Using Blockchain For Smart Electrical Grids

Igor Kotsiuba
G. E. Pukhov Institite for Modeling in Energy Engineering, National Academy of Sciences of Ukraine
Kyiv, Ukraine

Artem Velykzhanin
Computer Science and Engineering department, Volodymyr Dahl East Ukrainian National University
Severodonetsk, Ukraine

Oleg Biloborodov
Central Research Institute of Armament and Military Equipment of Armed, Forces of Ukraine
Kyiv, Ukraine

Inna Skarga-Bandurova
Computer Science and Engineering department, Volodymyr Dahl East Ukrainian National University
Severodonetsk, Ukraine

Tetiana Biloborodova
Computer Science and Engineering department, Volodymyr Dahl East Ukrainian National University
Severodonetsk, Ukraine

Yury Yanovich
Bitfury, Amsterdam, Netherlands

Viacheslav Zhygulin
Bitfury, Amsterdam, Netherlands

Abstract—Smart Grids are an emerging technology promising significant changes in the economy and society. One among many challenges in their development and distribution is security. Considering both the recent attacks on energy grids as well as the distributed structure of these systems, the traditional means of cyber protection are not sufficient, and investigations have become more difficult—and even, in some cases, impossible. In this article, we introduce a few applications for smart grid forensic science, discuss the opportunities, and outline the open issues in the topic. We review the opportunities and challenges for forensic investigations in blockchain-based Smart Grids and propose a decentralized transaction platform custom designed for the energy sector that supports many recent innovations including advanced metering infrastructure, distributed generation, etc.

Keywords—*smart grid, blockchain, forensics, data.*

I. INTRODUCTION

Nowadays, the Smart Grid has become the vector of the energy policy of many countries. Global competition in the field of energy efficiency in the economy has shifted mainly to the formation of intelligent energy networks. Key objectives in the implementation of Smart Grids are energy security, economic growth and environmental sustainability.

The presence of Smart Grids signals a complex transformation of electrical generation and electricity sharing into a new paradigm of flexible integrated transmission and distribution systems. Their development is associated with modernization of the whole range of power generation, transition and consumption based on improved management, protection, and optimization of the technological elements of the electric power system. The use of renewable energies also requires fine-tuning, concurrence, and numerical regulation of energy production [1]. Hence, the following three main characteristics of the electric world can be summarized as:

- intelligence (smart systems, energy saving, targeted power supply) [2, 3];
- systematic (integrated regulation technology, electric power storage technology, decentralization, direct Peer-to-Peer (P2P) energy trading, multidirectional trading within a local area) [4–6];
- greening (renewable energy, alternative fuel for transport, carbon markets) [7, 8].

The concept of innovative transformation in the electric power industry provides for the construction of a fully integrated, self-regulating and self-renewable system with network topology with all generating sources, local and separate networks and all types of consumers of the electrical grid. One example can be found in PowerMatcher, a self-sufficient distribution system that includes both distributed generation and loads arising from appliances and other physical devices that integrates distributed energy resources in the operation of the electricity system and meets the requirements for privacy protection, openness and scalability [3]. In general, there are many benefits to a digital power grid. However, this digital complexity comes with vulnerability and is a serious concern for researchers. Cybersecurity is a very real issue at the application, network and physical layers of Smart Grid infrastructure [9]. This is further

complicated by interoperability and proprietary nature of technologies, wireless interference, etc. One of the promising solutions in this area is to apply other sophisticated techniques able to counteract cybercriminals and support smart grid communication infrastructure. This new idea that applies Smart Grid security on blockchain- based platforms is currently being researched by several researchers around the world [10–13].

Since 2008, there have been several attempts to build blockchain-based green energy trading platforms and energy markets [14, 15]. Meanwhile, legal institutions have not established the applicable regulations, and the application of blockchain to Smart Grids does not seem immediately obvious [16]. However, these grids are being built and cyber risks are a part of their objective reality. To find a solution to this issue is essential.

The idea of applying cyber forensic science for protection blockchain-based Smart Grid platforms being researched by few computer scientists and researchers around the world [10, 17].

Therefore, the main goal of this paper is to integrate forensics techniques with the monitoring process to ensure the integrity of the Smart Energy Transaction Platform and discuss where blockchain is a complementary technology for these forensic options.

The rest of the paper is organized as follows.

Section 2 describes the levels of integration of the blockchain into the system of smart energy networks. Section 3 depicts the challenges for forensic in Smart Grids in connection with a blockchain. Section 4 discusses the question how existing blockchain solutions can improve the forensic investigation in Smart Grids. The proposed approach is given in Section 5.

Conclusions are drawn in Section 6.

II. SMART GRID AND BLOCKCHAIN

Talking about Smart Grid, we always assume infrastructure (Fig. 1). A Smart Grid consolidates traditional power plants with virtual power plants (VPP).

A VPP is a structure that combines three elements:

- distributed generators (wind turbines, photovoltaic stations, mini- and micro-CHP, etc.);
- consumers — load regulators (household and industrial);
- energy storage systems.

