public key, to verify that the message is sent by the sender. Many asymmetric encryption algorithms [6] are available, such as SHA256, RIMPE160, RSA, Elgamal, Rabin, D-H, and ECC.

2.2 Existing applications of Blockchain

Blockchain has been attracting increasing awareness in recent years. Many research articles discuss the application prospective of Blockchain in different domains of human society. Reference [7] applied Blockchain to digital supply chain system to achieve disruptive transformation in the network. Reference [8] considered the sensitivity of personal data and the insecurity of third-parties, and proposed a Blockchain based decentralized personal data management system to ensure the privacy preservation of the user's personal data. Reference [9] introduced Blockchain into the robotic swarm system for the purpose of making the robotic swarm operate more secure, flexible and profitable. Reference [10] explored the payment clearing and credit information systems in the banking industry using Blockchain. Reference [11] proposed to build a Blockchain based decentralized record management system for patients to relieve years of heavy regulation and bureaucratic inefficiency in the electronic medical record domain.

The real-world applications of Blockchain concentrate on two domains: finance and energy. In finance domain, the most representative application is the Bitcoin system [4] established by Satoshi Nakamoto. Bitcoin demonstrates a huge success in digital currency. Until now, Bitcoin has

been supported by 10 million users, and the current exchange rate is approximately 1 BTC ~ 10000 USD [12]. Other digital currency systems are also developed to imitate the Bitcoin's operation mode. These systems include Ethereum [13], Litecoin [14], and Coinbase [15]. In addition, many banks are also aware of the potential of Blockchain, and have made strategic plans to incorporate Blockchain into their businesses.

Several pilot projects are being developed to bring Blockchain into the energy field. In Australia, the Power Ledger company [16] aims to use Blockchain to enable residential houses trade redundant solar power with each other. Similar work is also being performed in Germany; the Conjoule company [17] sets up strategic plans to make German homes trade surplus renewable energy through Blockchain. In the United States, the LO3 Energy established the "TransActive Grid" trial project in New York in 2017, using Blockchain to implement peer-to-peer energy trading for ten residential units [18]. In addition, the Share & Charge project [19] is launched to establish an open network for mobility companies to implement private electric vehicle charging pile sharing through Blockchain; this network has been successfully applied in Germany and the United States.

3 Blockchain based cyber-physical infrastructure for future energy systems

In this section, we look into a cyber-physical infrastructure for future energy systems, with the architecture depicted in Fig. 1. Major components of the cyber

