This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks

Gaoqi Liang, *Member, IEEE,* Steven R. Weller, *Member, IEEE,* Fengji Luo, *Member, IEEE,* Junhua Zhao, *Senior Member, IEEE,* and Zhao Yang Dong, *Fellow, IEEE*

***Abstract* —The cyber security of modern power systems has drawn increasing attention in both academia and industry. Many detection and defense methods for cyber-attacks have therefore been proposed to enhance robustness of modern power systems. In this paper, we propose a new, distributed blockchain-based protection framework to enhance the self-defensive capability of modern power systems against cyber-attacks. We present a comprehensive discussion on how blockchain technology can be used to enhance the robustness and security of the power grid, by using meters as nodes in a distributed network which encapsulates meter measurements as blocks. Effectiveness of the proposed protection framework is demonstrated via simulation experiments on the IEEE-118 benchmark system.**

***Index Terms*—Blockchain, Modern power systems, Cyber-attacks, Distributed network, False data injection attacks**

I. INTRODUCTION

MODERN power systems have experienced a profound evolution to facilitate social development. Unlike conventional power systems, the infrastructure of modern power systems relies strongly on advanced communication and control technologies [1]. While this technological trend on the one hand provides new opportunities to optimize the energy efficiency of the grid, it also imposes significant requirements and challenges on the robustness, efficiency, and security of the underlying information infrastructure [2]. These advances have been driving modern power systems towards becoming complex cyber-physical systems. However, due to the deep integration of both cyber and physical resources, attacks from the cyber layer have the potential to mislead decision-making in the control center and cause system disturbances, financial loss, or even more serious consequences, e.g., blackouts. In this sense, data vulnerability has become an unneglectable issue, as evidenced by malicious events caused by cyber-attacks, a recent high-profile example of which was the 2015 Ukraine blackout [3-5].

As a representative cyber-attack, the false data injection attack (FDIA) [6-8] manipulates system data to mislead the control center without being detected by the bad data detection module. Many studies [9-13] have demonstrated the impacts of FDIAs on modern power systems. In real situations, the system security could be threatened by not only FDIAs but also many other kinds of cyber-attacks, such as denial of service (DoS) attacks, data framing attacks, and cyber topology attacks [14-17]. Therefore, ensuring the integrity and consistency of data is of critical importance for the secure and economical operation of the grid.

Many methods have been proposed to detect and defend against cyber-attacks based on existing centralized data communication and storage mechanisms [18]-[19]. However, existing communication and storage of meter measured data mechanism in modern power systems are less than fully effective against cyber-attacks, even if some meters are upgraded to phasor measurement units (PMUs). These PMUs are susceptible to cyber-attacks due to their reliance on the global positioning system (GPS) measurement mechanism [20] [21], not to mention the high capital cost of using PMUs.

Given the geographical distribution of meters/sensors in modern power systems, enhancing the self-defensive capabilities of such systems against cyber-attacks calls for the adoption of state-of-the-art developments in distributed system security technologies [22-24]. In this sense, the distributed power system can be considered not only as a network of distributed generation, energy storage and energy management, but also a distributed advanced measurement infrastructure (AMI) network [25] [26] including distributed data acquisition, information monitoring and knowledge storage, on both system side and demand side.

Blockchain, first proposed in 2008 [27], is designed to achieve peer-to-peer electronic payments directly, without participation of a trusted third party. In blockchain, all peers form a distributed network. Each peer acts as a node of the network and can participate in calculating the solution to a

This work is partially supported by a China Southern Power Grid research grant (WYKJ00000027) and partially supported by a Visiting Scholarship of State Key Laboratory of Power Transmission Equipment & System Security and New Technology (Chongqing University, China) (2007DA10512716401), and Shenzhen Municipal Science and Technology Innovation Committee project (GJHZ20160301165723718) and (JCYJ20170410172224515).

G. Liang and J. Zhao are with the Chinese University of Hong Kong, Shenzhen, Guangdong, China (e-mail: lianggaoqi@cuhk.edu.cn; junhua.zhao@outlook.com).

S.R. Weller is with the School of Electrical Engineering and Computing, University of Newcastle, Callaghan, NSW, 2308, Australia (e-mail: steven.weller@newcastle.edu.au).

F. Luo is with the School of Civil Engineering, University of Sydney, Sydney, NSW, 2006, Australia, and also with the State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University, China (e-mail: fengji.luo@sydney.edu.au).

Z.Y. Dong is with the Electric Power Research Institute, CSG, Guangzhou, China, and also with the School of Electrical Engineering and Telecommunications, University of New South Wales, NSW 2006, Australia (e-mail: joe.dong@unsw.edu.au).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

hash-based mathematical problem ensuring integrity of transactions. Each transaction record is encapsulated as a block and added onto the existing block chains. The recorded block contents are collectively referred to as the *ledger*. All information is then updated synchronously to the entire network so that each peer keeps a record of the same ledger.

In the literature, practical applications of blockchain technology are mostly concentrated in the financial domain, such as virtual currency, cross-border payment and settlement, bills and supply chain finance, securities issuance, and transactions. The Bitcoin system [28] is the most prominent application of blockchain technology, which maintains a global, distributed ledger for peer-to-peer transactions, and runs a consensus algorithm on a large number of distributed computers. Since its release in January 2009, Bitcoin has been supported by 10 million users, and the current exchange rate is approximately 1 BTC ~ 10,000 USD [29]. Other financial companies (e.g., Ethereum [30], Coinbase [31], Ripple [32], Chain [33], Circle [34], and so forth) have been established in recent years. Moreover, Storj [35], an end-to-end cloud storage network, and Factom [36], a distributed record keeping system, have also been proposed as emerging blockchain-based business models. Applications of blockchain in other domains are still in the early stages. The application of blockchain in robotic swarm system was studied by Ferrer [37], in which global knowledge is maintained within the swarm. In this application, blockchain provides a more secure, flexible control environment for swarm robots. Sharples and Domingue [38] proposed to store education information records in blockchains in such a way to conveniently record and verify each person's identity. In energy systems, Aitzhan and Svetinovic [39] proposed to build a token-based, decentralized energy trading system using blockchain. In their system, multi-signatures and anonymous encrypted message propagation streams are used to secure the energy trading transactions. Dorri *et al.* in [40] [41] analyzed the challenges and solutions of blockchain in Internet of Things (IoT) and proposed a method for the application of blockchain on a smart home environment.

Distinct from the existing literature, this paper proposes a distributed, blockchain-based data protection framework. Mainly contributions are as follows：

(1) The proposed framework substantially increases the self-defensive capabilities of modern power systems against data manipulation by cyber attackers. In conventional power systems, an attack is deemed successful if cyber attackers tamper with meter measurement data locally, replace data packages transmitted to the control center via a communication channel, or hacks into control center. In the proposed framework, an attack does not result in a successful manipulation unless an attacker tampers with (or replaces) data packages on a *majority* of channels; or hacks into sufficient meters to manipulate data.

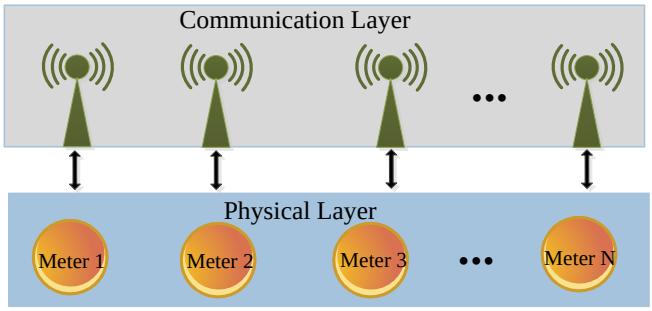


Fig. 1. Blockchain based Reconfigured SCADA Network

(2) The proposed framework is consensus-based, and exploits particular characteristics of the power grid environment, details of which will be explained in the following sections. The proposed approach therefore stands in marked contrast to conventional power system data defense countermeasures.

