


Technical Note

An Ethereum Blockchain-Based Prototype for Data Security of Regulated Electricity Market

Aasim Ullah ^{1,*} , S M Shahnewaz Siddiquee ², Md Akbar Hossain ³ and Sayan Kumar Ray ³

¹ School Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland 1010, New Zealand

² Department of Energy Engineering, University College Cork, College Rd, T12HY8E Cork, Ireland; 119222676@umail.ucc.ie

³ School of Digital Technologies, Manukau Institute of Technology, Manukau 92068, New Zealand; akbar.hossain@manukau.ac.nz (M.A.H.); sayan.ray@manukau.ac.nz (S.K.R.)

* Correspondence: aasim@kth.se; Tel.: +64-22439370

Received: 22 September 2020; Accepted: 25 November 2020; Published: 27 November 2020



Abstract: Data security of present-day power systems, such as the electricity market, has spurred global interest in both industry and academia. The electricity market can either be regulated (state-controlled entrance, policies, and pricing) or deregulated (open for competitors). While the security threats in a deregulated electricity market are commonly known and have been investigated for years, those in a regulated market still have scope for extensive research. Our current work focuses on exploring the data security of the regulated electricity market, and the regulated New Zealand Electricity Market (NZEM) has been considered for this research. Although the chances of cyberattacks on state-controlled regulated electricity market are relatively less, different layers of the current SCADA systems do pose some threats. In this context, we propose a decentralized Ethereum Blockchain-based end-to-end security prototype for a regulated electricity market such as the NZEM. This prototype aims to enhance data security between the different layers of the current SCADA systems. The detailed operation process and features of this prototype are presented in this work. The proposed prototype has prospects of offering improved data security solutions for the regulated electricity market.

Keywords: SCADA; blockchain; Ethereum; security; electricity market

1. Introduction

The worldwide demand for electricity is expected to rise by 1.3% per year until 2040, primarily due to the effect of globalization [1]. This surge in demand has led to the interconnection of a wide range of distributed energy resources and electricity infrastructures, which are primarily the different electricity generation sites and the distribution channels. This inter-connectivity is commonly known as the Internet of Energy (IoE). The data generated from the various elements of IoE need to be managed securely as they are subject to hacking and cyberattacks, which include jamming, false data injection, and distributed denial-of-service attacks [2]. For example, a cyberattack on the U.S. grid in Western US created periodic blind spots at a grid control center and several small power generation sites for about 10 h on 5 March 2019. Contemporary power systems encountered remarkable advancement of data security in recent years. Contrary to traditional power systems, the NZEM is yet to adopt the advancement. One of the reasons is governing administration issues about company fixed revenues for line companies. There are distributed generation and several regional power suppliers in NZEM. Data security of the suppliers is an important term for any power market, and NZME is not an exception.

Supervisory Control and Data Acquisition (SCADA) systems are an integral part of the physical infrastructure of NZEM that monitors and stores real-time data of the grid network. A SCADA system is generally composed of a centralized control module and associated field level devices, i.e., sensors and actuators. The control module of SCADA provides a decision support platform that performs the related control task of the system. Given the dynamics of the SCADA system, the key features that make the SCADA system more susceptible to cyberattacks lie within its architecture and standard communication protocols. In many cases, the SCADA system adopts standardized technologies without enhancing the default security protocols. This practice can allow malicious agents to take over the SCADA system easily by exploiting the known vulnerabilities of the default security protocols. Subsequently, the usage of an unsecured network to connect multiple control modules also makes the system open for malicious attacks. Recently, most of the technical information about the specific SCADA control modules have been widely available as open-source content. This information, however, can be used to compromise the security of the entire SCADA system. Currently, there are many methods in place to reinforce SCADA network security that range from improved authentication for the user for access control, better firewalls, and intrusion detection system, protocol vulnerability assessment, and improved security for the connected devices and platforms operating system. However, all the typical vulnerabilities are still being exploited by the adversaries utilizing improved malicious agents and approaches. An example of a cyberattack aiming at SCADA system vulnerabilities in recent years was the Ukrainian power outage in 2015.

Blockchain technology, equipped with the key features of digital, chronological, time-stamped, distributed ledger, consensus-based, and cryptographically sealed, is considered as a potential tool to provide the data security of the electricity market. The smart contract in blockchain can be used not only to enhance the speed and security of a smart grid [3] but also to prevent the retroactive alteration of data. Blockchain technology has immense prospects in better and secured streamlining of management of SCADA data transactions and peer-to-peer data transactions. The prospect of implementing blockchain technology for a regulated electricity market is investigated in this paper, and a decentralized end-to-end Ethereum Blockchain prototype is proposed to enhance the data security between the different layers of the current SCADA systems used in regulated electricity market like NZEM. In comparison to other existing blockchain protocols, Ethereum has more durability, which implies that it has reduced possibility of becoming obsolete since it stores data immutably. Its decentralized and distributed peer-to-peer data transaction is unique compared to other existing cryptocurrencies. Moreover, Ethereum's smart contracts feature eradicates the demand for a third-party payment system. Moreover, it provides users with a platform and programming language for building the applications. Therefore, in this work we have considered the Ethereum blockchain to address the following major research inquiries for a regulated market using SCADA system:

- (1) How can blockchain smart contracts support the state-owned regulated market?
- (2) How can blockchain safe-guard grid data for the communication level of the SCADA system which is sensitive to cyber-threat?
- (3) What are the prospective privacy and safety regulation for applying blockchain to NZEM?

The remaining paper is structured as follows. While Section 2 presents a review of the data security in power systems, the current status of data security in regulated and deregulated electricity markets is presented in Section 3. Section 4 discusses the decentralized Ethereum blockchain-based end-to-end data security prototype, and the paper concludes in Section 5.

2. A Review of Data Security in Power System and introduction of Blockchain

Data security in power system offers new prospects to maximize the energy performance of the power market. It provides the efficiency, and security for the fundamental detailed facilities of energy suppliers [4]. Modern cyber-security systems for power systems have turned complex and the cyberattacks are becoming smarter every day. The profound incorporation of cyberattacks can deliver false information to the control management facility team and eventually can result in system disorder,

fiscal impairment, or critical consequences such as long hour's blackouts. A current severe example of cyberattack was the 2015 Ukraine blackout [5].