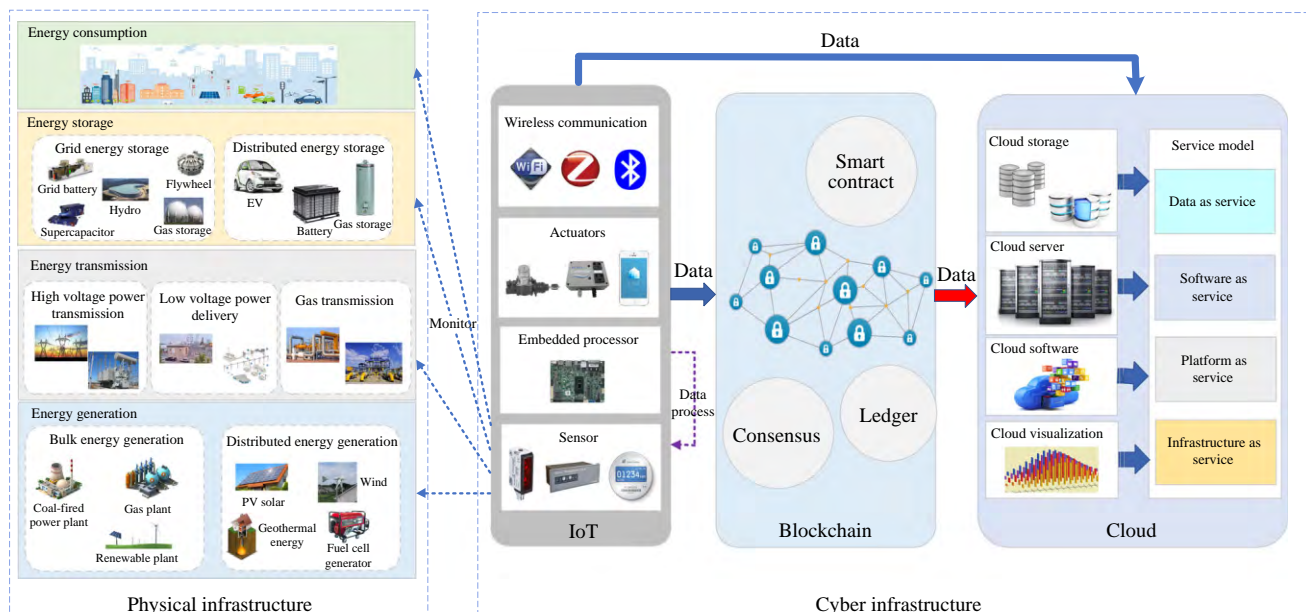


Fig. 1 Cyber-physical infrastructure of future energy systems

infrastructure include: Blockchain based distributed data storage and verification platform, Internet of Things (IoT) based ubiquitous sensing environment, and cloud based multi-dimensional service delivery system. These three parts collaborate together to form the backbone of the cyber infrastructure and support the operation of the physical infrastructure. The physical infrastructure covers energy entities in all energy generation, transmission, and delivery sides.

3.1 Physical infrastructure of future energy systems

The physical infrastructure includes wide-area, heterogeneous energy resources and entities. This physical infrastructure covers all four segments of energy flow: energy generation, transmission, consumption, and storage.

Physical resources in the energy generation segment includes both bulk energy generation plants and distributed generation resources. The bulk plants could include the conventional power plants (coal-fired power plants, pump hydro power plants, hybrid gas plants, etc.) and the renewable power plants (wind farm, solar farm, etc.). The distributed generation resources include the distributed renewable sources, diesel generation units, electric vehicle, etc.

The energy transmission infrastructure includes energy transmission networks with different levels, as well as the energy transmission devices such as transformers, substations, and so forth.

Physical resources in the energy consumption segment comprises of various kinds of energy loads, such as the industrial power load, residential appliances, electric vehicle, building heating system, and so forth.

The energy storage facilities include different kinds of energy storage devices, such as the battery energy storage system, heat storage, super capacitor, hydro pump storage, and so forth. The energy storage devices can be connected with the energy grid at different levels, i.e. the grid side (e.g. grid-connected hydro pump storage and battery energy storage), community/microgrid level (e.g., flywheel and battery energy storages), and end-user level (e.g., residential battery energy storage and electric vehicle).

In addition to the physical resources in energy generation, transmission, consumption, and storage segments, there are other energy entities which are built on top of the physical resources, which are also considered as part of the physical infrastructure. These energy entities include the energy market system, load aggregator, energy retailer, and so forth.

The monitor, control, and coordination of entities of the physical infrastructure should be supported by a robust cyber infrastructure. In the proposed cyber-physical

infrastructure model, the cyber infrastructure is mainly backboned by three technologies as below.

3.2 IoT based ubiquitous computing environment

IoT is a natural outcome of the ubiquitous sensing technology and wireless sensor network. In IoT, many objectives are equipped with microcontrollers, wireless communication interfaces, and suitable protocol stacks that enable them communicate with one another and the users, becoming an integral part of the Internet [20]. In last decades, widely deployments of smart meters and other network sensing devices (e.g. phasor measurement unit (PMU)) has been considered as an application of IoT paradigm in energy system. In the proposed cyber-physical infrastructure, IoT technology will further penetrate into each segment of the energy system, and interact with other components of the cyber infrastructure (Blockchain and cloud). The IoT infrastructure is composed of four parts: ubiquitous sensors and actuators, wireless communication components, and embedded computing processors.

In all four segments of the energy system, IoT facilities will collect multi-dimensional and multi-domain data, which lay foundations to the operation of the Blockchain and cloud systems (discussed later), and support the decision making of various energy stakeholders. For example, in the energy generation side, the IoT infrastructure would collect the operation status and CO₂ emission of the generation units, wind speed, solar radiation, etc.; in the transmission segment, IoT could monitor the energy network condition through the wide-area sensing devices including PMU, supervisory control and data acquisition (SCADA) system, etc.; in the energy consumption segment, IoT could collect the big data including the appliance-level energy consumption data of buildings, environmental condition, transportation network condition, and so forth; in the energy storage segment, IoT could monitor the state-of-charge of the battery energy storage system, the depreciation condition of the energy storage systems, and so on.