This paper is organized as follows. Section II presents the system infrastructure needed for the proposed distributed blockchain-based data protection framework. Section III presents the working mechanism of the proposed framework. Section IV presents a performance analysis which includes Blockchain technology innovation/comparison, potential disadvantages and practical challenges, and efficiency evolution. Section V presents a case study based on the proposed framework. Finally, conclusions are drawn in Section VI.

II. System Infrastructures of the Distributed Blockchain based Data Protection Framework

There are typically three basic processes for the supervisory control and data acquisition (SCADA) module in modern power systems: data gathering at remote terminal units; plaintext transmission via a communication channel to the control center; and information storage in the control center [1]. The current information-gathering and storage mechanism provides centralized management but with high risks of data being manipulated by cyber attackers. The proposed framework greatly reduces the risk of data being successfully manipulated by providing a distributed information gathering and storage mechanism. Consequently, some system infrastructure must be updated or replaced to facilitate the working mechanism of the proposed framework. In this section, we detail the system infrastructure required for the proposed blockchain-based data protection framework.

A. Reconfigured SCADA Network

In the proposed framework, a reconfigured SCADA network is used to gather, transmit and store data. The overall power system layers are as usual, but with a different SCADA network in which each meter is assembled by data collection device, signal sender, signal receiver, and data process device. The physical layer and communication layer is shown in Fig. 1. The operations in both energy management system (EMS) and market management system (MMS) are supported by the collected information from the physical layer. The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

communication layer in the proposed system is isolated from the Internet.

In the reconfigured SCADA network, data acquisition modules still collect real-time measurements from the grid, including voltage, current, real and reactive power flow, breaker status, transformer tap position, and so forth [10]. Geographically distributed meters/sensors form a distributed meter-node network, in which each meter/sensor acts as a node. We assume that the graph corresponding to the meter-node network is *connected*, i.e., there is a communications path linking each distinct pair of nodes. Only meters/sensors which are authorized by the grid can perform data acquisition functions. In this sense, the meter-node network is interdependent, and can be considered as a private blockchain network. More importantly, interactions among the nodes in the network are automatically performed based on a certain consensus mechanism, without any human intervention. This is significantly different from the Bitcoin system, in which transactions are launched by humans.

B. *Key Features of Meters*

In order to interact with each other through the proposed blockchain framework (details of which will are discussed in the next section), each meter needs to be possess functional features which are not common in today's widely deployed meters. We summarize these required features as follows:

- Each meter is identified by a unique address;
- Each meter is equipped with specific software to support the generation of a public key and private key;
- Each meter is equipped with RAM, computational hardware, data collection device, signal sender, signal receiver and data process device; and
- Meters are capable of communicating with each other through wired or wireless communication channels.

The above characteristics imply that it will be necessary to upgrade the existing metering infrastructure to some extent.

III. Working Mechanism of the Distributed Blockchain Based Data Protection Framework

In the proposed framework, all collected data are eventually stored in a *ledger* in the form of connected blocks which exists in distributed form in each meter's memory. Before storage, each of the following procedures are necessary to guarantee data accuracy: data broadcast; data verification via voting mechanism; data content accumulation in block, mining process; verification the mining result via voting mechanism; and distributed ledger synchronization. In this section, we show in detail of the working mechanism of the proposed framework, which consists mainly of data transmission, verification, and storage.

A. *Data Encryption and Broadcast*

Each meter-node in the network is assigned a public key and a private key. The public key is the node's main accessible information that is publicly available in the meter-node network. The private key is the node's private information that is used to validate a node's identity and the operations that it may perform. Since it is a distributed blockchain-based network, the data collected by each node must be encrypted and then broadcast to other nodes. The data encryption and broadcast processes are illustrated in Fig. 2.

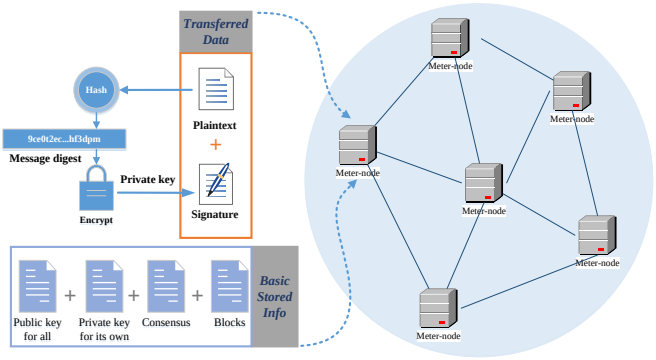


Fig. 2. Data Encryption and Broadcast Process

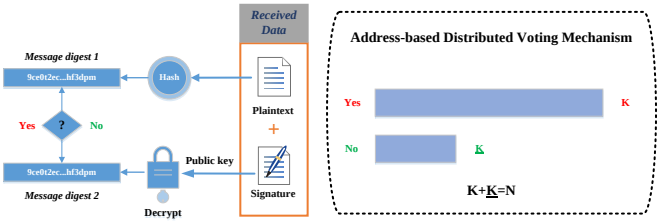


Fig. 3. Data Decryption and Verification Process

Data within each meter-node is comprised of basic stored information and transferred data, as shown in Fig. 2. The basic stored information within each meter-mode consists of the public keys of all meter-nodes, the private key of that meter-node, and preset consensus and accumulated blocks. The transferred data (for broadcast to other nodes) consists of plaintext and signatures. In the data encryption process, newly collected plaintext data is processed using a secure hash algorithm (SHA), generating a *message digest*. The private key of each meter-node is used to encrypt the message digest of that node, thereby forming a digital signature which can be decrypted using its public key. The transferred data is then broadcast to all other meter-nodes via the communication network.

B. *Data Decryption and Verification*

All meter-nodes which receive broadcast information need to decrypt the received data and verify the results. As shown in Fig. 3, the receiver hashes the received plaintext into *message digest 1*, and decrypts *message digest 2* from the digital signature by using the sender's public key. If *message digest 1* equals *message digest 2*, the received information is successfully verified; otherwise the received data is considered as false. Data integrity and consistency issues exist in the broadcasting process. That is, the transferred data might be tampered with, delayed, or even discarded, creating inconsistency between *message digests 1* and *2*.

In the proposed framework, all nodes use an *address-based distributed voting mechanism*, i.e., each node has precisely one chance, to verify the integrity and consistency of the received data. As shown in Fig. 3, only once positive agreement is reached among the nodes, is the data recognized as correct.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

Table I
MEANINGS OF THE ATTRIBUTES

Items	Meaning
Block number	The sequent number of the current block, which is used as the title of the block.
Data content	All encapsulated data for the current block
Timestamp	The time when the last verified data is encapsulated into the current block
Previous hash result	The hash result of the previous block
Hash result	The hash result of the current block
Nonce solution	The solution of the puzzle problem for the current block

Considering an N meter-node network, each node votes on its verification result. Denote the number of the most votes by K (the remaining amount is K), where $K \le N$. Only when the following criterion is satisfied is the data accepted:

$$\frac{K}{N} > \tau \tag{1}$$

where τ is a threshold whose value must be strictly greater than 50% to ensure that the voting result of the accepted data is in agreement at the majority of nodes. Consequently, all verified data over a certain period are packaged as a block to be connected to the previous ledger.

C. Mining and Generation of Blocks

All stored information in the distributed blockchain network is cryptographically linked block by block. Many secure hash algorithms (SHAs), such as SHA-1, SHA-256, SHA-384 and SHA-512 [43] [44], can be applied to solve the problem of condensing the message in the current block to produce a message digest. These SHAs are iterative, one-way hash functions, with different functions generating different structures and dimensions of the message digest.

Hash functions have unique properties that can connect blocks cryptographically. Firstly, the hash function is hard to invert, i.e., it is computationally infeasible to find the input message based on the corresponding output message digest. Secondly, it is computationally infeasible to find two different messages that produce the same message digest. Thirdly, any changes to a message will (with overwhelming probability) result in a different message digest [45].

In the following, we use the SHA-256 function to explain the mining and blockchain ledger generation mechanism of the proposed framework. The SHA-256 hash function has intermediate computational complexity and is applied in Bitcoin system. However, other hash functions can be also easily integrated into the framework.

