Securing the Smart Grid: A Blockchain-based Secure Smart Energy System

George Suciu, Mari-Anais Sachian, Marius Dobrea, Cristiana-Ioana Istrate, Ana Lavinia Petrache
R&D Department
BEIA Consult International
Bucharest, Romania
george@beia.ro, anais.sachian@beia.ro,
marius.dobrea@beia.ro, cristiana.istrate@beia.ro
ana.petrache@beia.ro

Alexandru Vulpe, Marius Vochin
Telecommunications Department
University POLITEHNICA of Bucharest
Bucharest, Romania
alex.vulpe@radio.pub.ro, marius.vochin@upb.ro

***Abstract*—This paper presents how a Smart Grid system is secured and how blockchain implementation provides confidentiality and integrity for such a system. One main issue that has to be addressed in smart grid systems is databases security. Blockchain has been proven to be a safe alternative to be used in mining systems because it allows a secure applicability in databases. Another important feature is that each hash in a crypto mining system cannot be changed if it has such an algorithm behind its build, thus resulting in a secure and reliable system. This paper aims to show how blockchain can affect and be used in a smart power management system going forth from the SealedGRID platform. This system enables the user to monitor in real time the power usage in a smart grid system, therefore, this platform being built with security and resilience against attacks in mind.**

***Index Terms*--blockchain, cryptocurrency, smart energy, Smart Grid, smart meter**

I. Introduction

This paper presents the applicability of Blockchain in the use case of a photovoltaic panel system that supplies a building and the surplus energy that is used for data mining. The photovoltaic systems (PV) [1] used in other countries are discussed to be implemented with the integration of a decentralized distribution network using Blockchain. Energy systems are undergoing rapid transformations in increasing the number of renewable energy sources such as PV and wind energy. In 2016 it was observed that 24.6% of gross electricity consumption in the United Kingdom was generated by Renewable Energy Sources (RES), mainly from onshore and offshore wind farms, and photovoltaic panel plants, representing 44.9% and 12.5% of the total 35.7 GW installed RES capacity. In the case of Germany, in 2018, it was observed that 40% of gross electricity consumption was generated by Renewable Energy Sources (RES), mainly from onshore and offshore wind farms, representing 50% and 40% of the total 117.88 GW installed RES capacity. RES is variable, and it is difficult to predict the weather conditions, which generate new challenges in the management and operation of electrical systems, as more flexibility measures are needed to ensure safe operation and stability [1].

The energy transition from centralized power plants to distributed energy assets challenges existing utility business models due to higher market participation of customers and coordination of an increasing number of Internet of Things (IOT) devices. Simultaneously, innovations of blockchain technologies, such as the inclusions of an application layer in Ethereum have been portrayed as a potential building block to address these challenges. Despite being discussed extensively in the press, the academic community has identified substantial research gaps regarding the technology [2]. The solution in this article has a base on the development of an architecture monitoring the electricity consumption of miners using blockchain technology. The structure of the architecture is made of photovoltaic panels that are connected to the inverters and ensures the production of electricity that is monitored via the IoT Verbund [3] device, whereas the monitoring of electricity consumption, the Fibaro [4] smart plugs are used.

Section II of the paper presents the Related Work, where the primary data mining systems are described. Then section III presents the security of the equipment used in the architecture for the electrical power consumption of the building. Section IV illustrates the smart power management of Beia’s building consisting of the inverters to which the photovoltaic panels are connected, together with the IoT Verbund device and the Fibaro electrical energy monitoring devices. Going forth, in section V the system architecture of the SealedGRID project is defined, and finally, in section VI, the results are concluded.

II. Related Work

Many advances were made in the electronic field and as well in the money sector regarding blockchain technology and also how the power management is done. But most important discoveries were made in the blockchain field. The most used electrical devices in the blockchain field are graphics processing units (GPUs), Field Programmable Gate Arrays FPGAs and Application-Specific Integrated Circuit (ASIC). One of the main contributors to this type of devices were Xilinx [5].

The Smart Energy Grid (SEGs) [6] integrates a cost-effective fault-tolerant ICT high technology-based system, which focuses on data exchange between nodes.

The presence of renewable energy resources, although with some limitations, allows for locally distributed energy production. The concept of MicroGrid is a case of SEGs and such a system is an intelligent network, a case of SEGs, that can manage renewable energy resources and energy demands from consumers. It has in its structure a house consisting of photovoltaic panels, a storage device, and system user's platform.