The ubiquitous actuating characteristic of IoT enables energy resources to fast respond to external control signals and be controlled in a real-time/near real-time manner. The edge computing capability of embedded processors of IoT devices enable different energy resources be able to perform computing tasks and achieve objectives that are hard to be achieved by centralized management. For example, distributed energy resources can perform data pre-process logics (data consistency checking, noise filtering, etc.) before it is transmitted to a wider environment (e.g., Blockchain and cloud); the distributed energy resources in a certain area can communicate with each other to perform decentralized control decision-making, and so forth.



STATE GRID

STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

3.3 Blockchain based distributed and decentralized processing system

Blockchain provides a decentralized and distributed processing environment to interface the IoT infrastructure. It provides following fundamental services to handle the IoT data and support the interactions of different energy entities.

- 1) Decentralized data storage. Backboned its chain structure and consensus mechanism, Blockchain creates copies of data on networked nodes, and synchronize data through the Internet. The chain structure ensures the data is traceable and non-tamperable; the consensus mechanism ensures the verification and synchronization of data. This provides a secure environment for storing the IoT data to support the upper-level applications. The multiple data copies in the Blockchain can also effectively avoid the single-point failure of the whole system.
- 2) Programmable smart contract. As mentioned before, the smart contract in the Blockchain refer to a set of software codes that specify responsibilities of each contract participant and the execution conditions of the contract. Therefore, Blockchain provides a platform to program smart contracts based different application logics.
- 3) Authorization. The information stored in the Blockchain is traceable and non-tamperable, meaning that it provides a trusted mechanism to do verification and authorization for assets, agreements, intellectual property rights, and so on.

3.4 Cloud based multi-dimensional service delivery platform

IoT and Blockchain form an edge computing environment as a whole. Cloud computing then provides a service-oriented approach to manage the information from IoT and Blockchain. Cloud computing system is backboned by distributed datacenters, which are equipped with servers, storage devices, middleware, and low latency communication failures [21, 22].

In the proposed cyber-physical infrastructure, the cloud system works on top of the IoT and Blockchain. It interfaces the IoT and Blockchain systems, and provides a service-oriented architecture-based interactive environment for energy users and stakeholders. The big data collected by IoT can be stored in Blockchain or uploaded to the cloud, depending on different applications and practical requirements. The cloud can also access the information stored in the Blockchain, and perform application-oriented analysis. Based on the capabilities of hardware

virtualization and dynamic computational resource provision, the cloud system can seamlessly integrate the data and information from the IoT and Blockchain infrastructures, and deliver multi-dimensional services to energy users and stakeholders:

- 1) *Infrastructure as service (IaaS)*. The hardware virtualization technology allows the creation and delivery of virtualized server and storage instances to users. In this way, users can create and access computational instances (servers, data storages, etc.) remotely in the on-demand manner, and operate them just as local resources;
- 2) *Data as service (DaaS)*. Users can transparently access the data in IoT and Blockchain infrastructures through the cloud data service interface and cloud authorization mechanism;
- 3) *Platform as service (PaaS)*. Energy stakeholders can develop various applications on the cloud. For example, the smart contract programs can be implemented through the cloud portal by using the cloud side development tools, and be applied in the Blockchain system.
- 4) *Software as service (SaaS)*. Energy stakeholders can directly access the cloud software and tools through the cloud portal. For example, they can use the SQL or objected-oriented data query languages to query the IoT data based on need; or they can use cloud visualization tools to visualize the data.

In summary, the IoT, Blockchain, and cloud coordinated work together to form a secure, effective, service-oriented, and ubiquitous computing environment, which can well support various application domains in future energy systems.

4 Promising application domains of Blockchain in future energy systems

Taking advantages of the Blockchain's features introduced in Section 2, Blockchain has huge potential to be applied in future energy systems. In this section, we outline some potential application domains as below.