In the blockchain network, each block has the following attributes: block number, data content, timestamp, previous hash result, hash result, and nonce solution. The meanings of the attributes are shown in Table I.

SHA-256 uses logical functions to output 32-bit words with elements from {0, 1,…, 9, A, B,…, F}, which include two steps: pre-processing step and hash computation step.

In the pre-processing step, all related information is summarized as follows:

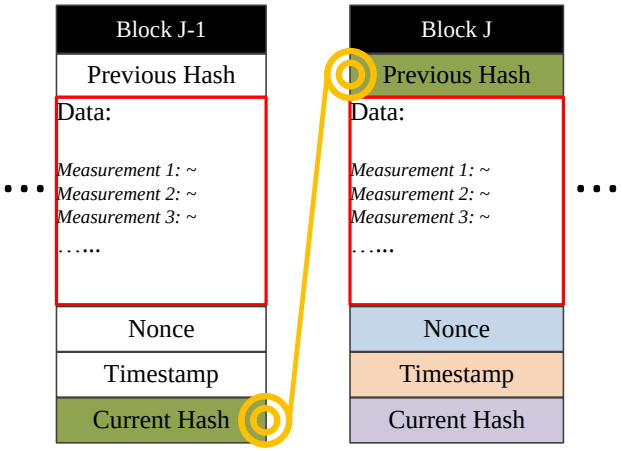


Fig. 4. Block Contents and Chain Connections

$$S = b + d + t + hp + nonce \tag{2}$$

where b represents the block number; d represents the data content; t represents the time point; hp represents the previous hash result; $nonce$ represents the random number; and S represents the overall message.

Suppose all measurement data over a certain period have been verified and packaged into the data content of the J-th block. Then, based on the data content of the J-th block, the hash value of the $(J-1)$-th block, and the current timestamp, some meter-nodes solve a puzzle problem to find an appropriate nonce in such a way to output the hash result for the J-th block. This process is referred as *mining*, and the meter-nodes which participate in mining are referred as *miners*.

The generation of the puzzle problem is in the hash computation step. In the hash computation step, SHA-256 is applied twice on the input message, i.e., S shown in Eq. (2), as an extra security layer to produce the message digest, shown as:

$$FinalHash = hash(SHA256, hash(SHA256, S)) \tag{3}$$

The puzzle problem is to find the appropriate nonce value to make the $FinalHash$ value less than a given target, T, shown as:

$$FinalHash \le T \tag{4}$$

Brute force is the only known way to solve the puzzle problem and it is therefore highly computational intensive. The computational difficulty of problem solving depends on the value of T, which can be decided in different implementations. The smaller the value of T, the more difficult it is to generate the appropriate nonce value.

Some (or even all) nodes can operate as miners by attempting to solve the puzzle problem independently. Once the first miner finds the nonce, it broadcasts the value to other nodes to let them check whether the solution is correct by validating whether it satisfies constraint (4) or not. Then, the *address-based distributed voting mechanism* is used again to vote on the verification result. The result is tested by Eq. (1), which ensures that only if there are enough nodes agreeing on the nonce value, is the current block allowed to cryptographically connect to the previous ledger. Consequently, all distributed ledgers are updated synchronously, and all nodes move on to the procedures of the next block. Finally, the blocks are linked as illustrated in Fig. 4.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

It should be noticed that in the proposed framework, mining is a competition among all miners, while there is no reward as an incentive for miner who solves the puzzle problem first. All nodes are strictly driven by the consensus; and all miner behaviours are pre-programed and automatically generated.

D. Consensus Mechanism

The consensus mechanism, also known as the distributed protocol or smart contract, is a network rule that every node follows. Besides the working mechanism—which is automatically implemented by every node—there are specific rules for the framework in a power system context. The consensus in the proposed framework has the following representative characteristics.

1) Setting of Public/Private Key Update Frequency

As shown in Fig. 2, each node has all other nodes' public keys in addition to its own private key. If public and private keys are stolen by an adversary, it would be challenging for the network to prevent data from being manipulated by cyber attackers. Regular update/replacement on key information is therefore an effective method of enhancing security.

Consider an *N*-meter network, and suppose that the estimated average time for the attacker to steal the public and private key of the *i*-th node is t_i, $i = 2,3,...,N$, where $t_i > 0$. Suppose the t_i is sorted in increasing order, i.e., $t_{i-1} < t_i$, where $i = 2,3,...,N$. From Eq. (1), we know that in order to tamper with measurement data when data is in transmission, the minimum number of stolen pairs of public and private keys on nodes should satisfy $K > \tau \cdot N$; and thereafter, $K = ceil(\tau \cdot N)$, where $ceil(\cdot)$ denotes rounding up to the nearest integer. Therefore $\bar{\Psi}$, defined as the required time for an attacker to steal key information from all *K* nodes, satisfies the following inequality:

$$t_K \le \bar{\Psi} \le \sum_{i=1}^{K} t_i \tag{5}$$

where $t_K = \max\{t_i\}, i = 1,2,...,K$. Thus $t_K \le \bar{\Psi}$ represents the scenario in which an attacker steals the key information from *K* nodes simultaneously, while $\bar{\Psi} \le \sum_{i=1}^{K} t_i$ represents the scenario in which an attacker only has the capability of stealing a single key at a time. Therefore, the key update frequency for the network, denoted as Ψ, should be selected to satisfy $\Psi < t_K$.

2) Block Generation

Since each block contains several measurements, data content accumulation in each block is therefore a necessary procedure in the block connection process. If one block accumulates excessive measurement data, this process could take sufficiently long that higher layer applications in EMS, such as state estimation, would be adversely impacted. Conversely, too frequent mining is a computational burden for the blockchain system. We propose the following two strategies as solution methods.

Strategy 1: Generating Block by Fixed Time

In this strategy, each block is generated at a fixed time interval. Each block then contains the verified measured data within that interval. Once a block is generated, the mining work starts. The unverified data is packaged into the next block. The setting of the time interval for the block generating can be different for different power systems.

For an *N*-meter network, let α denote the time interval of block generation, let β denote the average number of measured data items in each block, and let Φ denote the system state estimation time interval. The setting of α should satisfy the following two constraints:

$$\alpha < \Phi \tag{6}$$

$$\beta \cdot floor(\frac{\Phi}{\alpha}) \ge N \tag{7}$$

where constraint (6) restricts the block mining time interval to be strictly less than the state estimation time interval. This is because all collected measurements should be used in the state estimation module to calculate the whole system's statuses. Constraint (7) ensures that all measurement data have been well stored in the chain before the next round of state estimation, where $floor(\cdot)$ denotes rounding down to the nearest integer.

Strategy 2: Generating Blocks by Fixed Size

In this strategy, each block is generated so as to have the same block size, i.e., each block contains the same number of verified data items. Therefore, in this strategy, the generating time interval between two blocks is variable.

For an *N*-meter network, let $\bar{\beta}$ denote the block size (measured by the number of data items), let $\bar{\alpha}$ denote the average time interval between two blocks, and let Φ denote the system state estimation time interval. The setting of $\bar{\beta}$ should satisfy the following two constraints:

$$\bar{\alpha} < \Phi \tag{8}$$

$$\bar{\beta} \cdot floor(\frac{\Phi}{\bar{\alpha}}) \ge N \tag{9}$$

where the physical meanings of constraints (8) and (9) are similar to the constraints (6) and (7), respectively.

3) Miner Selection

The other major problem is the selection of meter-nodes to solve the puzzle problem in the mining process. Since miners must be equipped with substantial computational capability in such a way to rapidly obtain puzzle solutions, this requirement therefore potentially implies high investment costs. We propose the following two strategies as alternatives.

Strategy 1: Pre-Specified Nodes as Miners

In this strategy, some nodes are pre-specified to act as miners, and are responsible for solving the puzzle problem. For an *N*-meter network, let ϕ denote the number of pre-specified miners ($1 \le \phi \le N$). Therefore $\phi = N$ indicates that all nodes participate in the mining process. In this case, the computational hardware investment cost on the miners would

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

be very high as the puzzle problem solving process is computationally intensive. Different values of ϕ in the range [1, *N*) then represent different compromises between the mining efficiency and computational hardware investment [46]. One demerit of this strategy is that the pre-specified miners could become the targets of cyber-attackers.

