Blockchain-based Security Protocol for Next-Generation Smart Grid Transactions

Lokendra Vishwakarma and Debasis Das

Computer Science and Engineering Department
Indian Institute of Technology, Jodhpur

Abstract: The World is rapidly shifting from conventional energy sources to renewable energy sources (e.g., smart grid). The widespread adoption of the smart grid requires it to be attack-proof and leak-proof, and demand decentralization the system for energy distribution to provide transparency in the smart grid system. However, this new modern energy system faces different challenges, such as the large-scale Internet of Things (IoT) devices adaptation, single-point failure due to a centralized system, slow transaction processing, and the emerging cybersecurity threats. To solve all these issues of the smart grid, we propose a novel blockchain-based security scheme. This scheme is intended to secure the transactions and make the energy distribution decentralized, reliable, transparent, and immutable. Instead of applying conventional blockchain protocol in the proposed scheme, we have modified the blockchain, which is more suitable in a smart grid application called Modified Blockchain (ModBlock). The decentralized nature of blockchain prohibits singular points of failure and enables secure communication between consumers and service providers. We have provided security analysis and performance evaluation. The performance evaluation showed enhancement in consensus delay, throughput, block verification time, computation cost, energy consumption, storage and communication cost compared to state-of-the-art schemes.

1. Introduction

A smart grid is a new age technology of energy distribution, which includes various operations and energy measures such as grid operators, smart meters, smart appliances, and renewable energy resources. The smart grid provides better controllability and observability compared to the traditional energy system and also provides a solution for low energy utilization rate. Due to the real-time interaction, the energy distribution company can make corresponding distribution and pricing adjustments. To enhance the access of distributed and scalable energy resources at a large scale, Internet technology is combined with the smart grid, which is formally called Energy Internet (EI), or Internet of Energy (IoE) or Smart Grid 2.0. Such innovative approaches aim to ensure the availability of energy anywhere at any time. Some challenges are made due to connectivity in Internet-enabled smart grid, aka EI is becoming more abundant. The centralization of the EI is prone to single point failure and also the tampering of the stored data at a central node. Thus, decentralization is a new and growing trend in smart grid technology [1]. However, due to the inclusion of the Internet in the smart grid, many challenges remain, such as the privacy of user information, security of data of power grids stored and shared with central nodes. The user information may be stolen by the attacker, while it is in transit. Therefore, it is on high priority to provide security and privacy of the user information and power grid data. To solve all these issues of smart grid technology, we propose a novel scheme, which is a blockchain-based security protocol. Formally, blockchain is the underlying technology of digital currency (e.g., Bitcoin, Ethereum, etc.). It is a decentralized, tamper-proof, immutable, and transparent technology that can achieve peer-to-peer transaction security which is independent of any third party. Blockchain permanently records the user information and transactional data in the form of blocks, and Merkle root [2] in the block header verifies whether the transaction data has been tampered with or not [3]. Hence, tamper-proof and distributed shared ledger are the key properties of blockchain technology, where blocks are arranged cryptographically in a special data structure. The issues of traditional centralized smart grid technology can be solved by acknowledging the blockchain properties. However, the consensus algorithms of conventional blockchain protocols such as Proof-of-Work (PoW), Proof-of-Stake (PoS), practical byzantine fault tolerance (PBFT) are not suitable for smart grid application due to high consensus delay and low throughput. Therefore, we developed a new blockchain protocol called ModBlock for the proposed scheme.

2. Methodology

1. ModBlock for Smart Grid

In ModBlock protocol, the miner node, which is connected as a peer-to-peer network, forms the logical ring as depicted in Figure 1. The miner who created the block gets the next chance after every node in the ring created the block, i.e., the block creation done by any node follow the clockwise direction, and unlike Bitcoin-NG, Bitcoin, ByzCoin, Algorand, HoneyBadger, Elastico, OmniLedger, and Monoxide in ModBlock every node in the network gets the equal chance to create the block. Hence, there is a Block Creation Time Quantum of every miner node to create a block. After the end of this quantum time, the next node in clockwise direction starts creating the block and so on. The reason for this logical ring formation is to get an equal chance to create the block, which eliminates the leader election process and reduces the computation overhead of the leader election process. The node who's turn to create the block is called the leader node. This leader node further creates the data block, which contains the user transactions. Addition of any node in the middle of the ring is not allowed. However, for transaction transmission, block transmission and block verification, peer-to-peer communication is followed.