A traditional power grid system delivers power from a few central generators to a group of users. However, smart grid systems use two-way flows of electricity and information. In this way, a smart grid system builds an energy delivery network with advantages like security, reliability, resilience, efficiency, and sustainability. In this matter, MicroGrid uses a Blockchain system.

The Blockchain system is part of the ICT technology. A blockchain network can provide a user-friendly application for managing power consumption. A blockchain consists of a ledger and a consensus mechanism. It also needs a cryptographic algorithm for hashing. The ledger is a register that is replicated between blocks. The consensus mechanism has the purpose of avoiding sending corrupted information further and uses proof-of-work (PoW) in which the participating nodes must solve a numerical problem [7].

A Blockchain network is composed of blocks that contain registers. These blocks are chained together using a linked list of hash pointers. If they suffer changes, re-hashing of previous blocks is needed. A register change can lead to inconsistencies e.g. when the hash pointer changes [8].

An advantage of blockchain is the tamper proofing of all transactional information. This means that all the transactions are distributed among the nodes of a peer-to-peer network. Each registered transaction is sent to all peer nodes for validation [8], thus making blockchain a secure way to protect data in Smart Grid Systems.

However, in Smart Grid systems can occur threats against smart energy security. One of them is that the variation of energy level, that is delivered, can bring power outages, overload and it can disturb energy devices. To solve such an issue, one approach which can be taken is to decrease the output of energy sources to avoid malfunctioning on the entire grid operation. This decision depends on Distributed Energy Prosumers.

Other attacks [9] against smart meter networks are: The Jabbering attack that takes place on end-to-end links were the attacker places a malicious smart meter which sends flooding traffic, causes de-synchronizations, so connection is interrupted. Other examples of attack include fake control signals, re-synchronizing, and puppet attack. In the latter, the attacker is disguised, so it can send messages in the network. When a node receives these messages, it can be controlled by the attacker. This puppet node sends more messages in the network, consuming network's energy and resources. Puppet attacks can reduce 20-10% of message delivery ratio, so the smart grid metering network is affected. Another malicious act seen in smart grid systems is the Stack smashing attack which takes place at the network application layer and causes damage to the operating system. Also, the action of overwriting/overloading of memory buffers with bogus data that can be more than the memory can handle, can cause disclosure of sensitive data, which can be manipulated by the attackers. Experimental attacks demonstrated that application layer (software, user access) of the smart grid layer is vulnerable to DoS attacks, but also to Jamming attacks on radio spectrum: a high frequency causes connection failure and the Routing part of a smart grid network is vulnerable to Dos attacks. As a result, Smart Grid systems have to be secure from such attacks, so it can provide predictability and reliability.

III. Security for the SealedGRID Architecture

The SealedGRID architecture comprises a Remote Attestation Mechanism (RAM) which provides identity verification, security for trust computing and allows the remote party to prove the trustworthiness of operating systems and software. Also, they enable remote authorized entities to detect changes in static files (e.g., configuration files) and runtime attestation for executable programs for improving resistance to malware. Anonymization of trusted computing operations is applicable to bidirectional communications along with the remote attestation.

Within SealedGRID, the RAM is included in the Trusted Execution Environment (TEE), whereas the Cryptographic Storage is included in this environment. In this way, data received by the platform is protected. TEE provides confidentiality and integrity and is applied for generation and storage of cryptographic keys, generation of random numbers, executing cryptographic operations and securing storage of the certificates.

SealedGRID will also make use of the blockchain technology, the basic concept of it being that it uses the process of the distributed database which performs some transactions that are entirely open to the participants. The blockchain system verifies all the operations that are made, and once the transaction is done, it keeps track of all the transactions, therefore being impossible to destroy those records. The blockchain gives a real verification to the transactions and keeps a solid record which can never be misguided [10]. Blockchain technology can be used for all multi-level transactions where high traceability and visibility is needed. The supply chain taken as an example specifies where the lockout can influence the management and signing of contracts and enables the control of the originality of a product. Each block contains the information about a "transaction", stored secured and encrypted. These blocks are chronologically arranged in the form of a chain with a few particularities [11]:

- a blockchain cannot be modified without altering all the next blocks in the chain;
- the entire chain is stored decentralized, on the computers of all participants or, finally, on many computers.

These two features of the blockchain are crucial because they make the information, which is already on multiple computers in the world, impossible to modify. If you modify a block, all of the following blocks signal that something is wrong, and since many people already have the original version of the chain, any attempt to make a change in the chain would be immediately noticed. It is a very secure method of recording data, making sure that it cannot be modified or tampered with in the future without the majority's agreement.