Strategy 2: Randomly Selected Nodes as Miners

In this strategy, the computational hardware configurations of all the nodes are same, but not all nodes are required to act as miners. For each mining process, miners are randomly selected from among the nodes. Compared with strategy 1, this strategy calls for greater investment in hardware and, furthermore, is more complex as each time the miners need to be re-selected. However, the random miner selection strategy is more secure. For an *N*-meter network, let $\bar{\phi}$ denote the pre-specified miner number; at each time instant there are a total of $C_N^{\bar{\phi}}$ possibilities to generate the miners. When *N* is large, the mining process is well-protected against cyber attackers.

4) Release of Meter's Memory Periodically

With continuous operation of the system, the blockchain ledger will become progressively larger. For example, suppose the size of the block header and tailer is 80 bytes, the data content is 1,000 bytes, and blocks are generated at a frequency of 1 per minute. Then after one year the size of the ledger would be (1000+80)×60×24×365 = 541 MB. For these parameters, freeing up the meter memory on an annual basis is sufficient for recycling memory space. In the proposed framework, the data content of the blocks needs to be backed up and meter memory released periodically.

IV. Performance Analysis of the Distributed Blockchain based Data Protection Framework

In this section we analyse the performance of the proposed framework, motivated by three key observations. Firstly, since blockchain technology was first proposed and applied as a financial technology [27], application to power systems must necessarily consider relevant domain-specific aspects of this new application area. Secondly, since the proposed framework is applied beyond the capabilities of existing equipment in most systems, any application must be based on the development of modern power systems and corresponding technologies. Therefore, potential disadvantages and practical challenges should be explicitly presented. Thirdly, the motivation of applying blockchain technology to power systems is that the proposed framework provides a more secure environment for information gathering and storage compared with traditional systems. We therefore present comparisons in which the probability of a successful cyber-attack is quantified.

Table II
Technology Comparisons

Items	Blockchain in Bitcoin System	Blockchain in the Proposed Framework
Network	Public	Private
Transaction initiator	Human intervention	Completely automatic
Transaction content	Money	Collected measurement
Transaction relationship	Continuously, related	Independent, unrelated
Checking historical blocks prior to the voting process	Required	Unnecessary
Chain connection speed	Approximately 7 transactions per second [37]	Much faster
Reward to node	Yes	No
Double-spending attack	A threat	Not exist
51% attack	Difficult	Difficult but threshold adjustable

A. Blockchain Technology Innovation and Comparison

The proposed application of blockchain to power system security differs in several key aspects from the original financial technology (i.e. Bitcoin) setting. Table II summarizes key technology comparisons.

Unlike the Bitcoin system, in which the blockchain is based on a public network, the proposed framework is private. In other words, only authorized meters can operate as nodes which transfer and store data. Combined with the fact that communication among nodes is isolated from the Internet, the proposed framework provides a more secure environment than Bitcoin. Moreover, distinct from Bitcoin system where human intervention is required to launch a transaction, the proposed framework is a completely automatic network.

Since the collected data at each node in the proposed framework is measured by a corresponding meter, gathered information is (in principle) independent and unrelated to earlier measurements. It is therefore unnecessary to check historical blocks prior to the voting process. In Bitcoin data verification, the system need to ensure that the Bitcoin sender has sufficient balance to afford the specified transaction. In contrast, the proposed framework requires only the voting process for data verification, i.e. actions analogous to Bitcoin deposit checking are not required in the proposed system. In other words, there is no 'Merkle tree situation' [39] in the proposed framework. Therefore, chain connections in the proposed framework is simpler and faster than that in the Bitcoin system. The mining speed of finding the nonce for the current block becomes the only factor that is highly important when blocks are being linked as a chain in the proposed framework. In this situation, technical or algorithm improvement in developing a fast, reliable and energy-efficient mining method is the major concern.

In the proposed framework, mining is a competition among all miners, while there is no reward as an incentive for miner who solves the puzzle problem first. All nodes are strictly driven by the consensus; and all miner behaviours are pre-programed and automatically generated.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

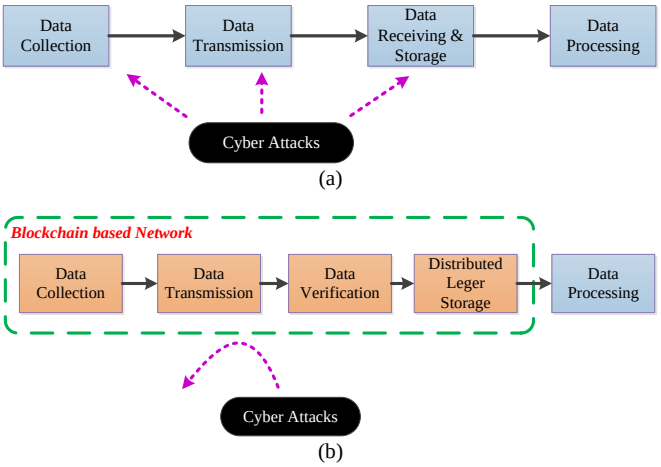


Fig. 5. (a) General procedure for existing data communication; (b) General procedure for blockchain-based data communication

One notable hazard for the Bitcoin system is the so-called "double-spending attack" [47] a cheating behaviour in which a bitcoin-sender spends a single digital token twice. The double-spending attack is not a threat for the proposed framework, however, because in the grid operational environment, there is no transaction activity between nodes.

One another important cyber-attack issue related to the blockchain based system is the so called "51% attack" problem [47], in which an attacker is able to take control of the majority of nodes to produce a false agreement on the voting result. Normally, for a public system with a large number of nodes, it could be extremely difficult to launch a successful 51% attack. For the proposed framework, there are often a large number of sensors deployed in substations, transmission lines and so forth. Taking control of the majority of the geographically distributed meters/sensors would be an extremely difficult task for cyber attackers. Furthermore, according to Eq. (1), the threshold is adjustable and should be equal or larger than 50%. For example, supposing there are 10,000 meters/sensors in a network and the threshold is set to be 70%. Then, in order to achieve false agreement on the voting result, a cyber-attacker needs to tamper with at least 7,000 sensors simultaneously. This suggests the "51% attack" would be very difficult, if not impossible, to be applied in the proposed framework.

B. *Potential Disadvantages and Practical Challenges*

The proposed framework explores a new direction for the development of securing modern power systems by leveraging state-of-the-art concepts from distributed security. There are, however, potential disadvantages and practical challenges in the proposed framework. As shown in Table III, three main type of items are presented to give readers a comprehensive and balanced viewpoint.

Firstly, in the practical deployment of the proposed framework, one potential disadvantage is *timeliness*. Fully supporting the operation of the proposed framework may necessitate upgrading or replacing existing sensing devices and communication networks. These upgrades or replacements may require non-trivial financial investment and could involve the coordination of multiple functional departments in different

Table III
POTENTIAL DISADVANTAGES AND PRACTICAL CHALLENGES

Items	Disadvantages		Challenges
Timeliness	Upgrade /replacement	Sensing devices	Cost vs. benefit
		Communication networks	
Security	Majority Manipulated	Sensors	Technology development
		Communication channels	
Redundancy	Information disclosure	Distributed data storage	Defending strategy

regions. The corresponding challenge for power system operators is to balance the necessary investment in upgrades or replacement with the benefits from enhanced security. Nonetheless, cost alone is not necessarily a deterrent to adoption of new technology in smart grid if the benefit is warranted.

We anticipate that deployment of the proposed framework based on a microgrid or a part of the power system, such as a substation, is far more practical and timely than the deployment of comprehensive smart grid infrastructure.

