Distributed Blockchain-based Data Protection Framework for Modern Power Systems Against Cyber Attacks

A SEMINAR REPORT

Submitted in partial fulfillment of the

requirements for the award for the degree of

BACHELOR OF TECHNOLOGY

In

ELECTRICAL ENGINEERING

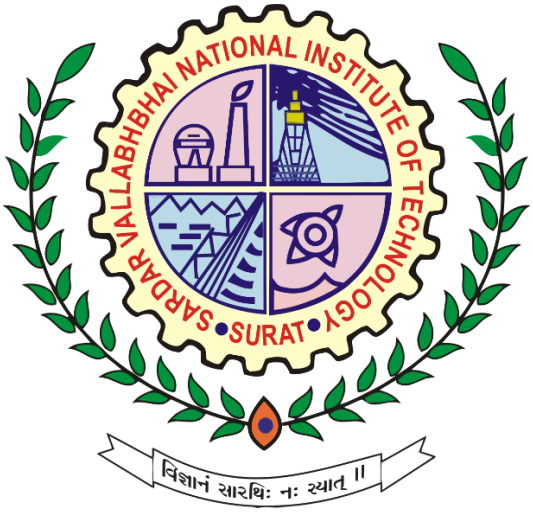
By

Yaswanth Sai Vendra

(ROLL NO: U20EE096)

Under the supervision of

Dr. Vasundhara Mahajan



DEPARTMENT OF ELECTRICAL ENGINEERING

SARDAR VALLABHBHAI NATIONAL INSTITUTE OF TECHNOLOGY (SVNIT)

SURAT, GUJARAT-395007(INDIA)

OCTOBER 2022

सरदार वल्लभभाई राष्ट्रीय प्रौद्योगिकी संस्थान, सूरत
Sardar Vallabhbhai National Institute of Technology
(SVNIT), Surat, Gujarat - 395007

CANDIDATE'S DECLARATION

I hereby certify that work which is being presented in this seminar report entitled **"Distributed Blockchain-based Data Protection Framework for Power systems Against Cyber Attacks"** in partial fulfillment of the requirements for the award of the BACHELOR OF TECHNOLOGY in ELECTRICAL ENGINEERING and submitted in the department of Electrical Engineering of the Sardar Vallabhbhai National Institute of Technology(SVNIT), Surat, Gujarat is an authentic record of my own work carried by me under the guidance of Dr. Vasundhara Mahajan, Associate Professor, DOEE, SVNIT Surat.

The matter submitted in this report has not been submitted by me or anyone for the award of any other degree or in any other institute.

(Signature)

(Yaswanth Sai Vendra)

This is to certify that the above statement made by the student is correct to the best of our knowledge.

Date: 15/10/2022 Place: SVNIT, Surat

(Dr. Vasundhara Mahajan)

Supervisor

सरदार वल्लभभाई राष्ट्रीय प्रौद्योगिकी संस्थान, सूरत
Sardar Vallabhbhai National Institute of Technology
(SVNIT), Surat, Gujarat - 395007

Examiner's Approval Certificate

The seminar entitled "**- Distributed Blockchain-based Data Protection Framework for Power systems Against Cyber Attacks**" submitted by Yaswanth Sai Vendra, U20EE096 **(Roll No)** in the partial fulfilment of the requirements for the award of the degree of "Bachelor of Technology in Electrical Engineering" of the Sardar Vallabhbhai National Institute of Technology, Surat is hereby approved

Date: 15/10/2022

Place: SVNIT, Surat

(Dr. Vasundhara Mahajan)

Supervisor

Examiner's Signature
(Name)

Examiner's Signature
(Name)

Chairperson

(Name)

ACKNOWLEDGEMENT

I acknowledge with great pleasure our deep sense of gratitude to Dr. Vasundhara Mahajan, Associate Professor, Department of Electrical Engineering, SVNIT Surat, for her constant encouragement and valuable guidance in the PG Project. I am very much indebted to her for suggesting this topic and helping me at every stage for its successful completion. The submission of this project gives me an opportunity to convey my gratitude to all those who helped me reach a stage where I am very much confident in launching my career in the competitive world of Electrical Engineering.

I express our profound thanks to Prof. A. K. Panchal, HOD, Dept. of Electrical Engineering, SVNIT Surat for his encouragement and providing me with outstanding facilities for the completion of my project work.