4.1 Data management

Essentially, Blockchain can be regarded as a distributed database system. It creates multiple data copies on networked nodes, and uses a certain consensus mechanism to verify the data. The chain structure of Blockchain can ensure the data to be non-tamperable and traceable. In this sense, Blockchain can support the secure data management in the grid. In this section, we look into two typical grid

data management application scenarios: ① grid data protection; ② smart meter data aggregation.

The first application scenario is the grid data protection, reported in the authors' recent work [23]. Sensor data in the grid side is important to the decision making of higher layer applications, and thus should be safely protected. Currently, the SCADA system provides a centralized data gathering and storage mechanism, which is vulnerable to cyber attackers. In [24], we designed a Blockchain based distributed information gathering and storage mechanism to securely manage the grid sensor data.

Figure 2 shows a reconstructed SCADA network based on Blockchain. Sensors are located in the physical layer; they communicate with each other with wired or wireless channels, forming a distributed communication network. In the network, each meter-node follows a predetermined working mechanism: ① each meter-node collects data of its location, encrypts the data using its private key, and broadcasts the encrypted data to the network; ② other meter-nodes decrypt the received data using their pre-stored public keys, and vote based on an address-based distributed voting mechanism to verify the data. Only when majority of the meter-nodes reach an agreement on the data's validity, can the data be accepted; ③ all accepted data items over a certain period are packaged into a block, which is connected to the existing ledger.

The second application scenario is the smart meter data aggregation. Aggregating meter data can make the system operator aware about the regional electricity consumption and operational condition of the distribution network. It can provide decision-support for various upper level applications, such as network load forecasting, stability analysis, and network planning. However, ensuring the data integrity, security, and privacy in the meter data aggregation process is a non-trivial task.

Figure 3 shows the conceptual framework of a Blockchain based meter data aggregation application. The

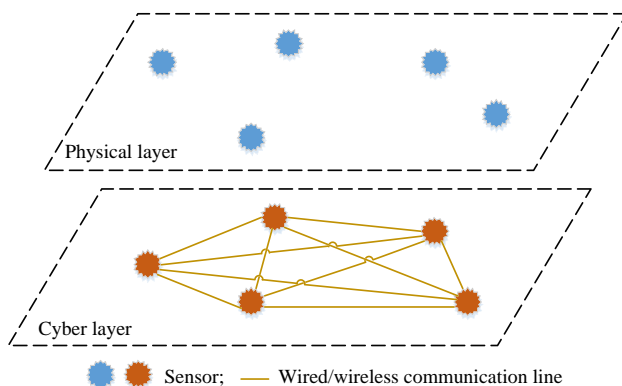


Fig. 2 Structure of the Blockchain based grid data protection mechanism

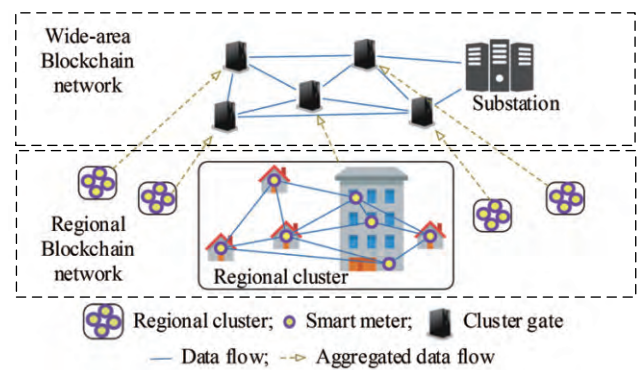


Fig. 3 Schematic of the Blockchain based meter data aggregation framework

system is backboneed by a two-tier hierarchical Blockchain, which consists of multiple regional cluster Blockchains and a wide area Blockchain. A regional Blockchain is a private Blockchain system recording the meter data of units in a certain geographical area. Smart meters are grouped as a cluster, acting as nodes of a regional Blockchain network. The wide-area Blockchain is secured and maintained by the substation and cluster gates which are data repositories or processors for the corresponding clusters. The control center is then allowed to access the wide-area Blockchain through substations, so as to read the aggregated regional smart meter data.