The blockchain splitting graph is shown in Fig. 1, where the black blocks represent the main blockchain, the red block is the initial one, and the cyan blocks are “orphans” that can be parts of the other chains.

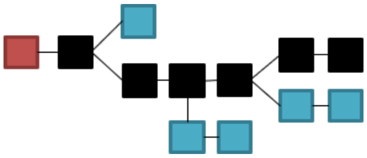


Figure 1. Graph of blockchain splitting [9]

IV. Smart Power Management

The purpose of experimenting with a photovoltaic system [12] was to see how the surplus energy made by the panels will influence the outcome of how much Ethereum will be generated by the GPU’s. Experimentations were made during the months of July and August 2018 when it has been observed that the photovoltaic panel system generates a significant surplus of energy. If the energy produced by the panels is not enough, then no more Ethereum will be produced, meaning that the incomes received by company will be lower. Such an outcome may arise because of cloudy days when there is only a small amount of sun energy. Since there was no need to transport electricity to the national energy system, we used the energy produced by the photovoltaic system for the mining system, as it is the simplest and most efficient solution for using surplus energy based on a blockchain system. The energy resulting from the variation between the surplus energy and the consumed energy enables the GPU feed to generate the corresponding Ethereum.

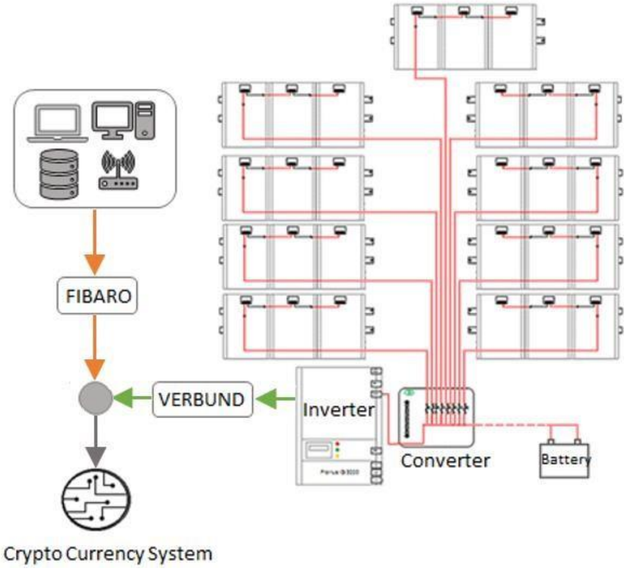


Figure 2. BEIA Power Consumption System

BEIA’s photovoltaic system, presented in Fig. 2, consists of 66 photovoltaic panels with a maximum power of 255W. In order to have the best efficiency in energy transportation and transformation from Direct Current into Alternating Current, the panels must be connected in series of three and then in parallel, so produced power by the panels is approximately 17000 W. One of the devices used by the system is the Verbund device, which aims to transmit the output parameters of an inverter to a visualization platform. The Verbund equipment records the desired parameters and can forward them by dialing the address [REST/JSON] of the JSON type. This call can only be made if it is in the same wireless network. With the help of the IoT2020 Siemens device, the data from the Verbund equipment is being transmitted via the MQTT (Message Queuing Telemetry Transport) protocol to the mqtt.beia-telemetry.ro server with a precise sampling period. After the data is sent, the Grafana platform takes the data from the server with the mqtt.beia-telemetry.ro link and the necessary parameters. Afterwards it displays it as a graph to make it easier to understand the events at the inverter level. The evolution in time of the electricity consumed and the produced energy monitored between the 10th of July and the 17th of August indicates the existence of surplus energy throughout the period, as shown in Fig. 3. The period is represented by 30 working days in the 9-18-hour range because it is necessary to change the number of used GPUs manually.

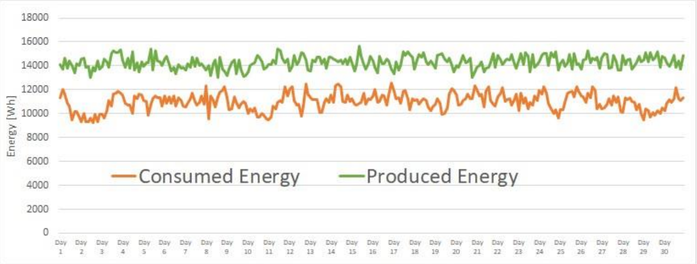


Figure 3. The evolution in time of the electricity consumed and the produced energy

Throughout the testing phase, it has been noticed that the average energy surplus value is 3315 W, going forth from the recorded data. The maximum amount of 5415 W which was monitored on day 29 and the minimum of 1113 W on day 16 presents the variation between the two values which comes from the activities performed at the headquarters, such as working days, meetings. It is noteworthy that every two weeks the consumption on the fifth working day, Friday, had an increasing tendency as seen in Fig. 4.