Household consumers (washing machines, refrigerators, televisions, microwave ovens, air conditioning systems, heating elements, etc.) are the most easily controlled loads. The management of a load of industrial users largely depends on the flexibility of their technological processes.

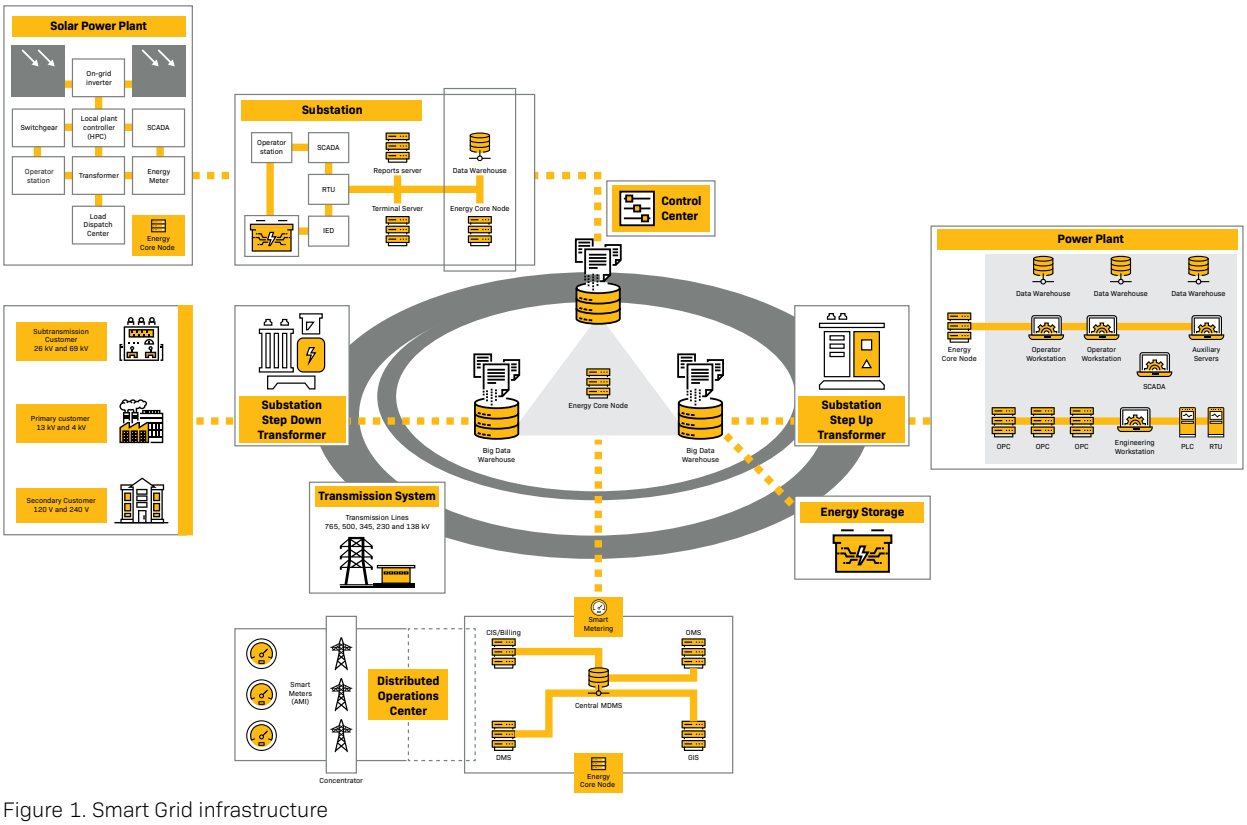

Figure 1. Smart Grid infrastructure

Table 1. Levels of integration blockchain with Smart Grid

Level	Name	Description	Requirements
0	Standards	Development and implementation of standards	Theory development, testing in research laboratories
1	Data collection	Basic functionality. Collecting information from smart devices and writing them to the blockchain (e.g. smart meters)	Fulfillment the level zero. Developed communication infrastructure
2	Micro-payments	Selling consumers' excess energy	Fulfillment the level zero and level one. Governmental support
3	Management tool	Directed electricity sales. It will be possible to build and operate fully functional decentralized energy exchanges	Fulfillment the level zero, one, and two

For some operations, flexibility increases due to energy storage systems. Typically, virtual power plants are connected to a medium or low voltage network. Elements of a virtual power plant can be located at considerable distances from each other. Networks (electrical and communication) are combined under the term Microgrid.

A feature of a Microgrid is its ability to work offline. Virtual power management is carried out remotely through the EMS system (Energy Management System), which receives information about the current state of each power plant and sends control signals to them. The EMS uses a global satellite navigation system (GPS) that synchronizes measurements of the complex values of current and/or voltage across all power plants of the virtual power plant.

Devices for such measurements are called PMU (Phasor Measurement Units). A virtual power plant may have a commercial purpose, technical (system services such as frequency and active power regulation, power quality maintenance, etc.) or combine both functions.