4.2 Open energy market architecture

The huge success of Blockchain in the finance field implies that it also has large potential to re-construct the energy market. The current energy market adopts a centralized trading structure. That is, market participants submit energy trading bids to the market operator, and the latter settles and manages the transactions.

Such centralized structure has three major limitations.

- 1) Firstly, it is vulnerable to the cyber-attack. The 2015 Ukraine blackout [25], the first blackout in the world caused by malicious software, has shown that modern cyber attackers have the capability to break down a national control center. Cyber-attacks against the market control center would lead to breakdown of the market operation, or at least significantly mislead the decision-making of the market operator [23].
- 2) Secondly, the centralized managed market structure makes it difficult to establish an open, cross-border energy market system. In despite of the successful demonstration of the Nordic Energy Market, a cross-border energy trading system for Nordic countries, the trust problem is stiller a major barrier of establishing the cross-border energy market.



STATE GRID

STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

- 3) Thirdly, the centralized market structure is hard to be scaled for accommodating a large number of market actors, especially the small-capacity energy “prosumers (producers-and-consumers)” emerged in the distribution side. In this context, Blockchain can provide fundamentally technical supports to establish open, decentralized, secure energy markets at different levels as follow.

In the grid-level, Blockchain can help to establish the trusted cross-border energy markets. Such markets could be inside of a country (e.g. cross-provincial energy markets) or be transnational. In these systems, the role of market operator is weakened from running the market to be the market supervisor, and there is no third-party regulator is needed to settle the energy transaction. Such secure cross-border energy markets will be beneficial to optimize the energy allocation in wider communities.

In the distribution network side, Blockchain can be harnessed to construct the decentralized energy market for autonomous energy entities (buildings, microgrids, load aggregators, small-capacity renewable power plant, etc.). Such market can be with a two-layer structure, depicted in Fig. 4. In the upper layer, a certain energy trading negotiation mechanism is desired to enable prosumers negotiate the amount and price of the energy trading; in the lower layer, Blockchain can be used to enable the secure and trusted settlement of transactions agreed in the first layer. Such market mechanism could improve the energy efficiency and foster the economics of the energy distribution side.

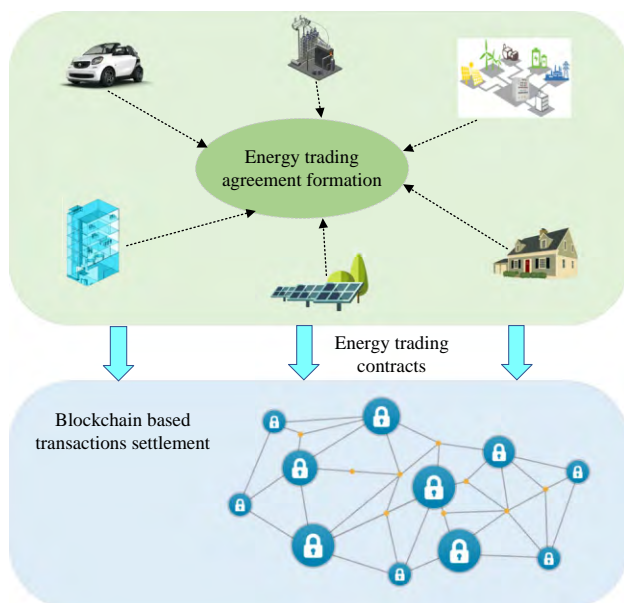


Fig. 4 Schematic of the energy trading system in the distribution side

4.3 Wide-area energy resource management

As a distributed computing technology, Blockchain provides a mechanism for data synchronization and trusted information recording. This can help the utility to manage wide-area energy resources to achieve grid-level objectives. As an example, in this section we look into a Blockchain based direct load control (DLC) framework, which uses Blockchain to coordinate the communication between the distribution company (DISCO) and distributed energy consumers and producers, with the aim to achieve the grid peak load reduction.