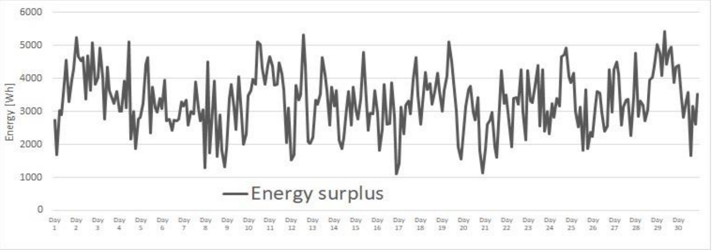


Figure 4. The evolution in time of the energy surplus

V. SEALEDGRID ARCHITECTURE AND IMPLEMENTATION

A. *Architecture*

This section presents the SealedGRID architecture and its main components, as seen in Fig. 5. The Smart Meter is placed within a house or building, its purpose being to collect the readings of the electricity consumption. The Aggregator represents the binder between the collector and the smart meters. It has the role to sum all the readings received by the meters and transmit the results to the Utility. In this way, data becomes available without putting too much load on the Utility.

The role of the Utility device is to accumulate high-frequency aggregated values, and to use them later as it is a demand for a response, or to sum these values, in the end resulting the total grid consumption. It can also be used for billing by computing the total consumption of a customer at the end of a billing period. The functions of the Utility are Federated Login, Access Control/Policy Maker, Key Management, TEE.

The SealedGRID architecture is especially based on the following requirements: End-to-End Security, Data-Driven Systems (Monitor→Analyse→Act), Platforms and Support Devices, Cross-Cutting Functionality, Tiered Approach, configurability, and Programmability. The Cross-Cutting functionality is necessary for the protection and the security of all layers of a smart grid. End-to-End Security provides security across all different layers and all the devices. The Tiered Approach will collect and process information both close to IoT devices and at a cloud level. Data-Driven Systems will be used for the SealedGRID project and will support the development of smart grid blockchain based monitoring platform. These types of systems are based on the collection and the processing of security-related data to assess risks, identify and visualize threats and produce alerts. The SealedGRID architecture should be the support for the protection of different Smart Grid platforms and devices. The last requirement, configurability, and programmability are necessary to make the architecture of SealedGRID project more flexible in accommodating different security mechanisms in a configurable and programmable fashion.

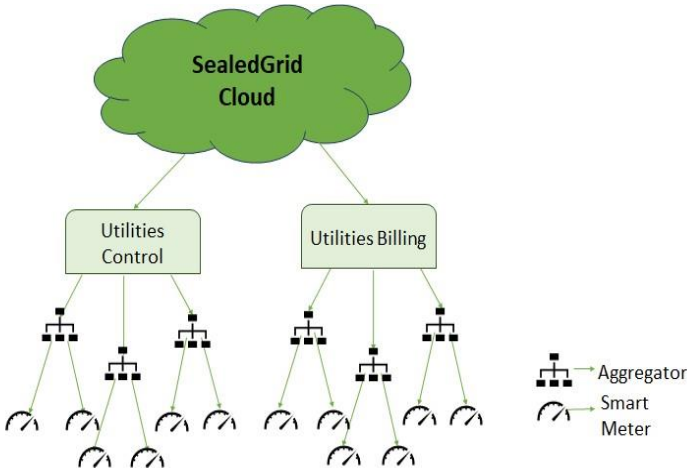


Figure 5. SealedGRID Architecture Overview

B. *Implementation*

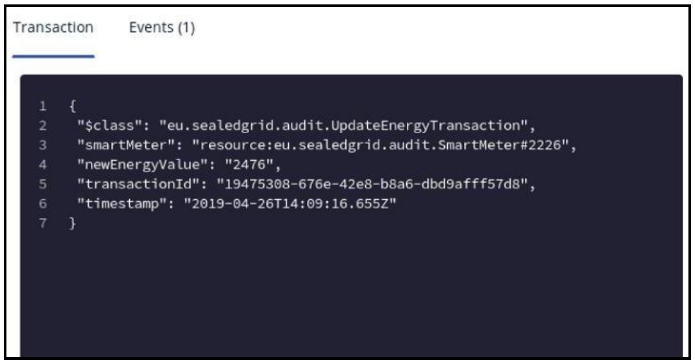
The SealedGRID project aims to develop a solution by equipping each participant entity with multiple modules. The targeted clients for the SealedGRID platform are represented by the households which will use the produced energy. Regarding the energy consumption, the SealedGRID project will allow the households to manage in real-time their energy consumption and even to work as energy producers.