I would also like to thank my parents, seniors and friends without whose support, I would not have been able to reach this important moment of our life.

At last, I gratefully acknowledge my deep indebtedness to all other people who helped me during the whole period of the work.

Date: October 2022

Place: SVNIT Surat Yaswanth Sai Vendra(U20EE096)

Abstract

Cyber Security Attacks on Modern Power Systems has been increasing rapidly these days. The Security of Modern Power systems is being a real concern which is lagging many important measures to deal with todays' Cyber-attacks. Modern Power systems consists of many computational devices and communication links which are prone for many vulnerabilities. Many detection and defense methods for cyber-attacks have therefore been proposed to enhance robustness of modern power systems.

Here I have Proposed distributed blockchain-based protection framework to enhance the self-defensive capability of modern power systems against cyber-attacks. Here I have explained 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. All these blocks will be linked to form a ledger after the transaction in each block is being verified by all the nodes in the network i.e., meters in our case.

Table of Contents

Chapter 1

Introduction to Modern Power Systems

Modern power systems have gone through many changes to facilitate and cope with the current social requirements. Unlike conventional power systems, the infrastructure of modern power systems relies strongly on advanced communication and control technologies. While evolution of technological trends on 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.

These advances have been driving modern power systems towards becoming more 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. In this sense, data vulnerability has become an unneglectable issue, as evidenced by malicious events caused by cyber-attacks.

As a representative cyber-attack, the false data injection attack (FDIA) 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. 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. However, existing communication and storage of meter measured data mechanism in modern power systems are less than fully effective against cyber-attacks. 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 including distributed data acquisition, information monitoring and knowledge storage, on both system side and demand side.

Chapter 2

Introduction to Cyber Security

2.1 Introduction to Cyber Security

Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. From a computing point of view, security comprises cybersecurity and physical security - both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. Information security, which is designed to maintain the confidentiality, integrity, and availability of data, is a subset of cybersecurity. The use of cyber security can help prevent cyber-attacks, data breaches, and identity theft and can aid in risk management.

When we are saying protection, the main three aspects we need to control are

- Unauthorized Access
- Unauthorized Deletion
- Unauthorized Modification

This can be also Explained by CIA triad which essentially stands for Confidentiality, Integrity and Availability. The CIA model is made to aid businesses in establishing procedures to safeguard their IT infrastructure.

Cybersecurity is a vast field consist of various domains and aspects but here in the case of power systems we are mainly concerned about

1. Information Security (Data Security)
2. Network Security.

Information Security is the measures taken to protect the information from unauthorized access and use. It is based upon CIA triad. It is the superset that contains cyber security and network security. It is necessary for any organization or firm that works on a large scale.

Network Security is the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.

Chapter 3

Introduction to Blockchain

3.1 Blockchain

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An *asset* can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

A blockchain is a distributed, peer-to-peer database that hosts a continuously growing number of transactions. Each transaction, referred to as a "block," is secured through cryptography, timestamped, and validated by every authorized member of the database using consensus algorithms (i.e., a set of rules). A transaction that is not validated by all members of the database is not added to the database. Every transaction is attached to the previous transaction in sequential order, creating a chain of transactions (or blocks). A transaction cannot be deleted or edited, thereby creating an immutable audit trial. A transaction can only be changed by adding another transaction to the chain.

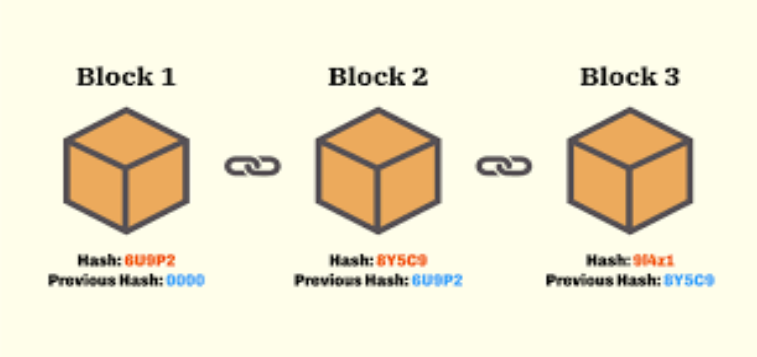


Figure 1: Blockchain Ledger

Table 1: components in a Block

Item	Description
Previous Hash	Hash code of the previous block
ID	ID of current Block
Time Stamp	Time at which this block is generated
Data	Data to be stored on blockchain