False data injection attack refers to the manipulation of system data to trick away the control center without the flag service [6]. There are several studies [5,7] that exhibit the effect of False Data Injection Attacks (FDIA) on the modern grid system. However, in reality, grid security can be compromised not only by FDIAs but also by other forms of cyberattack namely denial of service (Dos), cyber topology attacks and data framing attacks [8,9]. Hence it is very essential to ensure the integrity and consistency of data to make the grid more secure and reliable. Several strategies have been suggested to identify and prevent cyberattacks depending on traditional centralized data communication and storage process [10]. Moreover, currently existing communication and measured meter data storage mechanisms are not fully protected against a cyberattacks. In some cases, even if the meters have been upgraded to PMU (phase measurement systems), they are still vulnerable to cyber-threats due to their dependency on global positioning system. Enhancing the self-defensive capabilities of modern power systems against cyberattacks requires the adoption of state-of-the-art innovations in distributed system security technologies. In this regard a modern distributed power system can be viewed as distributed advanced measurement infrastructure that includes distributed data acquisition, data monitoring, and storage on both grid side and demand side [11].

First, introduced in 2008, blockchain is designed to facilitate peer to peer electronic transactions directly without the involvement of a third party [12]. In blockchain, each peer works as a node to form a distributed network where they participate in estimating the solution to a hash-based mathematical problem to ensure the integrity of the transaction. Each time when a transaction is made, it is encapsulated in a block and added to the blockchain framework. The recorded block contents are called as ledgers, and all the information is updated synchronously to the entire network so that the record of the ledger is kept by each peer in the network. Since the advent of blockchain, technology has been mostly focused on the financial domain in the form of maintaining virtual currency, cross border payments and settlements, security issuance, and payments. The most prominent application of blockchain technology is the Bitcoin system, a cryptocurrency framework which maintains a global distributed ledger for peer to peer transaction. Following the Bitcoin system, some companies, such as Ethereum, Coinbase, Ripple, Chain, Circle, etc., have been set up in recent years. Among other works, the blockchain swarm system by Ferrer [13] and Sharples and Domingue [14] is mentionable and has good prospects to be implemented for power systems.

Recently, there has been a shift observed in the energy market towards a distributed market structure [15] with increased number of prosumers and increase volume of data. In a centralized market structure, storing this large volume of data has higher costs, and the risk of compromising all data is very high under any cyberattack. It is also difficult for the market entity to access the previous data if they are stored in one organization under a centralized market. Hence, transparency issues also arise for the market operators. Addressing this problem, many authors have provided different techniques on adopting blockchain technology in the energy market to ensure better data security and market operation.

In [16], a distributed blockchain based protection framework has been proposed to improve the data security by resisting external network attacks in a modern power system. This proposed framework utilizes distributed security features of the blockchain system and uses smart energy meter as node to keep the recorded power data with a distributed ledger which ensures the integrity and consistency of the data.

In [17], a sovereign blockchain based smart grid management system is being proposed to protect the data of the consumers for ensuring the transparency and integrity of the data. It also protects the data from tampering under any cyberattack. This proposed system uses smart contacts to detect the grid operation and identify any malicious agents in the system.

In [18] a distributed blockchain based power market trading platform is proposed to provide P2P secured transactions. In this blockchain based P2P transaction model, all the participating nodes and

all transaction are stored. Since the data are stored in the blockchain and they are connected to all the nodes, they are more secure and transparent.

The security risks for a deregulated electricity market are therefore recognized and well defined. The security threat for regulated market is obvious, unknown, and meaningful to investigate. In this paper, the proposed Ethereum blockchain network deals with data security features of the regulated market system indicated as follows:

Decentralization: The fundamental element of this Ethereum blockchain signifies the data confidentiality on a distributing system (for any kind of data capturing, recording, updating or storing). It discharges the data-dependency on central node, which has high data security risk.

Transparency: In this work, the data script in each node written and updated transparently with trusted source in blockchain system.

Open Sourcing: Ethereum Blockchain system is very public. All data tracking can be verified publicly, and people and new applications in the system are easy to create. It itself can transfer and store revenue like a retail outlet. A transaction concerning two parties can exchange the transaction details.

Autonomous: Autonomy Chain Cloud of Ethereum Blockchain network controls the node by trusting a single head source for the entire system. The system ensures the data confidentiality so that no one can intercept it.

Immutability: In the used system, the transaction records are saved permanently and cannot be modified without having control on at least more than half of the nodes simultaneously.

Anonymity: Ethereum blockchain technologies solved the trust problem between node and node, so data transfer or even transaction can be anonymous, only needing to know the person's blockchain address.

Anonymousness: Ethereum blockchain system data transaction can be done anonymously. Knowing blockchain address suffice for any transaction.

3. Electricity Market and Data Security

This section highlights the current status of the regulated and deregulated electricity markets, the use of blockchain-based transaction and security in the electricity market, and the state of NZEM. It also provides an overview of the potential cybersecurity issues in the current electricity markets.

3.1. Traditional Data Security Issues in Regulated and Deregulated Market

In a regulated energy market like NZEM, a central control (utility company) is charged with electricity generation, distribution, and bidding. Hence the communication is restricted between the consumer's smart meter and the utility company. Most of the time, in such a traditional regulated market, communication between the different electricity nodes happens through the use of traditional communication protocols and encryption protocols, which are highly vulnerable to security threats and malicious attacks. A data breach in a single node can compromise the whole market framework leading to a chain of catastrophic events. On the other hand, in a deregulated market, consumers can decide to purchase electricity from different retailers. Since many entities (e.g., retailers, operators, consumers, etc.) can participate in active trading in a deregulated market, these different market entities may require access to different data for different purpose [19]. For example, a grid operator may require access to short-term or long-term consumption data, location and personal information of the consumer, and power quality index data such as voltage and frequency data in order to maintain grid stability. Any breach in data security on this ecosystem can pose potential harm to consumers, retailers, and operators. Since in a deregulated market the consumer is trading with different retailer, a peer to peer secure transaction and data security model can be effective against potential cyber or malicious attacks.