Another objective is to implement a scalable, highly trusted and interoperable SealedGRID security platform which can be applied to existing systems, e.g. SCADA. The authentication in the platform will assume digital certificates using Web of Trust and Blockchain technologies.

As entities, the designed blockchain scheme will include the participants (e.g. Domain, Viewer, Operator, Installer, SecAdm, RBACAdm, ContextManager, AccessManager), assets (e.g. SmartMeter, Aggregator, Utility, Policy, Role), transactions and events.

The tool used to develop the application is Hyperledger Composer, a programming model including a modeling language and a set of APIs in order to define and export business networks and applications that permit participants to create transactions which exchange assets. All transactions that belong to a business network are stored on the blockchain ledger, while the current state of assets and participants are stored in the blockchain state database. The blockchain spreads the ledger and the state database across a set of peers and guarantees consistent updates to the ledger and database are consistent across all peers using a consensus algorithm.

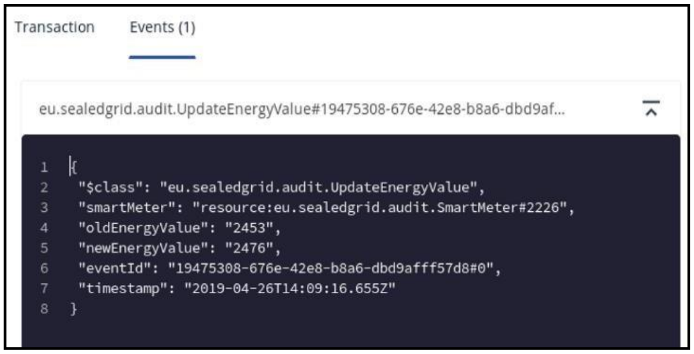
Using Hyperledger, we implemented the necessary codes for doing the needed transaction. As an example, a transaction that states the modification of the energy value at 2476, is displayed in Fig. 6.



```
{
 "$class": "eu.sealedgrid.audit.UpdateEnergyTransaction",
 "smartMeter": "resource:eu.sealedgrid.audit.SmartMeter#2226",
 "newEnergyValue": "2476",
 "transactionId": "19475308-676e-42e8-b8a6-dbd9afff57d8",
 "timestamp": "2019-04-26T14:09:16.655Z"
}
```

Figure 6. Update transaction defined in Hyperledger

Fig. 7 presents the event that shows the modification of the previous energy value of 2453 to the new value of 2476. This event will be able to be further used by any interested application that can be developed on top of this setup.

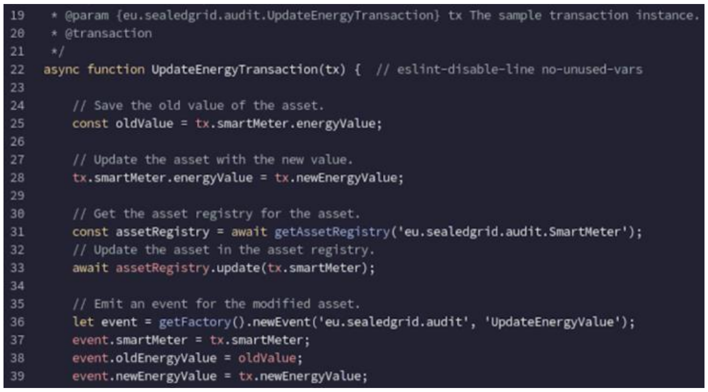


eu.sealedgrid.audit.UpdateEnergyValue#19475308-676e-42e8-b8a6-dbd9af...

```json
{
 "$class": "eu.sealedgrid.audit.UpdateEnergyValue",
 "smartMeter": "resource:eu.sealedgrid.audit.SmartMeter#2226",
 "oldEnergyValue": "2453",
 "newEnergyValue": "2476",
 "eventId": "19475308-676e-42e8-b8a6-dbd9afff57d8#0",
 "timestamp": "2019-04-26T14:09:16.655Z"
}
```