There are basic terminologies we use in Blockchain Ecosystem:

- Hash: Unique and fixed length string to identify the piece of data.
- Mining: Process of finding the solution to the block chain problem. Nodes get paid for mining the data in blocks.
- Block: A list of transactions which are mined together.
- Signature: Signatures are used to sign the transactions and verification of transactions. Private key is used to sign the transaction and public key is used to verify the transaction whether transaction is there is not.
- Gas: It is the measure of computation use of data.
- Gas Price: How much transaction costs per unit of gas.
- Gas Limit: Maximum amount of gas in a transaction.
- Transaction Fees: It is the amount of gas used times the gas price. Higher the nodes in BC higher will be the gas price.
- Hash algorithm: It's the hash algorithm used on data before storing it on blockchain. In case of Ethereum Blockchain, SHA256 (Secure Hash Algorithm) is used for hashing the data. Internally it makes use of keccak256 algorithm.

3.2 Types of Blockchain Network

Mainly there were four types of Blockchain Network

Public blockchain networks
A public blockchain is one that anyone can join and participate in, such as Bitcoin. Drawbacks might include substantial computational power required, little or no privacy for transactions, and weak security. These are important considerations for enterprise use cases of blockchain.

Private blockchain networks
A private blockchain network, similar to a public blockchain network, is a decentralized peer-to-peer network. However, one organization governs the network, controlling who is allowed to participate, execute a consensus protocol and maintain the shared ledger. Depending on the use case, this can significantly boost trust and confidence between participants. A private blockchain can be run behind a corporate firewall and even be hosted on premises.

Permissioned blockchain networks
Businesses who set up a private blockchain will generally set up a permissioned blockchain network. It is important to note that public blockchain networks can also be permissioned. This places restrictions on who is allowed to participate in the network and in what transactions. Participants need to obtain an invitation or permission to join.

Consortium blockchains
Multiple organizations can share the responsibilities of maintaining a blockchain. These pre-selected organizations determine who may submit transactions or access the data. A consortium blockchain is ideal for business when all participants need to be permissioned and have a shared responsibility for the blockchain.

3.3 Blockchain Consensus Mechanisms

The term 'consensus mechanism' is often used colloquially to refer to 'proof-of-stake', 'proof-of-work' or 'proof-of-authority' protocols. However, these are just components in consensus mechanisms that protect against Sybil attacks. Consensus mechanisms are the complete stack of ideas, protocols and incentives that enable a distributed set of nodes to agree on the state of a blockchain.

Types Of Consensus Mechanisms:

1. Proof of Work Based:

Validators create blocks. One validator is randomly selected in each slot to be the block proposer. Their consensus client requests a bundle of transactions as an 'execution payload' from their paired execution client. They wrap this in consensus data to form a block, which they send to other nodes on the Ethereum network. This block production is rewarded in ETH. In rare cases when multiple possible blocks exist for a single slot, or nodes hear about blocks at different times, the fork choice algorithm picks the block that forms the chain with the greatest weight of attestations (where weight is the number of validators attesting scaled by their ETH balance).

The network is kept secure by the fact that you'd need 51% of the network's computing power to defraud the chain. This would require such huge investments in equipment and energy; you're likely to spend more than you'd gain.

2. Proof of stake:

Proof-of-stake is done by validators who have staked ETH to participate in the system. A validator is chosen at random to create new blocks, share them with the network and earn rewards. Instead of needing to do intense computational work, you simply need to have staked your ETH in the network. This is what incentivises healthy network behaviour.

A proof-of-stake system is secure crypto-economically because an attacker attempting to take control of the chain must destroy a massive amount of ETH. A system of rewards incentivizes individual stakers to behave honestly, and penalties disincentivize stakers from acting maliciously.

3.4 Advantages of Decentralized Network Over Centralized Network

Centralized networks vs. Decentralized networks

	Centralized networks	Decentralized networks
Third-party involvement	Yes	No
Transparency	Less transparent	More transparent
Security	Vulnerable to attacks	More secure
Scalability	Easy to scale	Difficult to scale
Exchange fees	Higher fees	Lower fees

Figure 2: Centralized vs Decentralized Networks

Chapter 4

Distributed Blockchain-Based Data Protection Framework

4.1 Infrastructure of Implemented Framework

There are typically three basic processes for the supervisory control and data acquisition (SCADA) module in modern power systems:

1. data gathering at remote terminal units
2. plaintext transmission via a communication channel to the control center
3. Information storage in the control center .