Leveraged with the concepts of peer-to-peer data sharing and safe transaction facility, the blockchain technology was initially utilized for fiscal security. The energy market started using this technology primarily for data trading and also for energy transmission and dispatch [3]. Traditionally,

in a regulated energy market, utility companies own and operate the electricity. The tariffs of electricity are usually set and regulated by state commissions or regulatory boards. On the contrary, in a deregulated energy market, multiple competitors can buy electricity and sell it to the retail suppliers who then set different prices for the customers. The electricity service providers or competitors in a deregulated market form a cluster with their customers. It utilizes the decentralized blockchain technology to provide the security of the data flows from each customer to competitors in the cluster and from competitors to the government entity. Since it is a peer-to-peer secured transaction model, competitors do not have access to each other’s data.

Figure 1 shows the approach of transaction in the traditional blockchain-based transaction model. As shown in the figure, a traditional blockchain is a decentralized system that stores transaction data at each peer. Data is stored in a hub-based cloud system, and the process can then be executed by developing precise smart contracts for blockchain technology. Only the authorized Government people can see different competitor’s data as shown in Figure 1, but the competitors themselves will not have access to other’s data.

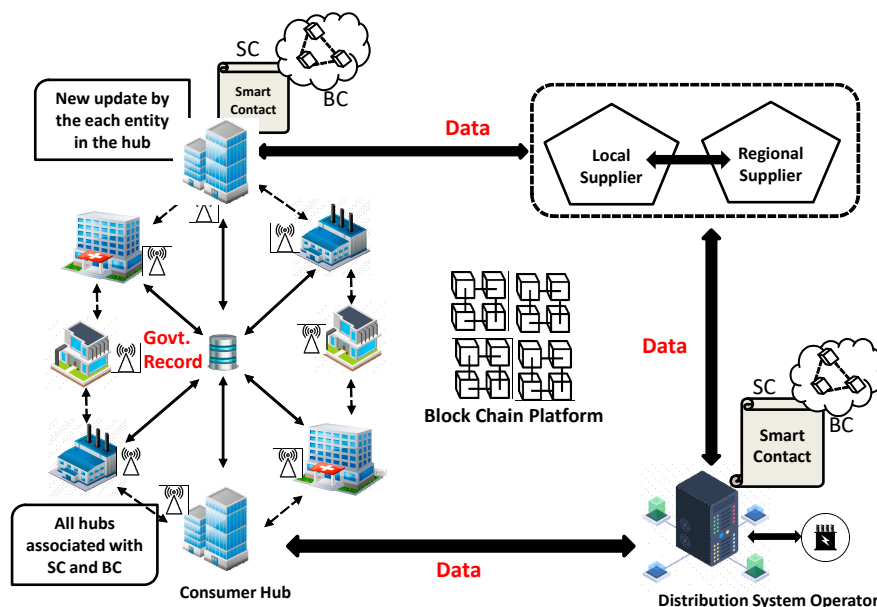


Figure 1. Traditional Blockchain based transaction model for deregulated market.

3.2. An Overview of NZEM as a Regulated Electricity Market

An electricity market is very much similar to any other market where products (in this case its electricity) are bought, sold, and traded in wholesale and retail fashion. The electricity market is thus divided into generation, transmission, distribution, and retail. The wholesale of electricity depends on power generation and connection to the grid by the transmission company. It also facilitates buying and selling of power between generators and re-sellers. The retail market is responsible to sell it to end-users. In NZEM, power generation companies can bid to supply electricity at grid injection points across the country whereas there tail companies bid for the electricity at grid exit points.

There are six principal power companies in NZEM, namely, Meridian, Con-tact, Genesis, Mighty River, Trust Power, and Todd. Half of NZEM’s electricity generation is based on hydro power and there are geothermal, wind farms, gas, biomass plants, and thermal stations as well. The generated power is then trans-mitted through the national power grid, which is owned, operated, and maintained by the state owned Transpower New Zealand. The national grid has nearly two hundred grid exit points (GXPs) throughout New Zealand, and these GXPs are the supply points for distribution networks. The line companies distribute electricity throughout New Zealand by linking the national grid, and they also sell electricity to retailers. The details of the distribution companies in

NZEM are publicly available just like other regulated market pricing and revenues. Re-tail companies in NZEM sell electricity to end-users. A list of energy retailers can be found in [20]. Retailers buy electricity at wholesale prices (contract and spot). The pricing and revenues for line companies in NZEM regulated market are fixed by the Commerce Commission. Residential users, industry buyers, and business clients all buy electricity from retail providers.

As discussed in Section 2, in a regulated market like NZEM where the entrance, policies, and pricing are state controlled, the data security threats are mostly in generation and transmission zones. On the contrary, for a deregulated market where distribution companies have no limit of revenue, the data security threat are mostly on the distribution retailer consumer zone. NZEM is a regulated market run by government bodies that keeps a check on the generation of revenues of suppliers. In such a regulated market, the entrance and price charges are entirely controlled by the government. Hence, for a model like NZEM, there are less data security threats to the information exchanged and shared between the suppliers. In recent years, like multiple other countries, New Zealand also upgraded its power system by incorporating different digital devices into the grid, turning it into a smart grid. The purpose of the smart grid deployment is to enhance the operational efficiency of the entire power system, including generation, transmission, distribution, and retail. In the smart grid, the different components of the power system can communicate with each other, and this makes the grid more “intelligent” in its overall operation. However, smart grids are more vulnerable to potential cyberattacks. The use of Supervisory Control and Data Acquisition (SCADA) system to manage smart grids makes it further vulnerable to cybersecurity threats. This is basically due to the integration of intelligent electronic devices, data concentrators, and other communication equipment. In general, cyber threats in a regulated grid infrastructure can be classified into four categories [21]: (i) Key-based attacks, (ii) Data-based attacks, (iii) Impersonation-based attacks, and (iv) Physical-based attacks. Each of these cyberattacks focuses on exploiting the features or protocols of specific entities in the grid to take control of the system.