In the proposed DLC framework, each energy consumer or producer has an immutable private ledger in the Blockchain that contains all its transactions (i.e. communications) and contracts with other nodes or the DISCO. The DLC process is launched by DISCO to create a load control transaction, and is featured with following procedures:

- 1) Contract formation. Firstly, the energy user and DISCO agree with the DLC by signing a contract. The DISCO generates and signs a load control transaction, in which the DLC contract is put in the metadata field encrypted with the public key of the customer. Then, this transaction is broadcast to all nodes. On receiving the transaction, the customer signs his part and broadcasts the transaction again so that it can be stored in the Blockchain.
- 2) Load data collection. Based on the contract, the DISCO generates genesis transaction for monitoring the status of each load in the energy user side. On receiving the genesis transaction, the load sends its status data to the DISCO using single signature DR transaction.
- 3) DLC control action determination. Based on the collected load data, the energy management system of DISCO determines load control actions.
- 4) Load control action delivery. The DISCO informs control actions to actuators in the user side by generating a multi-signature load control transaction and broadcasting to the Blockchain network.
- 5) Perform load control. On receiving the load control transaction generated by the DISCO, actuators in the user side apply control actions.

Above coordination process is depicted in Fig. 5.

4.4 Authentication

Blockchain can be used as an automatic and trusted system to provide authentication services for energy stakeholders. A typical application would be the carbon emission quota authentication. The concept of carbon

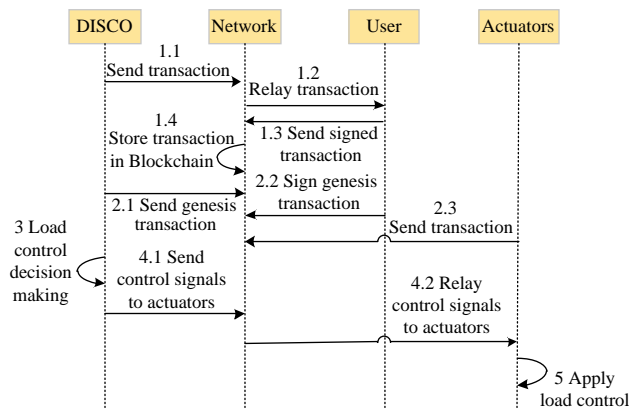


Fig. 5 Coordination diagram of the Blockchain based DLC process

emission quota was set up by the Kyoto Protocol in 1997. The carbon emission quota is an allowance assigned to an energy entity based on the evaluation of the possible carbon emission that would be produced in the production activities of the entity. The carbon emission quota can be traded among different energy entities through a certain market mechanism. Currently, many countries have established the carbon emission quota trading market, such as China, Korea, and European Union.

By using Blockchain, the carbon emission quota trading can be performed in a trusted and secure way. The quota assigned to an energy entity can be authenticated automatically and recorded in the Blockchain, making it trusted and non-tamperable. According to the carbon emission produced by the entity, Blockchain facilitates the quota trading by recording all transactions in traceable ledgers.

In addition to the carbon emission quota authentication, Blockchain can also provide authentication services for other objects, such as the energy asset authentication, demand response credit authentication, etc.

5 Challenges

Although Blockchain shows huge potential to be a secure, distributed cyber infrastructure solution for future energy systems, there still are potential limitations and practical challenges existed.

1) Information redundancy

Blockchain creates multiple data copies on networked nodes, which can support the secure data management in the grid. However, it also generates redundant information. Individual nodes have to participate in every transaction's verification process, and thus would take extra storage space and consume more power. Moreover, it would be convenient for cyber attackers to launch a targeted cyber-

attack on just one node to understand the whole network's dynamic information. There are reasons to believe that Blockchain-targeted computer viruses or attacks will emerge in future. Therefore, applying Blockchain to future energy systems requires more effective technologies to relieve the information redundancy issue.

2) Performance scalability

As a peer-to-peer system, Blockchain makes an inherent tradeoff between decentralization and system performance. Typical Blockchain systems process transactions at a speed which is one or several magnitude slower than their centralized counterparts. Unlike other distributed systems, adding more computing nodes into a Blockchain network might not increase the throughput of the network. Depending on the consensus protocol, adding more nodes could even significantly slow down the system. Currently, the academia and industry are working on designing new consensus protocols to mitigate this scalability problem.