A second potential disadvantage of the proposed framework is *security*. The proposed framework is based on the mechanism of the majority rule, i.e., geographically distributed sensors—hence many communication channels—greatly increases the difficulty faced by cyber attackers in manipulating sensors/channels so as to reach a false agreement. However, technological developments including computational power, data communication capabilities and even Blockchain technology itself are available not only to system operators but also potential cyber attackers. It therefore seems reasonable for cyber attackers to employ these technologies. Moreover, malicious cyber-tampering attacks [54-59] and malware propagation [60] [61] in distributed systems and AMI networks may also be employed by cyber attackers as a means of compromising the proposed blockchain-based protection framework. The context, therefore, is a scenario in which both cyber-attackers and system operators take full advantage of developing technologies and state-of-the-art security attacks and defences.

A third and final potential disadvantage of applying the proposed framework is *redundancy* which thereafter may cause information disclosure. The distributed reconfigured SCADA network provides much redundant data, since each one of the registered sensors/meters in the network has a record of all nodes' measured data during some period of time. An attacker may therefore read all distributed stored data by hacking into a single sensor/meter. While access to measured information does not directly harm the system, stealing system operation information is sometimes extremely important for cyber attackers to surveil the target network, and so design effective attack strategies. The design of appropriate defense strategies, such as limiting read permission, designing self-destruction procedures and so forth, requires further research beyond the scope of the present paper.

C. *Efficiency Evolution*

In this sub-section, we compute the probability of a successful, basic attack for both the existing system and the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

Table IV
SUCCESSFUL ATTACKING CAPABILITY AND PROBABILITY COMPARISONS

Items		Scenario 1	Scenario 2
Data before Send out	Capability	Hack into *n* meters	Hack into *n* meters; Gain *n* pairs of key info
	Probability	$\frac{1}{3}\prod_{i=1}^{n}\lambda_i$	$\frac{1}{3}\prod_{i=1}^{n}\bar{\lambda}_i\times(\prod_{i=1}^{n}\bar{\xi}_i)$
Data in Transmit	Capability	Hack *n* channels	Hack $\bar{K}$ channels; Gain *n* pairs of key info
	Probability	$\frac{1}{3}\prod_{i=1}^{n}\eta_i$	$\frac{1}{3}(\prod_{i=1}^{\bar{K}}\bar{\eta}_i)\times(\prod_{i=1}^{n}\bar{\xi}_i)$
Data after Received	Capability	Hack into control center	Hack into *K* meters; Gain *n* pairs of key info
	Probability	$\frac{1}{3}\mu$	$\frac{1}{3}(\prod_{i=1}^{K}\bar{\eta}_i)\times(\prod_{i=1}^{n}\bar{\xi}_i)$

proposed framework. Mathematical certification and simulation results are used to illustrate the efficiency of the proposed framework.

1) Successful Attacking Probabilities in two Scenarios

As summarized in our previous work [5], theoretically there are three ways for cyber attackers to launch an attack to tamper with data, and consequently affect the operations of the higher layer applications: (1) compromise meters locally; (2) intercept and forge data packets when transferring to the control centre; and (3) modify the control centre database. In this sub-section, we therefore consider three forms of manipulation corresponding to the cases above when considering the probability of making successful cyber-attacks in either existing power systems or the proposed framework, namely that data is manipulated before, during or after transmission. Comparisons are summarized in Table IV.

When applying the proposed framework, blockchain provides a powerful "firewall" to prevent data from being successfully manipulated by cyber attackers. This comparison is illustrated in Fig. 5. For convenience, we denote the cyber-attack scenarios under the existing systems and the proposed framework as scenarios 1 and 2, respectively. For both scenarios, the same premises apply: considering an *N*-meter network, suppose the attacker needs to manipulate the first *n* meters ($n \le N$) in a certain period, so as to launch a valid attack. We wish to compute the overall probability of a successful attack in each scenario. For each scenario in the paper, we assume that all forms of manipulations are independent; the situation of combinations of these forms of manipulations to launch successful attacks is not considered.

For scenario 1, Fig. 5 (a) indicates that in the existing power systems, cyber-attackers may manipulate data after it is collected (but before it is transmitted), during data transmission, or when data is received and stored in control centre. We assume that the three forms of manipulations are independent.

Suppose in the first situation of scenario 1 that the probability for attackers to hack into each meter is independent and denoted as $(\lambda_1,\lambda_2,...,\lambda_n,...,\lambda_N)$, where $0\le\lambda_i\le 1$, $i=1,2,...,n,...,N$. The attacker needs to hack into corresponding *n* meters; and the success probability of launching this attack for this situation is therefore $\frac{1}{3}\prod_{i=1}^{n}\lambda_i$.

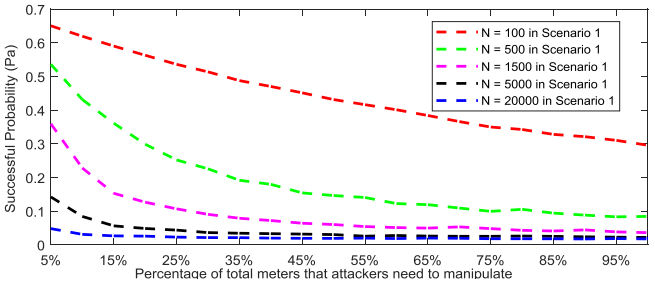
Suppose in the second situation of scenario 1, the probability for attackers to replace data package from the remote to control centre for all meters is independent and denoted as $(\eta_1,\eta_2,...,\eta_n,...,\eta_N)$, where $0\le\eta_i\le 1$, $i=1,2,...,n,...,N$. The attacker needs to hack into corresponding *n* communication channels; and the success probability of launching this attack for this situation is: $\frac{1}{3}\prod_{i=1}^{n}\eta_i$. Let μ denote the probability for the attacker to hack into control centre and manipulate the stored data, where $0\le\mu\le 1$. Then, the overall success probability, represented as P_a, of launching this attack for scenario 1 can be calculated as:

$$P_a=\frac{1}{3}(\prod_{i=1}^{n}\lambda_i+\prod_{i=1}^{n}\eta_i+\mu) \tag{10}$$

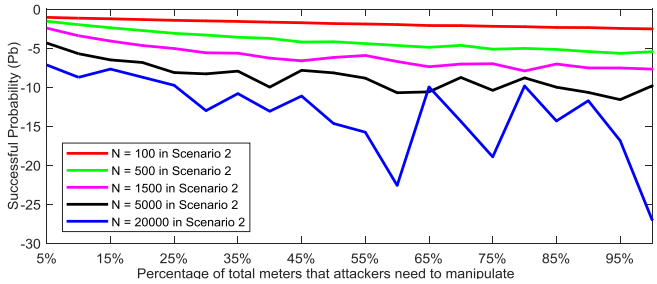
For scenario 2, Fig. 5 (b) indicates that in the proposed framework, cyber-attackers may manipulate data after it is collected (but prior to broadcast), or when data is transmitted to all other nodes via communication channels, or after data has been received at nodes (but prior to the data verification stage) in such a way to reach a false agreement through the voting mechanism.