The traditional blockchain-based transaction model for the deregulated market (explained in Figure 1) is not applicable to NZEM; rather a blockchain solution has more prospects if implemented for SCADA security as discussed in Section 4.

4. An Ethereum Blockchain Based End-to-End Security Prototype

In this section, an Ethereum blockchain prototype is presented to provide end-to-end security for the SCADA based regulated energy market. Hence, this section discusses the basic elements of a SCADA system and provides details about blockchain construction.

4.1. Overview of SCADA System

SCADA is a system of software and hardware elements used to monitor and control the NZEM. SCADA consists of different modules for monitoring, gathering, and analyzing real time system data. Functional modules of SCADA include hardware for process monitoring and process control, data acquisition module, user interface, communication modules, and software platform. The process control system of SCADA basically consists of remote terminal units (RTU's) and programmable logic controllers (PLC) that connect a series of sensors for real time monitoring and data collection.

Remote terminal unit or RTUs is a microprocessor controlled electronic device, which interfaces physical objects (such as circuit breakers) in the power grid to a SCADA system. Figure 2a illustrates the functional architecture of a SCADA system. In a high-level architecture, the functional components of SCADA can be described as below:

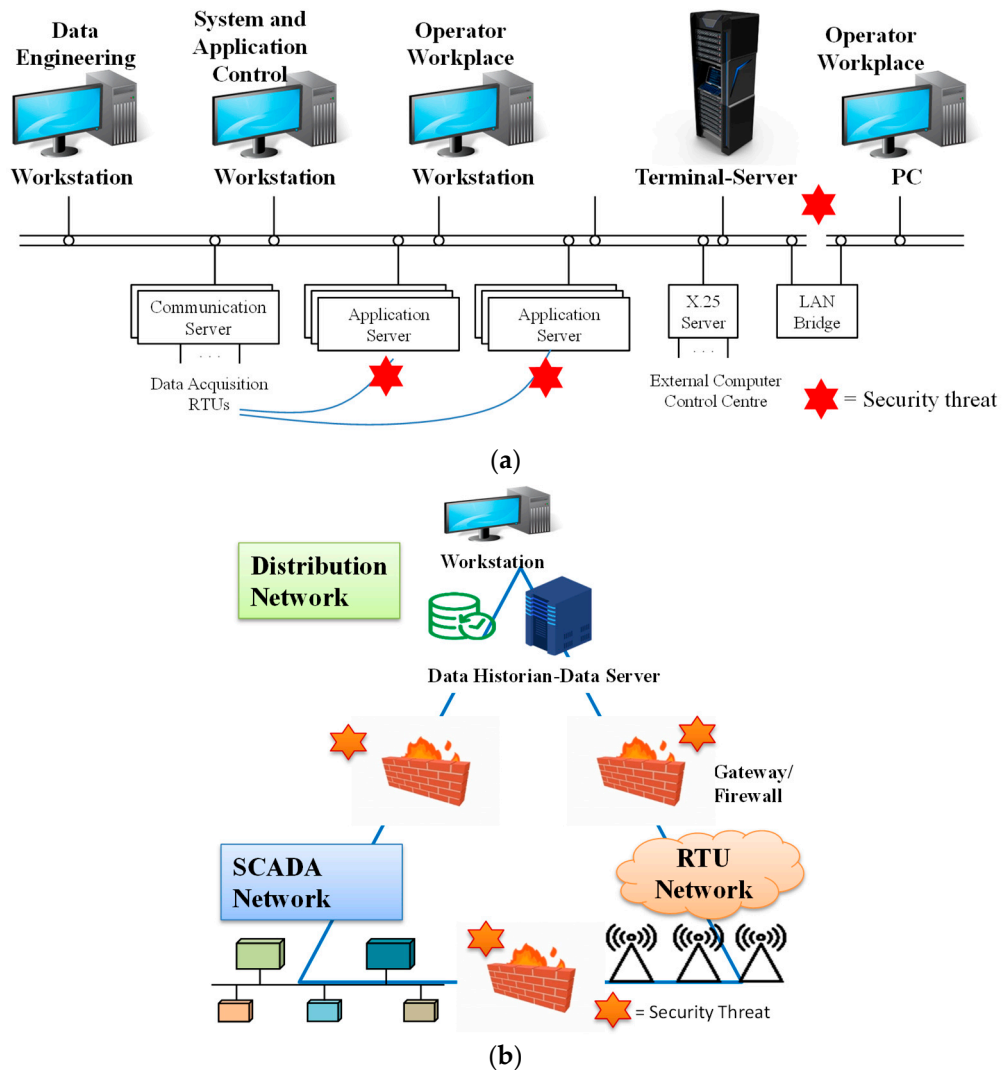


Figure 2. Prospective security threat in (a) Supervisory Control and Data Acquisition (SCADA) network (b) Gateway/firewall of internal network.

(1) Operational Equipment: Operational equipment of SCADA in a smart energy network perspective is the circuit breakers, which can be operated by actuators or relays.

(2) Local processors: These may have multiple inputs from instruments (e.g., programmable logic controller, remote control unit, intelligent electronic devices, etc.) and outputs to the operational equipment. They include PLC, RTUs, intelligent electronic devices, and automation controller for monitoring and control.

(3) Communication Module: This can be wired or wireless and facilitates communication (through analog or discrete signals) between all the different functional modules using a predefined communication protocol. On a larger scale, a long-range communication module can utilize phone network, satellites, microwave, or cellular packet data.

(4) Host Computer: It acts as the central monitoring and control point and also hosts the software platform to facilitate the monitoring and interaction.