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.

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. 3.

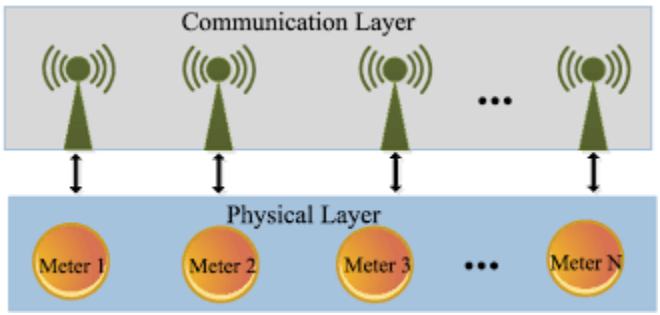


Figure 3: Reconfigured SCADA Network

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.

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, each meter need to be possess these functional features:

- 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.
- Meters are capable of communicating with each other through wired or wireless communication channels.

4.2 Working Mechanism of 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
- Distributed ledger synchronization

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.

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.

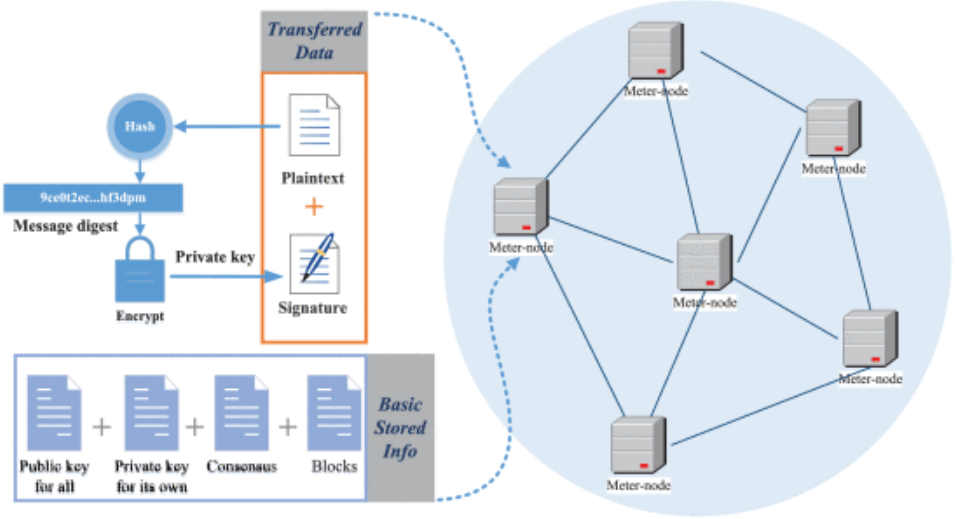


Figure 4: Data Encryption and Broadcast Process

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. 5, 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. 5, only once positive agreement is reached among the nodes, is the data recognized as correct

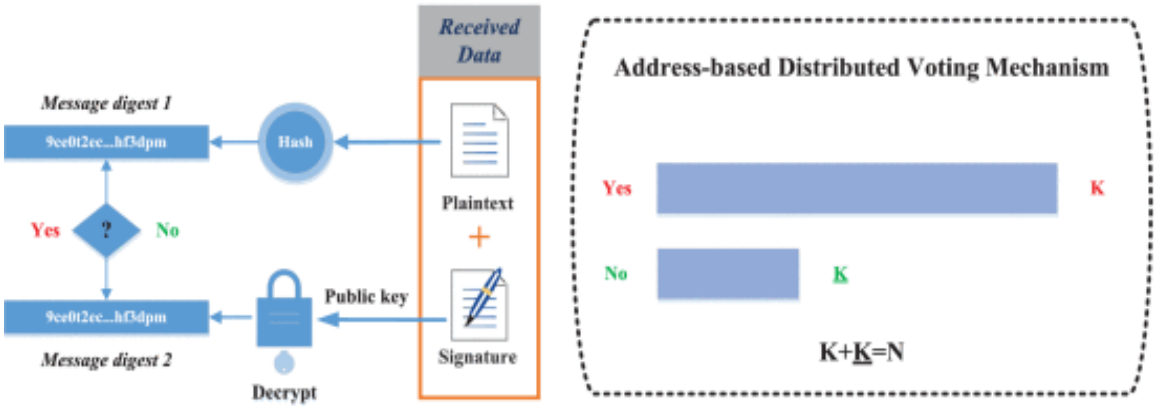


Figure 5: Data Decryption and Verification Process

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 $\underline{K}$), where $K \leq N$. Only when the following criterion is satisfied is the data accepted:

$$K/N > \tau \quad (1)$$

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.