Suppose in scenario 2 that the probability for attackers to steal each meter's key information is independent and set to be $(\bar{\xi}_1,\bar{\xi}_2,...,\bar{\xi}_n,...,\bar{\xi}_N)$, where $0\le\bar{\xi}_i\le 1$, $i=1,2,...,n,...,N$. Suppose that in the first situation of scenario 2, the probability for attackers to hack into each meter is independent and denoted as $(\bar{\lambda}_1,\bar{\lambda}_2,...,\bar{\lambda}_n,...,\bar{\lambda}_N)$, where $0\le\bar{\lambda}_i\le 1$, $i=1,2,...,n,...,N$. The attacker needs to hack into corresponding *n* meters, and also steal corresponding *n* pairs of key information so as to encrypt the false data; and the success probability of launching this attack for this situation is: $\frac{1}{3}\prod_{i=1}^{n}\bar{\lambda}_i\times(\prod_{i=1}^{n}\bar{\xi}_i)$. For the second situation of scenario 2, there are in total $N(N-1)/2$ communication channels in the proposed framework. Suppose that the probability for attackers to replace a data package when transmitting from one node to other nodes is independent and denoted as $(\bar{\eta}_1,\bar{\eta}_2,...,\bar{\eta}_{N(N-1)/2})$, where $0\le\bar{\eta}_i\le 1$, $i=1,2,...,N(N-1)/2$. Since the proposed framework has a voting threshold τ ($50\%<\tau<100\%$), the attacker must have the ability to hack into at least $\bar{K}=ceil[\tau\cdot N(N-1)/2]$ communication channels in order to launch a successful attack. Moreover, the attacker needs to steal *n* pairs of key information. Then, the success probability of launching this attack for this situation is: $\frac{1}{3}(\prod_{i=1}^{\bar{K}}\bar{\eta}_i)\times(\prod_{i=1}^{n}\bar{\xi}_i)$. For the third situation of scenario 2, before data verification process, the attacker needs to hack into majority, i.e., *K*, where $K=ceil(\tau\cdot N)$, meters at minimum and steal *n* pairs of key information to reach a false voting agreement. Then, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid



(a) Successful Proabilties in Real Number



(b) Successful Probabilities in Natural Logarithm

Fig. 6. Successful Attacking Probabilities Comparison

success probability in this situation is $\frac{1}{3}(\prod_{i=1}^{K}\bar{\lambda}_i)\times(\prod_{i=1}^{n}\bar{\xi}_i)$. Therefore, the overall successful probability, represented as P_b, of launching this attack for scenario 2, can be calculated as:

$$P_b=\frac{1}{3}[\prod_{i=1}^{n}\bar{\lambda}_i\times(\prod_{i=1}^{n}\bar{\xi}_i)+(\prod_{i=1}^{\bar{K}}\bar{\eta}_i)\times(\prod_{i=1}^{n}\bar{\xi}_i)+(\prod_{i=1}^{K}\bar{\lambda}_i)\times(\prod_{i=1}^{n}\bar{\xi}_i)] \quad (11)$$

It should be noticed that there is another case for attackers to manipulate data when data is received and in storage process in scenario 2, namely to hack into (at least) *K* meters and replace the stored distributed ledgers. An attack of this form requires an attacker to possess much more powerful computational capability to solve puzzle problems when reconnecting blocks. In this sub-section we do not consider this case; the probability of a successful attack is assumed to be negligibly small but is also difficult to estimate.

2) Efficiency Illustration

The probability deviation, represented as ΔP, for the above two scenarios is shown as follows,

$$\begin{aligned}\Delta P &= P_a - P_b \\ &= \frac{1}{3}\left\{(\prod_{i=1}^{n}\lambda_i+\prod_{i=1}^{n}\eta_i+\mu)-(\prod_{i=1}^{n}\bar{\lambda}_i+\prod_{i=1}^{\bar{K}}\bar{\eta}_i+\prod_{i=1}^{K}\bar{\lambda}_i)\times\prod_{i=1}^{n}\bar{\xi}_i\right\}\end{aligned} \quad (12)$$

where $n\le N$, $K=ceil(\tau\cdot N)$, $\bar{K}=ceil[\tau\cdot N(N-1)/2]$, $50\%<\tau<100\%$, $0\le\lambda_i\le 1$, $0\le\bar{\lambda}_i\le 1$, $0\le\eta_i\le 1$, $0\le\bar{\eta}_i\le 1$, $0\le\bar{\xi}_i\le 1$ and $0\le\mu\le 1$.

The form of the mathematical function above makes it difficult to perform direct comparisons as there are many uncertainties in variables. We therefore illustrate the efficacy of the proposed method through Monte Carlo simulation experiments. In order to make a clear statement of the advantages of our proposed framework in self-defensive capability of preventing data from being manipulated, we simulate both aforementioned probabilities. As shown in Fig. 6, we simulate 5 pairs of comparative experiments, in which the value N is set to be 100, 500, 1500, 5000 and 20000, respectively. The *n* value increases uniformly from 5% of value N to 100% of value N with the rate at 5% for each pair of the experiment in Fig. 6. All variables of λ_i, $\bar{\lambda}_i$, η_i, $\bar{\eta}_i$ and $\bar{\xi}_i$ are set to be in the range of [0.9,1]; the value of μ is set to be in the range of [0,0.1]; and the value of threshold τ is randomly chose in the range of [0.5,1]. The exact value of each variable is randomly chosen in that range for each experiment. For each pair of experiments, the simulation result shown in Fig.6 is 1000 random trials on average.

It is clearly seen from Fig. 6 that the successful attack probabilities for both scenarios keep decreasing as the number of meters able to be manipulated by an attacker increases. More importantly, it is clear that the proposed framework substantially outperforms the existing system in preventing meters from being manipulated. For 5 pairs of the experiments, the largest successful attack probability for scenario 1 and scenario 2 exist in the cases of manipulating 1% of corresponding *N* value, which is (65.07%, 34.52%); (53.64%, 21%); (35.98%, 8.71%); (14.25%, 1.29%) and (4.85%, 0.078%); respectively.

V. Case Study

The IEEE-118 benchmark system consists of 54 generators, 118 nodes and 186 branches. In this case study, the IEEE-118 benchmark system is used as the basic foundation of cyber-attack scenarios under existing method and the proposed framework, represented as scenario 1 and scenario 2, with some common features: each node deploys a meter to collect analog information (voltage, current, power flow, etc.); each branch deploys a breaker to collect digital information (OPEN/CLOSED line status); and each branch deploys two meters on both ends of the line to collect analog information (voltage, current, power flow, etc.). Therefore, basic situations of both scenarios are shown as follows:

Scenario 1: there are a total of 118+186+186×2=676 sensors gathering information from corresponding remote location. Therefore 676 communication channels are linked from sensors to the control center.

Scenario 2: there are a total of 118+186+186×2=676 sensors gathering information from corresponding remote locations. Therefore there are 676×(676-1)/2 = 228,150 communication channels between sensors.

We only consider the uncertainty of the cyber attacker's successful attack probabilities on hacking into sensor, hacking into communication channels, and stealing key information; and the total number of manipulated data so as to launch a successful attack.

In simulations, we assume the cyber attacker aims to launch a successful FDIA to the IEEE 118-bus system by manipulating gathered sensor information so as to influence system operation; the number of needed manipulated sensor data represents as *n* with the range of [1, 676]. We assume in both scenarios the cyber attacker can independently choose the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2018.2819663, IEEE Transactions on Smart Grid

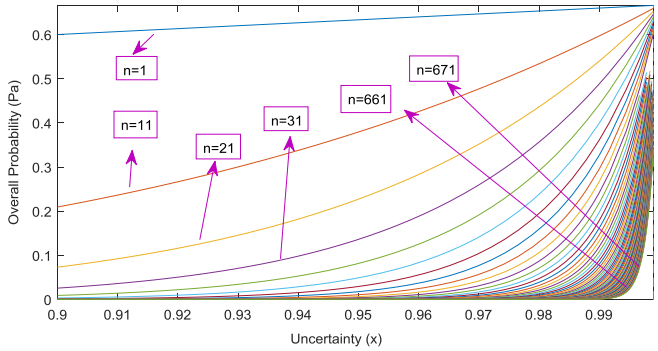


Fig. 7. Successful Attacking Probabilities in Scenario 1 based on IEEE-118 system