4.2. SCADA Configuration and Smart RTU

In this proposed blockchain prototype, the Smart RTUs in the physical layer of SCADA are considered as nodes for a decentralized network. Using a cloud simulation environment, we show the effectiveness of the proposed prototype in protecting the system from cyberattacks. In the simulation,

a cloud-based SCADA network is used to accumulate, broadcast, and store data in the proposed prototype. Customized collection, transmission, and receipt of signal data between the communication and physical layer are done through the smart RTUs of SCADA. The communication path is linked through the RTU-nodes. Only authorized users, who have access to the communication, are able to certify the data acquisition and process for the reports or signaling of different process used in the production environment. Advanced metering infrastructure (AMI) plays an important role in the proposed decentralized data security system. It is envisioned that AMI should contain the following key features:

- (1) Individual smart RTU with distinctive IP address, data storage and process drive, RAM, signal sender–receiver device. All RTUs of the same layer need to be inter-channelled.
- (2) A public–private key must be used to encrypt each smart RTU.
- (3) Accessibility of bidirectional information gateway for related parties and associated systems.

In the following subsection, we are going to discuss an Ethereum blockchain prototype to facilitate an end-to-end data protection. The proposed Ethereum blockchain has three elements: (i) Block, (ii) Smart Contract, and (iii) Miner.

4.3. Block Construction

The literal meaning of blockchain is chain of blocks. A block is a container data structure, which stores key transaction information, like day and time of transaction, amount of transaction, participant in transaction, and so on. Internally, the blocks are linked by the cryptographic and hashing concepts. A hash function routes random data to meaningful preset sized data. In summary, each block is connected with one-way (i.e., data is irreversible) hash string-links and the resultant hash value is different from the previous hash values. In the process, the blocks are collision resistant, which means that if any transaction in the block is changed by an unauthorized entry, it invalidates all hash addresses of the block sequences one by one. The communication amid the client-nodes is routinely carried out without individual intervention. Figure 3 shows the construction of the chain along with the details of the contents of block connections.

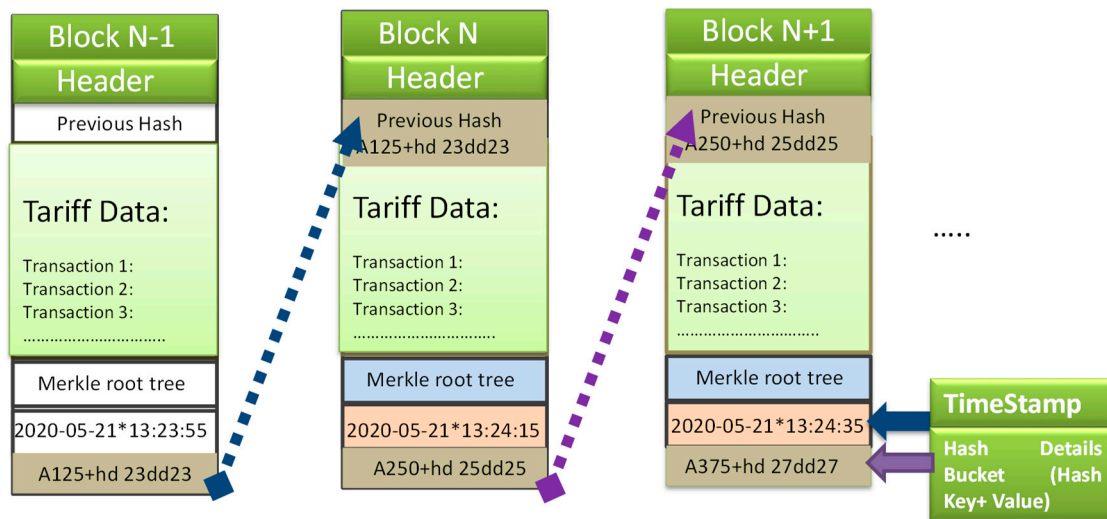


Figure 3. Construction of the chain along with the details of the contents of block construction.

4.4. Development of Ethereum Smart Contract

Smart contracts help a customer (or miner) to trade data of any value via a transparent, conflict-free system whilst preventing any third-party access. Initially, a single ledger is offered to the customer as a source of trust from blockchain, and data exchange then happens between nodes. Smart contracts are a collection set of elaborated logic, which are developed in JavaScript platform. Protected data are stored

in blockchain database and can be retrieved only by authorized users. Figure 4 shows the construction flowchart of Smart Contract and its interaction with a different layer of the SCADA system. The data monitoring is developed in Python Zerynth IDE environment [22], and the communication layer for smart RTUs is made with microchips of espressif [23].

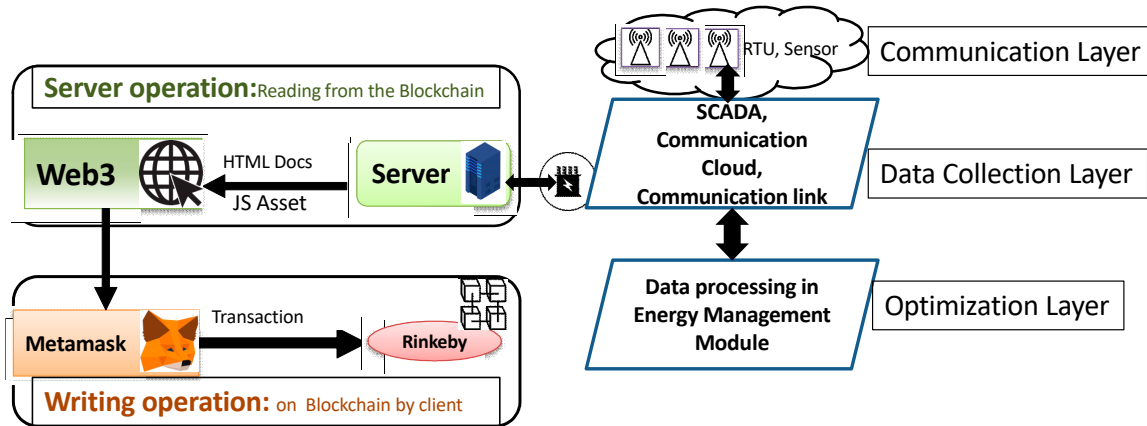


Figure 4. The Construction flowchart of Smart Contract.