3) Security of smart contract

Smart contracts are essentially programs written by human. As a result, they may contain design flaws and bugs. In the software industry, a common practice to address these flaws and bugs is to release software upgrades or bug fixing patches. However, the immutable and irreversible natures of Blockchain make this process cumbersome and inefficient, if not impossible. Moreover, smart contracts usually deal with valuable digital assets directly, which makes them attractive targets to exploit. Verification tools should be developed and utilized to detect design flaws and bugs in smart contracts before the actual deployment. Additionally, sound update mechanism and emergency plans should be designed at the beginning stage instead of as an afterthought.

4) Coordination of Blockchain with other parties

Adopting Blockchain in future energy systems is not so straightforward as it will require non-trivial efforts to coordinate Blockchain with other information infrastructures, including IoT, cloud, etc. Cloud resources and IoT devices are usually with limited bandwidths, while Blockchain protocols often produce significant computer network traffics. This implies issues on the compatibility of Blockchain and other information technologies. More importantly, the implementation of Blockchain based applications requires the cooperation of different functional energy organizations (independent system operators, energy retailers, distribution companies, energy users, etc.), which is also a non-trivial work.

5) Integration of Blockchain and energy physical infrastructure



STATE GRID

STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

In the cyber layer, Blockchain and smart contract ensure the security and timelessness of energy trading. However, the changed energy allocations caused by the trading would affect the energy flows in physical grids, which would consequentially result in some problems, such as network congestion and overloading, voltage deviation, etc. Therefore, corresponding solutions need to be developed to coordinate the cyber and energy physical infrastructures and ensure the secure, reliable, and efficient operation of energy grids.

6 Conclusion

This paper discusses the prospective of Blockchain technology in future energy systems. A comprehensive cyber-physical infrastructure prototype is proposed, which is backboned by IoT, Blockchain, and cloud. Several promising application domains of Blockchain in future grids are presented, and potential challenges are discussed. In summary, Blockchain's characteristics of decentralized, scalable, secure, trusted, and non-tamperable make it has large potential to play important role in future energy systems with other advanced ICTs.

The authors are currently working on implementing the applications presented in this paper. In future, more energy-related application scenarios are expected to be explored on Blockchain.

Acknowledgements This work was supported by the Australian Research Council Discovery Projects (Nos. DP170103427, DP180103217). The authors acknowledge Mr. Ali Dorri at The University of New South Wales, Australia for his valuable comments on the Blockchain and communication networks; the authors also acknowledge Dr. Yang Chen from the Microsoft Asia for his comments on Blockchain.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- [1] Amin SM, Wollenberg BF (2005) Toward a smart grid: power delivery for the 21st century. *IEEE Power Mag* 3(5):34–41
- [2] Huang A, Crow M, Heydt G et al (2011) The future renewable electric energy delivery and management (FREEDM) system: the energy internet. *Proc IEEE* 99(1):133–148
- [3] Dong ZY, Luo F, Lai J et al (2017) Data-centric energy ecosystem in active distribution networks. *Southern Power System Technology* 11(10):45–61
- [4] Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>. Accessed 31 October 2008
- [5] King S, Nadal S (2012) PPCoin: peer-to-peer crypto-valuta met proof-of-stake. <https://peercoin.net/assets/paper/peercoin-paper-nl.pdf>. Accessed 19 August 2012
- [6] Ebrahim M, Khan S, Khalid U (2013) Symmetric algorithm survey: a comparative analysis. *Int J Comput Appl* 61(20):12–19
- [7] Korpela K, Hallikas J, Dahlberg T (2017) Digital supply chain transformation toward Blockchain integration. In: *Proceedings of the 50th Hawaii international conference on system sciences*, Hawaii, USA, 16 January 2017, 10 pp
- [8] Zyskind G, Nathan O, Pentland A (2015) Decentralizing privacy: using Blockchain to protect personal data. In: *Proceedings of the 2015 IEEE security and privacy workshops*, San Jose, USA, 21–22 May 2015, pp 180–184
- [9] Ferrer EC (2017) The Blockchain: a new framework for robotic swarm systems. *arXiv Preprint*. arXiv: 1608.00695
- [10] Guo Y, Liang C (2016) Blockchain application and outlook in the banking industry. *Financ Innov* 2(24):1–12
- [11] Azaria A, Ekblaw A, Vieira T et al (2016) MedRec: using Blockchain for medical data access and permission management. In: *Proceedings of the international conference on open and big data*, Vienna, Australia, 22–24 August 2016, pp 25–30
- [12] Blockchain/Bitcoin Charts. <https://blockchain.info/charts/market-price>. Accessed 25 February 2018
- [13] Ethereum. <https://www.ethereum.org/>. Accessed 13 March 2018
- [14] Litecoin: open source P2P digital currency. <https://litecoin.com/>. Accessed 13 March 2018
- [15] Coinbase: buy/sell digital currency. <https://www.coinbase.com/?locale=en>. Accessed 13 March 2018
- [16] Power ledger: a decentralised energy marketplace. <https://web.powerledger.io/>. Accessed 13 March 2018
- [17] Conjoule: our shared energy future. <http://conjoule.de/en/home/>. Accessed 13 March 2018
- [18] LO3 energy: the future of energy. <https://lo3energy.com/>. Accessed 13 March 2018
- [19] Share and charge. <http://shareandcharge.com/en/>. Accessed 13 March 2018
- [20] Buyya R, Broberg J, Goscinski A (2011) Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener Comput Syst* 29:1645–1660
- [21] Luo F, Dong ZY, Chen Y et al (2012) Hybrid cloud computing platform: the next generation IT backbone for smart grid. In: *Proceedings of the IEEE PES general meeting*, San Diego, USA, 22–26 July 2012, 7 pp
- [22] Luo F, Zhao J, Dong ZY et al (2016) Cloud-based information infrastructure for next-generation power grid: conception, architecture, and applications. *IEEE Trans Smart Grid* 7(4):1896–1912
- [23] Liang G, Weller SR, Luo F et al (2017) Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism. *IEEE Trans Smart Grid*. <https://doi.org/10.1109/TSG.2017.2677911>
- [24] Liang G, Weller SR, Luo F et al (2018) Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Trans Smart Grid*. <https://doi.org/10.1109/TSG.2018.2819663>
- [25] Liang G, Weller S, Zhao J et al (2016) The 2015 Ukraine blackout: implications for false data injection attacks. *IEEE Trans Power Syst* 32(4):3317–3318