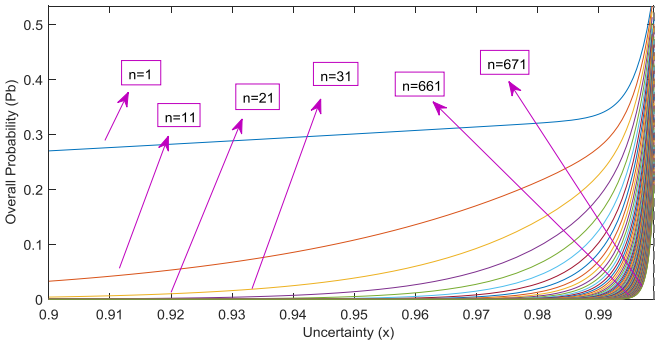


Fig. 8. Successful Attacking Probabilities in Scenario 2 based on IEEE-118 system

aforementioned attacking cases shown in Table IV in Section IV. We assume the successful attacking probability for the attacker to hack any information (except hacking into control center in scenario 1) is equal and set to be x with the range of [0.9, 0.999], i.e., $x = \lambda_i = \bar{\lambda}_i = \eta_i = \bar{\eta}_i = \bar{\xi}_i$. We assume the successful attacking probability for the attacker to hack into control center in scenario 1 is 0.001; and the voting threshold τ is set to be 51% in scenario 2. Therefore, $K = ceil[51\% \times 676] = 345$; and $\bar{K} = ceil[51\% \times 676 \times (676-1)/2] = 116{,}357$. Therefore, there should be:

$$P_a = \frac{1}{3}(2x^n + 0.001) \tag{13}$$

$$P_b = \frac{x^n}{3}(x^n + x^{116357} + x^{345}) \tag{14}$$

As shown in Fig. 7 and Fig. 8, uncertainty in both x and n are considered. For both scenarios, when the cyber attacker has a definite number of manipulated data, the overall successful attacking probability increases along with the increase of his/her successful probability in hacking into meters/channels. When the cyber attacker has a definite capability in hacking into meters/channels, the more number of manipulated data is needed, the less overall successful attacking probability he/she has. However, it is obvious in both figures that no matter for the case of definite x or definite n, the overall successful attacking probability in scenario 2 is much lower than that in scenario 1. More importantly, it should be noticed that the range of x: [0.9, 0.999] adopted in this case study is very high, implying that the power system is almost completely exposed to cyber attackers.

VI. Conclusion

This paper proposes a distributed blockchain-based data protection framework for enhancing the data security of the modern power system against cyber-attacks. The proposed framework substantially enhances the self-defensive capabilities of power systems against cyber-attack by harnessing the distributed security features of blockchain technology first employed in the Bitcoin crypto-currency. The proposed framework therefore represents a promising new direction in cyber-security for modern power systems. Key technical details are presented, Blockchain technology innovation and comparisons are illustrated, and key implementation challenges are highlighted. We also present an efficiency evaluation of the proposed framework against cyber-attacks. Our work shows that blockchain can be considered as a promising solution for the data security of the modern power system.

Improvements in the underlying blockchain technology, including improvement of blocks' connection speed, acceleration of reliability and security, reduction of investment and risk, are expected to benefit blockchain-based applications. As one concrete example, the so-called "Red Belly Blockchain" can process 660,000 transactions per second on 300 machines in a single data center [62] [63], whereas the Bitcoin network is limited to around seven transactions per second. Future breakthroughs in blockchain technology are to be anticipated, thereby enhancing industrial acceptance and deployment in practical power system settings. In future research, we will consider further refinement of the consensus algorithm, and perform an assessment of associated software and hardware investment costs vs. benefits.

References

[1] F.F. Wu, K. Moslehi and A. Bose, "Power system control centers: Past, present, and future," *Proc. IEEE*, vol. 93, no. 11, pp. 1890–1908, 2005.

[2] F. Luo, J. Zhao, Z.Y. Dong, Y. Chen, Y. Xu, X. Zhang and K.P. Wong "Cloud-based information infrastructure for next-generation power grid: conception, architecture, and applications," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1896–1912, Jul. 2016.

[3] NCCIC/ICS-CERT, "Cyber-attack against Ukrainian critical infrastructure," released 25 February 2016. [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 [Accessed: 22 Jan. 2018].

[4] E-ISAC and SANS, "Analysis of the cyber attack on the Ukrainian power grid: Defense use case," released 18 March 2016. [Online]. Available: https://ics.sans.org/duc5 [Accessed: 22 Jan. 2018].

[5] G. Liang, S.R. Weller, J. Zhao, F. Luo and Z. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst*., vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[6] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. and Syst. Security (TISSEC)*, vol. 14, no.1, May 2011.

[7] G. Liang, J. Zhao, F. Luo, S.R. Weller, and Z. Dong. "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630 – 1638, Jul. 2017.

[8] R. Deng, G. Xiao, R. Lu, H. Liang and A.V. Vasilakos, "False data injection attack on state estimation in power systems – attacks, impacts, and defense: A survey," *IEEE Trans. Industrial Informatics*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[9] O. Kosut, L. Jia, R.J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Oct. 2011.

[10] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data injection attacks against power system state estimation: Modelling and countermeasures," *IEEE Trans. Parallel Distrib. Syst*., vol. 25, pp. 717–729, March 2013.

[11] J. Chen, G. Liang, Z. Cai, C. Hu, Y. Xu, F. Luo, and J. Zhao, "Impact analysis of false data injection attacks on power system static security assessment," *J. Mod. Power Syst. Clean Energy*, vol. 4, no. 3, pp. 496–505, Jul. 2016.

[12] S. Tan, W.Z. Song, M. Stewart, J. Yang and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Trans. Smart Grid*, April 2016. DOI: 10.1109/TSG.2016.2550801

[13] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[14] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun*., vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[15] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, March 2016, DOI: 10.1109/TSG.2016.2532347

[16] G. Liang, S.R. Weller, F. Luo, J. Zhao and Z. Dong, "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism," to appear in *IEEE Trans. Smart Grid*. Accepted on 12 February 2017.

[17] G. Liang, S.R. Weller, J. Zhao, F. Luo and Z. Dong, "A framework for cyber-topology attacks: line-switching and new attack scenarios," to appear in *IEEE Trans. Smart Grid*. Accepted on 4 October 2017.

[18] Y. He, G.J. Mendis and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep leaning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[19] X. Liu, Z. Li and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.

[20] S. Gong, Z. Zhang, H. Li, and A.D. Dimitrovski, "Time stamp attack in smart grid: physical mechanism and damage analysis," arXiv preprint arXiv:1201.2578, Jan. 2012.

[21] X. Liu, Z. Li and Z. Li, "Impacts of bad data on the PMU based line outage detection," arXiv preprint arXiv:1502.04236, Nov. 2015.

[22] A. Primadianto and C.N. Lu, "A review on distribution system state estimation," *IEEE Trans. Power Systems*, vol. 32, no. 5, pp. 3875–3883, Sep. 2017.

[23] W. Kong, Z. Dong, D.J. Hill, F. Luo and Y. Xu, "Improving nonintrusive load monitoring efficiency via a hybrid programming method," *IEEE Trans. Industrial Informatics*, vol. 12, no. 6, pp. 2148–2157, Dec. 2016.

[24] I. Alsaidan, A. Alanazi, W. Gao, H. Wu and A. Khodaei, "State-of-the-art in microgrid-integrated distributed energy storage sizing," *Energies*, vol. 10, no. 9, Sep. 2017.

[25] R.R. Mohassel, A. Fung, F. Mohammadi and K. Raahemifar, "A survey on Advanced Metering Infrastructure," *Int. J. Electrical Power & Energy Systems*, vol. 63, pp. 473–484, Dec. 2014.

[26] T.N. Le, W.-L. Chin, D.K. Truong and T.H. Nguyen, "Advanced metering infrastructure based on smart meters in smart grid," in *Smart Metering Technology and Services - Inspirations for Energy Utilities*, pp. 37–61, M. Eissa (Ed.), InTech, 2016.

[27] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[28] Bitcoin System Introduction on Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Bitcoin [Accessed: 22 Jan. 2018].

[29] Blockchain/Bitcoin Charts, [Online]. Available: https://blockchain.info/charts [Accessed: 22 Jan. 2018].

[30] Ethereum Homepage, [Online]. Available: https://www.ethereum.org/ [Accessed: 22 Jan. 2018].

[31] Coinbase Homepage, [Online]. Available: https://www.coinbase.com/?locale=en [Accessed: 22 Jan. 2018].

[32] Ripple Homepage, [Online]. Available: https://ripple.com/ [Accessed: 22 Jan. 2018].

[33] Chain Homepage, [Online]. Available: https://chain.com/ [Accessed: 22 Jan. 2018].

[34] Circle Homepage, [Online]. Available: https://www.circle.com/en [Accessed: 22 Jan. 2018].