Zerynth is designed to link the IoT platforms of smart RTU to cloud services. Figure 5 shows sample of a smart contract script developed for the local Ethereum node operation in blockchain. Verified smart contract data is then transferred to Rinkeby (refer to Figure 4), which is a platform of the Ethereum blockchain test network (test net) [24]. Rinkeby test net, in contrast to Ethereum main network (main net) is an authorized network.

```

import streams
# Ethereum modules
from blockchain.ethereum import ethereum
from blockchain.ethereum import rpc

# WiFi drivers
from espressif.esp32net import esp32wifi as net_driver
# for ESP-8266
# from broadcom.bcm43362 import bcm43362 as
net_driver
# for Particle Photon
from wireless import wifi

# SSL module for https
import ssl
#to read from analogue sensor
import adc

# Configuration file
import config
import math
import json
import requests

# import Real-Time Clock module
# import rtc
import timers
t=timers.timer()
t.start()

def get_epoch():
    user_agent = {"user-agent": "curl/7.56.0"}
    return
int(json.loads(requests.get("http://now.zerynth.com/",
headers=user_agent).content)['now']['epoch'])
    
```

Figure 5. A Smart contract script for local Ethereum node operation.

For the console panel, Web3-Ethereum JavaScript API is used in the project [25]. “Web3.js” is a selection of libraries that facilitates communication with local Ethereum node via IPC or HTTP connection. A deploy file and script codes are developed using HD wallet provider and web3. The HD wallet, with a public/private key tree feature, represented a master node (Meta Mask). Meta Mask is a crypto wallet for blockchain, which offers a risk-free approach on a unique decentralized web platform to link up to blockchain-based programs [26]. Moreover, Application Binary Interface (ABI) specification is used as a standard approach to communicate with contracts in the Ethereum environment.

4.5. Data Transaction Process for Mining

Ethereum is an electronic currency used for funds exchange in an encrypted system which does not depend on any legalized central banking system. The blockchain transaction system in Ethereum data framework as online payment system is described in this section.

Ethereum employs public keys to address deposits and send currency. The public keys also track the transaction details. In Ethereum blockchain systems, data exchanges or transactions are usually unseen and anonymous. The system fixes the “trust” issue in between nodes with its anonymity feature. Knowing a blockchain address provides the transaction details, which have two major sections:

Principal data: It features the details of transaction files, records, dealing, contract history, and bank clearing information.

Public data: Anyone can verify some transaction data at permitted level and can also participate in the process of getting consensus. As Ethereum is a Public Blockchain, permitted transaction details will be public, and the system can be involved in the progression of getting consensus. In Figure 6, an Encrypted process in active RTU nodes during transaction with public and private key details is shown.

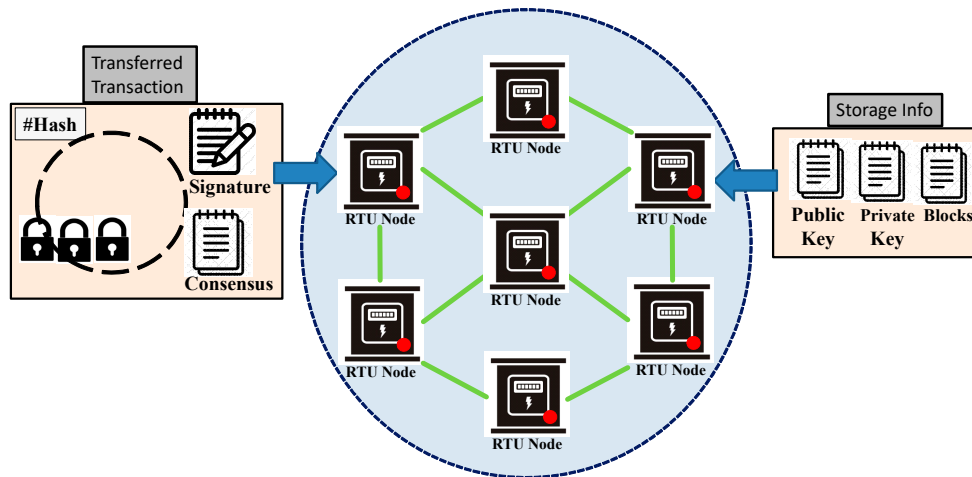


Figure 6. Encryption process in active remote terminal unit (RTU) nodes during transaction.

The transaction procedure confirms the computing potentiality to get hold of consensus and subsequently files the transaction details to network. For any authorized or unauthorized party, the unique ID is kept as necessitated. In Figure 7a, a Coinbase account for an authorized user is shown. The user can see the transaction details along with main Ethereum network details as shown in Figure 7b. The Metamask Ropsten Test Network and its transaction details are shown in Figure 7c. According to the transaction operation, there are four scenarios for transaction experienced:

- Old RTU node confirms identity and sends details to new RTU node.
- Old RTU node cannot confirm identity and failed details to new RTU node.
- New RTU node confirms identity and sends details to old RTU node.
- New RTU node cannot confirm identity and failed details to old RTU node.

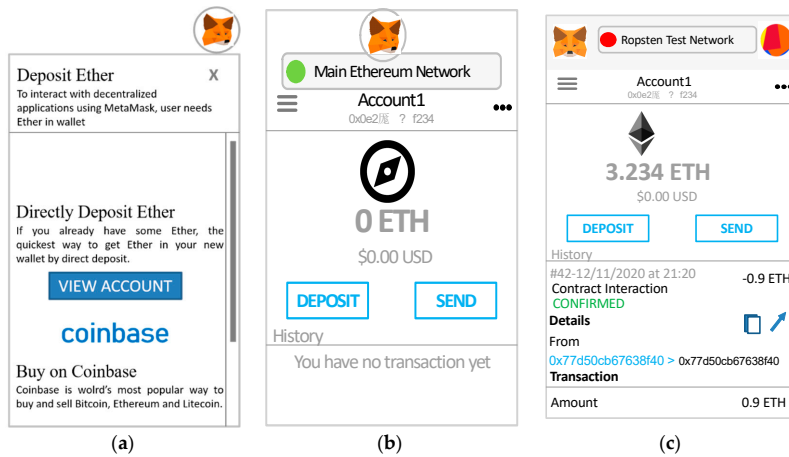


Figure 7. (a) Coinbase account to see the transaction details. (b) Main Ethereum network details. (c) Analyzing transaction details in Metamask Ropsten Test Network.