Figure 7. Update event defined in Hyperledger

The JavaScript code implemented in Fig. 8, exemplifies the updating procedure of the energy object, generating the corresponding transactions and events in the blockchain. JSON files showing the transaction (Fig. 6) and the event (Fig. 7) are given as an example.



```javascript
  * @param {eu.sealedgrid.audit.UpdateEnergyTransaction} tx The sample transaction instance.
  * @transaction
  */
async function UpdateEnergyTransaction(tx) {  // eslint-disable-line no-unused-vars

    // Save the old value of the asset.
    const oldValue = tx.smartMeter.energyValue;

    // Update the asset with the new value.
    tx.smartMeter.energyValue = tx.newEnergyValue;

    // Get the asset registry for the asset.
    const assetRegistry = await getAssetRegistry('eu.sealedgrid.audit.SmartMeter');
    // Update the asset in the asset registry.
    await assetRegistry.update(tx.smartMeter);

    // Emit an event for the modified asset.
    let event = getFactory().newEvent('eu.sealedgrid.audit', 'UpdateEnergyValue');
    event.smartMeter = tx.smartMeter;
    event.oldEnergyValue = oldValue;
    event.newEnergyValue = tx.newEnergyValue;
```

Figure 8. Energy update code in JavaScript

VI. CONCLUSIONS

This paper has presented the applicability of blockchain technology in a smart power management system, the security, and energy issues encountered in the experimentation phase and the proposed architecture for a Blockchain-based secure smart energy system.

As seen in the experimentation phase, the usage of surplus energy data in the mining system has resulted in the productionof 0.075 Ethereum/day relative calculated on an average basis.

As future work, the system will transmit the necessary data about the energy consumption and the energy produced in the Node-Red of the IoT2020 Siemens equipment, using a relay in order to power the GPU boards to cover up the surplus energy.

ACKNOWLEDGMENT

This work has been supported by “European Union’s Horizon 2020 research and innovation program under grant agreement No. 777996 (SealedGRID project) and No. 787002 (SAFECARE project)”.

REFERENCES

[1] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. Mccallum, and A. Peacock, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” Renewable and Sustainable Energy Reviews, vol. 100, pp. 143–174, 2019.

[2] M. Utz, S. Albrecht, T. Zoerner, and J. Strüker, “Blockchain-Based Management of Shared Energy Assets Using a Smart Contract Ecosystem,” Business Information Systems Workshops Lecture Notes in Business Information Processing, pp. 217–222, 2019.

[3] “Business Customers,” VERBUND – Austria's leading electricity company. [Online]. Available: https://www.verbund.com/en-at. [Accessed: 01-May-2019].

[4] F. D. Department, “FIBARO | Home Automation - Smart Home,” fibaro.com. [Online]. Available: https://www.fibaro.com/en/. [Accessed:01-May-2019].

[5] S. M. Trimberger, “Three Ages of FPGAs: A Retrospective on the First Thirty Years of FPGA Technology,” Proceedings of the IEEE, vol. 103, no. 3, pp. 318–331, 2015.

[6] A. Pieroni, N. Scarpato, L. D. Nunzio, F. Fallucchi, and M. Raso, “Smarter City: Smart Energy Grid based on Blockchain Technology,” International Journal on Advanced Science, Engineering and Information Technology, vol. 8, no. 1, p. 298, 2018.

[7] S. Zoican, M. Vochin, R. Zoican, and D. Galatchi, “Blockchain and Consensus Algorithms in Internet of Things,” 2018 International Symposium on Electronics and Telecommunications (ISETC), pp. 1-4, 2018.

[8] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, “Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids,” Sensors, vol. 18, no. 2, p. 162, 2018.

[9] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. Dong and A. Martin, “Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues,” IEEE Communications Surveys & Tutorials, pp. 1-1, 2019.

[10] J. Kaderabek, “Integration of Fibaro system to intruder and hold-up alarm systems,” 2017.

[11] F. Glaser, “Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis,” Proceedings of the 50th Hawaii International Conference on System Sciences (2017), 2017.

[12] G. Suciu, A. Pasat, R. Coanca, and S. Secu, “The adoption of photovoltaic solutions for increasing energy efficiency within SMEs,” 2017 14th International Conference on Engineering of Modern Electric Systems (EMES), 2017.