Zhaoyang DONG obtained his Ph.D. degree from the University of Sydney, Australia in 1999. He is with the University of NSW,

Sydney, Australia. He was previously professor and Head of School of Electrical and Information Engineering, the University of Sydney, and Ausgrid Chair and Director of the Ausgrid Centre for Intelligent Electricity Networks (CIEN). He also worked with Transend Networks (now TASNetworks) as manager for system planning. His research interests include power system stability and planning, smart grid/microgrid, renewable energy systems, computational intelligence, and distributed computing for power and energy systems. He is a Fellow of IEEE, and editor for IEEE Transactions on Smart Grid, IEEE PES Letters and IET Renewable Power Generation. He is an international advisor for Automation of Electric Power Systems journal.

Fengji LUO received the B.S. and M.S. degrees in software engineering and computer science from the Chongqing University, China, in 2006 and 2009, respectively. He received the Ph.D. degree in electrical engineering from the University of Newcastle, Australia, in 2013. Currently, he is an Early Development Fellow of the School of Civil Engineering, The University of Sydney, Australia. He also held academic positions with the Hong Kong Polytechnic University, the Centre for Intelligent Electricity Networks, The University of

Newcastle, Australia, and the University of New South Wales, Australia. His research interests include the renewable energy, demand side management, and computational intelligence and its applications in smart grid. He has published over 100 papers on referred journals and conferences. He received the 2015 Pro Vice Chancellor's Award for Research Excellence of The University of Newcastle, Australia; and was awarded the ATSE "2016 Australia-Japan Emerging Research Leader".

Gaoqi LIANG obtained the B.E. degree in automation from the North China Electric Power University, Baoding, China, in 2012, and the Ph.D. degree in electrical engineering from the University of Newcastle, Australia, in 2017. She is currently a postdoctoral fellow with the Chinese University of Hong Kong, Shenzhen, China. Her research interests include cyber-attacks on the modern power system, smart grid and its cyber physical security, data quality and its assessment and improvement, and electricity market.



STATE GRID

STATE GRID ELECTRIC POWER RESEARCH INSTITUTE