4.6. Miner Status

In blockchain technology, blocks are formed, and their content verified by miners, who compete between themselves in the process (so-called mining) of appending new blocks to the blockchain. This subsection examines the miner status based on different power data of different nodes of smart RTUs as shown in Figure 8. Etherscan, which is a block analytics as well as a block manager decentralized smart contracts platform for Ethereum, is used for this purpose. Ethers examine and browse the Ethereum platform for transaction details like encrypted data, block number, miner address, currency details, etc. (refer to Figure 9). The Meta Mask wallet uses the storing keys (like Ether and ERC20 tokens) for the Ethereum platform [27]. Samples of transactions added to the Rinkeby server are shown in Figure 9a, in which the access is given to the miner only.

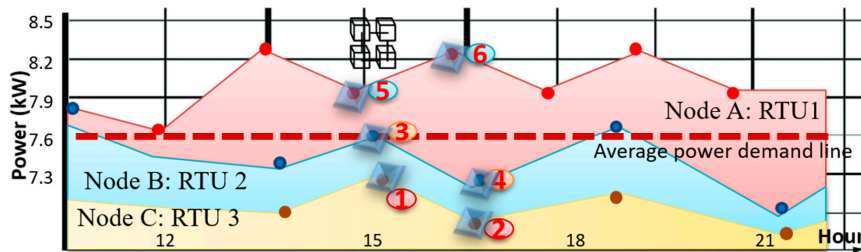
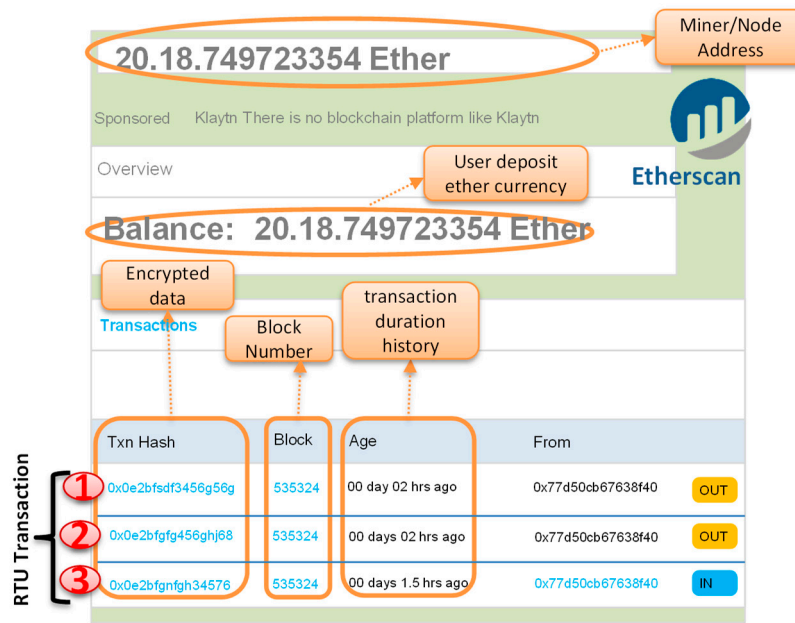
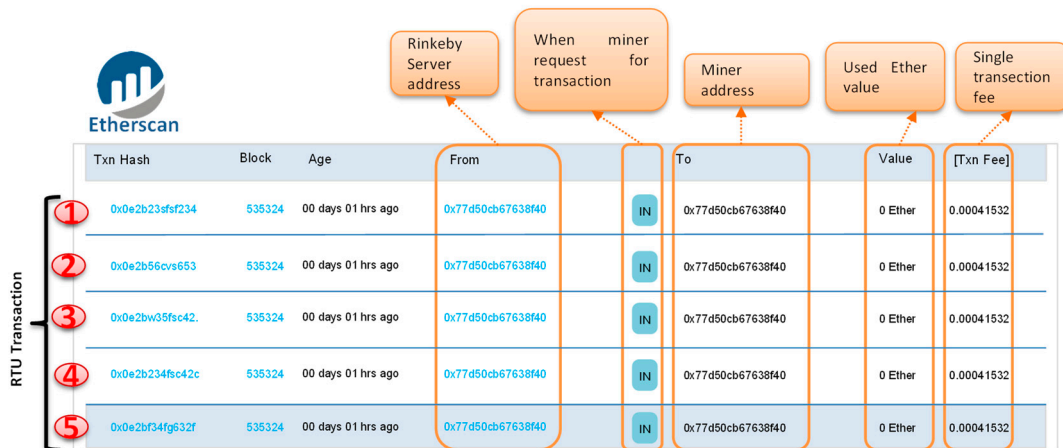


Figure 8. Chosen power data of different nodes of smart RTUs.

The monitoring status of the application layer of the SCADA system is indicated by the status OUT. Moreover, Figure 9b shows the detailed analysis of the transaction in which the miner sends the request for transactions to the Rinkeby server. The hash and miner address details can be derived from the Rinkeby server address. The integer Ether values and transaction fees show the Ether balance used for the individual transaction.



(a)



(b)

Figure 9. (a) Transaction added in the Rinkeby server. (b) Inspecting the smart-contract balance on Etherscan.

Figure 8 shows the power data of different companies and Figure 9 examines the associated transaction details for the same. It is found that peer-to-peer data transaction is secured through hash transaction. Any unauthorized party can just view the transaction as hashed message but cannot retain the original values or written text. It is evident from the miner status that the addresses are unique and can be accessed only by permitted parties. Moreover, peer-to-peer data transaction of Figure 9b shows that the Rinkeby server addresses for all five power data of the three different companies are unique. Therefore, any unauthorized entry has no chance of false data injection through the RTUs/Rinkeby address.