4.3 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, 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.

Here 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
- nonce solution.

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:

$$S = b+d+t+hp+nonce \quad (2)$$

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

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:

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

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

$$\text{FinalHash} \leq T \quad (4)$$

Brute force is the only known way to solve the puzzle problem and it is therefore highly computationally 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. 6.

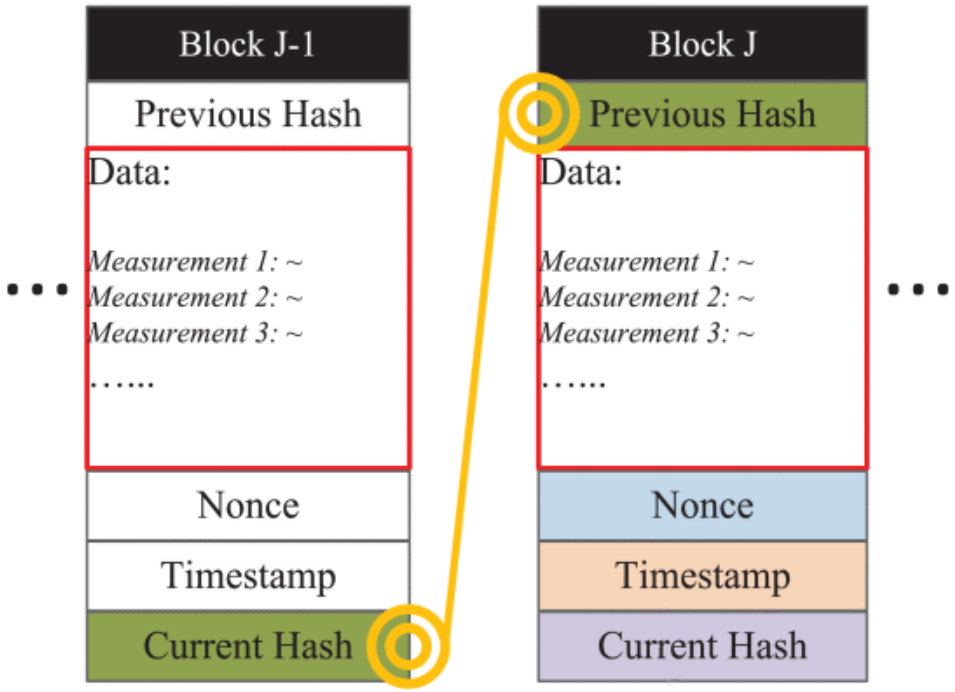


Figure 6: Blockchain Ledger

4.4 Consensus Mechanism

The consensus mechanism 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.

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.

1. 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:

$$\alpha < \Phi \qquad (6)$$

$$\beta \cdot \mathrm{floor}(\Phi/\alpha) \geq N \qquad (7)$$

   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 denotes rounding down to the nearest integer.

2. 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 β denote the block size (measured by the number of data items), let α denote the average time interval between two blocks, and let Φ denote the system state estimation time interval. The setting of β^{-} should satisfy the following two constraints:

$$\alpha < \Phi \qquad (8)$$

$$\beta \cdot \mathrm{floor}(\Phi/\alpha) \geq N \qquad (9)$$

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.

1. 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 ($1 \leq \phi \leq N$). Therefore $\phi = N$ indicates that all nodes participate in the mining process. In this case, the computational hardware investment cost on the miners would 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.

2. 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 ϕ denote the pre-specified miner number; at each time instant there are a total of $C\phi$ N 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 $(1000+80)\times60\times24\times365=541$ 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.

4.5 Performance Analysis of Framework

A. Comparision of Bitcoin and Our Proposed Framework

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

Figure 7: comparision of bitcoin vs Distributed Proposed Framework

B. 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

Figure 8: Potential Disadvantages and Practical Challenges

Conclusion

The proposed framework substantially enhances the self-defensive capabilities of power systems against cyber-attack by harnessing the distributed security features of blockchain technology. 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.

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] 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.

[4] 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.

[5] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.