2. Blockchain Enabled Smart Grid

This section explains the structure of the proposed scheme and arrangements of its different components such as smart meter, smartphone, miner node, and the grid operator, as shown in Figure 2. The miner node of the proposed scheme uses the consensus algorithm for transaction verification and also data block verification for the smart grid. The smart meter sends the transactions to the transaction pool of the miner node, which later verifies them and creates blocks into the blockchain. The details of the components of proposed scheme described below.
1. **Smart Meter:** The smart meter collects the data of power consumption and real-time monitoring information of the consumer. They are installed at the consumer location. Every smart meter has a unique ID which is generated at the production of smart meters. When a smart meter is installed, this unique ID is registered in the blockchain via miner node. Any data recorded in the smart meter is considered as the transaction, and these transactions are sent to the connected miner node. These smart meters generate multidimensional data and send them to the connected miner node. The smart meter is also connected to the smartphone for performing the smart feedback to the grid operator. The Smart meters are also connected to the grid operator.

2. **Smartphone:** The smart meter records the real-time power consumption and feedback from the grid operator, and it sends it to the connected smartphone. The consumer can also get real-time information such as power supply capacity, power strength, power quality, power charges, blackouts. All this information is beneficial to arrange the electrical home appliance accordingly. This real-time monitoring using a smartphone is helpful to arrange all these devices. Using the data received from the smart meter, the user can also optimize power usage.

3. **Grid Operator:** The grid operator is the entity which is responsible for power distribution and sales of electricity in the connected region. The grid operator is connected to the region using the smart meter. To ensure real-time monitoring and make a balance between demand and production is the main and important function of the grid operator. The grid operator collects the consumer power consumption in real-time and maintains the demand of the region. This practice reduces the sudden pressure on the grid during peak hours, such as during night hours, and enhances the reliability and robustness of the system. This practice also made the system fault-tolerant.

3. **Working**
The grid operator is connected to all the regions, where the smart meter is installed. These smart meters are connected to the user’s smartphone as well as to the nearest miner node. The smart meter collects multidimensional data such as real-time power consumption, blackouts, peak power consumption time, low power consumption time. This collected data is shared with a connected smartphone. The user uses it to optimize the power consumption and arrange the electric home appliance accordingly. Based on the data of power consumption, users can also optimize their power consumption dynamically. In that way, the charging of power consumption can be reduced. The smart meter also shared the power consumption data and payment data to the miners to store into the blockchain. The communication between the smart meter and miners is secured using Elliptic Curve Digital Signature Algorithm (ECDSA) based digital signature algorithm. The transaction sent by the smart meter to miners is temporarily stored at the transaction pool of the miner. The miners collect all the transactions, verify them and send them to the other miners. Then the miners create the block and broadcast it to the network for verification. Miner nodes use the consensus algorithm to create a new block. After verification, the block is appended into the distributed ledger. Every node keeps the identical copy of the distributed ledger.

3. **Conclusion**
In this paper, we have proposed the blockchain-based security protocol for transaction in the next-generation smart grid system. The proposed scheme is divided into two parts, blockchain modification usually called ModBlock and applying this ModBlock into the smart grid, i.e., a next-generation smart grid system. This scheme uses the blockchain to achieve decentralization, immutability and transparency for smart grid data. The ModBlock is the novel blockchain protocol, developed to better fit in the smart grid application. The proposed scheme is the security system for secure and fair energy distribution. Security analysis showed that the proposed scheme meets all the various security requirements. The performance evaluation of ModBlock and proposed scheme showed high accuracy and efficiency compared to state-of-the-art schemes. This scheme is useful to analyze the power consumption and enables the user to arrange the electric home appliance accordingly.
References


Lokendra Vishwakarma
Ph.D. Student, Computer Science and Engineering Department
Email: vishwakarma.3@iitj.ac.in

Dr. Debasis Das
Assistant Professor, Computer Science and Engineering Department
Email: debasis@iitj.ac.in