5. Conclusions

This paper proposes a decentralized Ethereum blockchain-based safety prototype for better data security of the regulated power market. The proposed prototype considerably promotes self-defensive functionality against cyber-attack and is an advancement towards data safety in power systems.

Substantial technical discussions in the context of the existing power systems are highlighted in this paper. The transaction performed is used to address the above-mentioned issue.

One way the proposed system is protecting the data from energy market from manipulation or fraud is utilizing the immutability characteristic of the blockchain framework. The proposed system uses ledgers to store the data and each block of the data is stored using a unique hash value. This feature ensures that the data stored cannot be manipulated by an external entity. Moreover, the proposed framework is decentralized, which makes it impossible for an external entity to compromise the market data using cyberattack such as DDoS.

Author Contributions: Conceptualization, analysis, methodology, and experiments, A.U.; manuscript preparation, A.U., S.M.S.S., and M.A.H.; data curation, A.U., writing—review and editing, A.U., S.M.S.S., M.A.H., and S.K.R. All authors have read and agreed to the published version of the manuscript.

Funding: The research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. IEA. World Energy Outlook 2019—Analysis. Available online: <https://www.iea.org/reports/world-energy-outlook-2019> (accessed on 20 August 2020).
2. Kim, S.K.; Huh, J.H. A study on the improvement of smart grid security performance and blockchain smart grid perspective. *Energies* **2018**, *11*, 1973. [[CrossRef](#)]
3. Mylrea, M.; Gourisetti, S.N.G. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale, and security. In Proceedings of the 2017 Resilience Week (RWS), Wilmington, DE, USA, 18–22 September 2017; pp. 18–23.
4. Luo, F.; Zhao, J.; Dong, Z.Y.; Chen, Y.; Xu, Y.; Zhang, X.; Wong, K.P. Cloud-based information infrastructure for next-generation power grid: Conception, architecture, and applications. *IEEE Trans. Smart Grid* **2015**, *7*, 1896–1912. [[CrossRef](#)]
5. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* **2016**, *32*, 3317–3318. [[CrossRef](#)]
6. Kosut, O.; Jia, L.; Thomas, R.J.; Tong, L. Malicious data attacks on the smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 645–658. [[CrossRef](#)]
7. Liang, G.; Zhao, J.; Luo, F.; Weller, S.R.; Dong, Z.Y. A review of false data injection attacks against modern power systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1630–1638. [[CrossRef](#)]
8. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. A framework for cyber-topology attacks: Line-switching and new attack scenarios. *IEEE Trans. Smart Grid* **2019**, *10*, 1704–1712. [[CrossRef](#)]
9. Xie, L.; Mo, Y.; Sinopoli, B. Integrity data attacks in power market operations. *IEEE Trans. Smart Grid* **2011**, *2*, 659–666. [[CrossRef](#)]
10. Liu, X.; Li, Z.; Li, Z. Optimal protection strategy against false data injection attacks in power systems. *IEEE Trans. Smart Grid* **2016**, *8*, 1802–1810. [[CrossRef](#)]
11. Kong, W.; Dong, Z.Y.; Hill, D.J.; Luo, F.; Xu, Y. Improving nonintrusive load monitoring efficiency via a hybrid programming method. *IEEE Trans. Ind. Inform.* **2016**, *12*, 2148–2157. [[CrossRef](#)]
12. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Big Island, HI, USA, 13–17 March 2017; pp. 618–623.
13. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Tech. Rep.; 2019. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 20 August 2020).
14. Ferrer, E.C. The blockchain: A new framework for robotic swarm systems. In Proceedings of the Future Technologies Conference, Vancouver, BC, Canada, 15–16 November 2018; Springer: New York, NY, USA, 2018; pp. 1037–1058.
15. Bao, J.; He, D.; Luo, M.; Choo, K.-K.R. A Survey of Blockchain Applications in the Energy Sector. *IEEE Syst. J.* **2020**, 1–12. [[CrossRef](#)]
16. Liang, G.; Weller, S.R.; Luo, F.; Zhao, J.; Dong, Z.Y. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Trans. Smart Grid* **2019**, *10*, 3162–3173. [[CrossRef](#)]

17. Gao, J.; Asamoah, K.O.; Sifah, E.B.; Smahi, A.; Xia, Q.; Xia, H.; Zhang, X.; Dong, G. Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid. *IEEE Access* **2018**, *6*, 9917–9925. [[CrossRef](#)]
18. Cheng, S.; Zeng, B.; Huang, Y. Research on application model of blockchain technology in distributed electricity market. In *IOP Conference Series: Earth and Environmental Science*; Art. No. 012065; IOP Publishing: Bristol, UK, 2017; Volume 93.
19. Strücker, J.; Kerschbaum, F. *From a Barrier to a Bridge: Data-Privacy in Deregulated Smart Grids*; AIS eLibrary: Atlanta, GA, USA, 2012.
20. Electricity. Available online: <https://www.powerco.co.nz/Get-Connected/Electricity/2> (accessed on 20 August 2020).
21. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustain. Cities Soc.* **2018**, *38*, 806–835. [[CrossRef](#)]
22. Enabling IOT (May 2020). Available online: <https://www.zerynth.com/> (accessed on 20 August 2020).
23. ESP Rainmaker. Available online: <https://www.espressif.com/> (accessed on 20 August 2020).
24. Ethereum Testnet. Available online: <https://www.rinkeby.io/#stats> (accessed on 20 August 2020).
25. web3.js—Ethereum Javascript API. Available online: <https://web3js.readthedocs.io/en/v1.2.6> (accessed on 20 August 2020).
26. Lee, W.M. Using the meta mask chrome extension. In *Beginning Ethereum Smart Contracts Programming*; Springer: New York, NY, USA, 2019; pp. 93–126.
27. Dannen, C. *Introducing Ethereum and Solidity*; Apress: Berkeley, CA, USA, 2017; Volume 1.

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).