[35] Storj Homepage, [Online]. Available: https://www.storj.io [Accessed: 22 Jan. 2018].

[36] Factom Homepage, [Online]. Available: https://www.factom.com [Accessed: 22 Jan. 2018].

[37] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," arXiv preprint arXiv:1608.00695, Aug. 2016.

[38] M. Sharples, and J. Domingue, "The blockchain and kudos: a distributed system for educational record, reputation and reward," the *11th European Conf. Tech. Enhanced Learning*, Lyon, France, 13–16 Sep. 2016.

[39] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable and Secure Computing*, Oct. 2016. DOI: 10.1109/TDSC.2016.2616861

[40] A. Dorri, S.S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," Proc. *2nd IEEE Percom Workshop on Security, Privacy and Trust in the Internet of Things in conjunction with IEEE Percom* (SPT-IOT), Hawaii, USA, 13-17 March 2017.

[41] A. Dorri, S.S. Kanhere and R. Jurdak, "Blockchain in Internet of things: challenges and solutions," arXiv:1608.05187, Aug. 2016.

[42] M.B. Taylor, "Bitcoin and the age of bespoke silicon," *Proc. IEEE 2013 Int. Conf. Compilers, Architectures and Synthesis for Embedded Systems*, Montreal, QC, Canada, 29 Sept.–4 Oct. 2013

[43] M. Pilkington, "Blockchain technology: principles and applications," *Research Handbook on Digital Transformations*, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016.

[44] FIPS PUB 180-4, "Secure has standard," released Aug. 2015. [Online]. Available: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf [Accessed: 22 Jan. 2018].

[45] A. Beikverdi and J. Song, "Trend of centralization in Bitcoin's distributed network," *16th IEEE/ACIS Int. Conf. Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, Japan, Takamatsu, June 1–3, 2015.

[46] K.J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," *25th IET Irish Signals & Systems Conf. 2014 and 2014 China-Ireland Int. Conf. Inf. and Commun. Technologies (ISSC 2014/CIICT 2014)*, Limerick, June 26-27, pp. 280–285, 2014.

[47] G. Bissas, B. Levine, A.P. Ozisik, G. Andresen and A. Houmansadr, "An Analysis of Attacks on Blockchain Consensus," arXiv preprint arXiv:1610.07985, Oct. 2016.

[48] S. King, and S. Nadal, "PPCoin: peer-to-peer crypto-currency with proof-of-stake," self-published paper, August 2012.

[49] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid", *Proc. IEEE*, vol. 100, no. 1, pp. 210 – 224, Jan. 2012.

[50] F. Cleveland, "Enhancing the reliability and security of the information infrastructure used to manage the power system," in *Proc. IEEE Power Engineering Society General Meeting*, pp.1–8, Tampa, FL, USA, 24–28 Jun. 2007.

[51] J. Katz and Y. Lindell, "Introduction to Modern Cryptography," Chapman & Hall/CRC, 2007.

[52] S.S.S.R. Depuru, L. Wang and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and Sustainable Energy Reviews*, vol. 15, no. 6, pp. 2736–2742, Aug. 2011.

[53] L. Zhang, A. Bose, A. Jampala, V. Madani and J. Giri, "Design, testing, and implementation of a linear state estimator in a real power system," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1782–1789, Jul. 2017.

[54] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 835 – 843, Dec. 2011.

[55] C.-C. Su, A. Hahn and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Electrical Power & Energy Systems*, vol. 99, pp. 45–56, Jul. 2018.

[56] J. Mendel, "Smart grid cyber security challenges: Overview and classification," *E-mentor*, vol. 1, no. 68, pp. 55–66, 2017.

[57] F.M. Cleveland, "Cyber security issues for Advanced Metering Infrastructure (AMI)," *in Proc. IEEE Power Engineering Society General Meeting*, Pittsburgh, PA, USA, 20–24 Jul. 2008.

[58] S. Lee, J. Bong, S. Shin and Y. Shin, "A security mechanism of Smart Grid AMI network through smart device mutual authentication," in *Proc. Int. Conf. on Information Networking (ICOIN)*, pp. 592–595, Phuket, Thailand, 10–12 Feb. 2014.

[59] B. Vaidya, D. Makrakis and H. Mouftah, "Secure multipath routing for AMI network in smart grid," in *Proc. 31st IEEE Int. Performance Computing and Comms. Conf. (IPCCC)*, pp. 408–415, Austin, TX, USA, 1–3 Dec. 2012.

[60] Y. Park, D.M. Nicol, H. Zhu and C.W. Lee, "Prevention of malware propagation in AMI," in *Proc. IEEE Int. Conf. on Smart Grid Comms. (SmartGridComm)*, pp. 474–479, Vancouver, BC, Canada, 21–24 Oct. 2013.

[61] Y. Guo, C.-W. Ten, S. Hu, and W.W. Weaver, "Preventive maintenance for advanced metering infrastructure against malware propagation," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp.1314–1328, May 2016.

[62] University of Sydney News, "University of Sydney's super-fast blockchain gets even faster," [Online]. Available: https://sydney.edu.au/news-opinion/news/2017/10/25/university-of-sydneys-super-fast-blockchain-gets-even-faster.html, 25 Oct. 2017 [Accessed: 9 Feb. 2018].

[63] T. Crain, V. Gramoli, M. Larrea and M. Raynal, "(Leader/randomization/signature)-free Byzantine consensus for consortium blockchains," *arXiv preprint arXiv:1702.03068v2*, 22 Feb. 2017 [Accessed: 9 Feb. 2018].

Gaoqi Liang (S'13–M'17) obtained the B.E. degrees 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 physical system, power system security, and electricity market.

Steven R. Weller (S'88–M'94) received the B.E. (Hons. I.) degree in computer engineering in 1988, the M.E. degree in electrical engineering in 1992, and the Ph.D. degree in electrical engineering in 1994, all from the University of Newcastle, Australia. During 1994–1997, he was a Lecturer in the Department of Electrical and Electronic Engineering, University of Melbourne, Australia. In 1997, he joined the University of Newcastle, where he is currently a Professor in the School of Electrical Engineering and Computing. His research interests are in control theory and its applications. He was the recipient of the 2012 IET Control Theory and Applications Premium Award, and the 2017 IFAC Foundation Award.

Fengji Luo (M'13) obtained the B.E. and M.E. degrees in software engineering from Chongqing University, Chongqing, 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 a research fellow at the University of Sydney, Australia. His research interests include demand side management, computational intelligence applications, and smart grid informatics. He was selected as one of the eight scientists of the "2016 Australia-Japan Emerging Research Leader Exchange Program".

Junhua Zhao (M'07–SM'17) received his Ph.D. degree from the University of Queensland, Australia. He was a Senior Lecturer at the University of Newcastle, Australia, and also with the Center for Intelligent Electricity Networks (CIEN), University of Newcastle, Australia. Currently he is an Associate Professor with the Chinese University of Hong Kong, Shenzhen, China and also with the Electric Power Research Institute, CSG, Guangzhou, China. His research interests include power system analysis and computation, smart grid, cyber physical system, electricity market, data mining and its applications.

Zhao Yang Dong (M'99–SM'06–F'17) obtained his Ph.D. degree from the University of Sydney, Australia in 1999, where he was the Head of the School of Electrical and Information Engineering. He is now a Professor in the School of Electrical Engineering and Telecommunications, the University of New South Wales (UNSW). He is now a member of the ARC College of Experts. Prior to joining UNSW in 2017, he was Ausgrid Chair and Director of Ausgrid Centre of Excellence for Intelligent Electricity Networks (CIEN) at the University of Newcastle, Australia. He also held academic and industrial positions with the Hong Kong Polytechnic University, the University of Queensland, Australia and Transend Networks, Tasmania, Australia. His research interest includes Smart Grid, power system planning, power system security, load modeling, renewable energy systems, electricity market, and computational intelligence and its application in power engineering. Prof. Dong is an editor of IEEE TRANSACTIONS ON SMART GRID and IEEE POWER ENGINEERING LETTERS.