The functional capacities of virtual power plants can be attributed to:

- control of dispersed generation (optimization of network modes);
- management of electricity consumption (comparing the load schedules of consumers and power sources);
- market management of the reserve capacity (the possibility of using reserve power).

The effect of introducing Smart Grids will manifest many benefits for the consumer by increasing the electricity supply, reliability, and energy efficiency, and through participation in the consumption management program, there is a chance to influence the consumption of electricity. There is also the possibility of receiving revenue from the sale of surplus capacity to the network. For the grid, this will reduce the peak load of the network, optimize load control and network regimes, integrate virtual power plants into the system while maintaining its stability, as well as increase the network assets load, reduce unclaimed power and reduce investment in the network.

The levels of integration of the blockchain into the system of smart energy networks can be divided into the four levels presented in Table 1.

III. CHALLENGES FOR FORENSIC IN SMART GRID

As it mentioned in [18–20], Smart Grids are susceptible to cyber attacks. Each level has its own vulnerabilities; therefore, it is impossible to avoid cyber-incidents. The hackers who struck the power centers in Ukraine "were skilled and stealthy strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, then launching a synchronized assault in a well-choreographed dance" [21].

When considering the Smart Grids, we should consider that attacks can arise from various parts of a power system including supervisory control and data acquisition (SCADA), electric transportation infrastructure, smart meters, advanced metering infrastructure (AMI), an energy storage subsystem and/or any vital components of the Smart Grid.

To cope with these challenges in distributed networks, we need to log information that will enable users to effectively investigate cyber crimes and predict system failures. Recently Cohen C. [22] discussed a potential way that cyber-investigators can de-anonymize up to 60% of bitcoin clients on the network and open new avenues for forensics in blockchain. Erol-Kantarci M. and Mouftah H. T. [17] defined Smart

Grid forensic science as a powerful security component of the power system and have also described the applications, obstacles, and open issues in this area. Following their study, we summarized challenges for forensics in Smart Grids in connection with blockchain. Column 'Challenges' depicts all issues that can be solved by the blockchain-based systems.

Another challenge for forensics in Smart Grids is data volume. The different power devices generate vast data and then stream them through the communication infrastructure. Data streams are assumed to be an infinite sequence of time-stamped records. Each record consists of key-value pairs, where the keys are the attributes of the reading, and the values are the corresponding data of the reading [23]. Storage and processing of the enormous amount of data introduce significant challenges together with the privacy issue.

IV. WILL BLOCKCHAIN BE ABLE TO SOLVE THE PROBLEMS WITH SMART GRID FORENSIC?

Blockchain is an ideal technology to help make forensics principles more widely used, as well as to enhance datasets. Blockchain logs the truth information; thus, these datasets are entirely trustable [24]. It enables utilities to monitor every instance of every data structure created by an application and monitors all accesses, when the situation is freed, and when the memory in which it was stored was overwritten. From the above reasoning, we assume that the combination of blockchain, Smart Grids, and Forensics can address the following global energy challenges:

- Ensure the reliability of electricity supply to consumers and forecasting major system failures of power systems to prevent catastrophic consequences;
- Manage electric networks at all levels of energy resource distribution and automation of electricity consumption through the Internet;
- Decentralize the energy market and implement optimal energy distribution systems by alternative energy expansion.

More specifically, blockchain can strengthen forensic investigations in Smart Grids and can enable the following tasks in particular applications (smart metering, SCADA networks, Wide area measurement and control, Disaster forensics):

Metering

- Privacy of personal information;
- Secure data collection and storage;
- Data storage and processing cost;
- Compression techniques that do not lose alarm content.

SCADA network

- Scalable data collection.

Wide area measurement and control

- Data processing and storage;
- Secure data collection and storage;
- GPS spoofing attacks.

Disaster forensics

- Data collection during severe disasters;
- Smart Grid control under communication system failure or damage;
- Event logging hardware for highly critical assets (similar to flight data recorders).

Audio/video authentication by ENF

- Obtaining pattern database for old recordings.

V. PROPOSED SOLUTION

A. Basic components

The proposed solution (Fig. 2) is a decentralized transaction platform based on blockchain and tailored to Smart Energy sector, containing all the latest technology such as advanced metering infrastructure, distributed generation, demand-side management, etc. Besides financial transactions in the energy market, it covers other use cases more than just the crypto-payments and can be extended to perform any number of Smart Grid forensic tasks mentioned in Table 2.

The operation of the platform is provided by computational nodes. Practically, each node is a computer server running under Windows Server 2016 OS or Red Hat Enterprise Linux OS where 'Energy Core' is deployed. Nodes form a network. The entire network is divided into subnets or sidechains.

The system consists of several types of nodes:

- Full nodes

Full nodes (ECore) are deployed on the core objects of energy infrastructure, such as power plants; it is worth pointing out that we need big data warehouses to storage all energy data. Remaining facilities are placed on the light nodes.

- Light nodes

Light nodes generate transactions containing specific information, i.e. on the authorization of the operator, emergency shutdown, and network frequency. Other words, any event forms

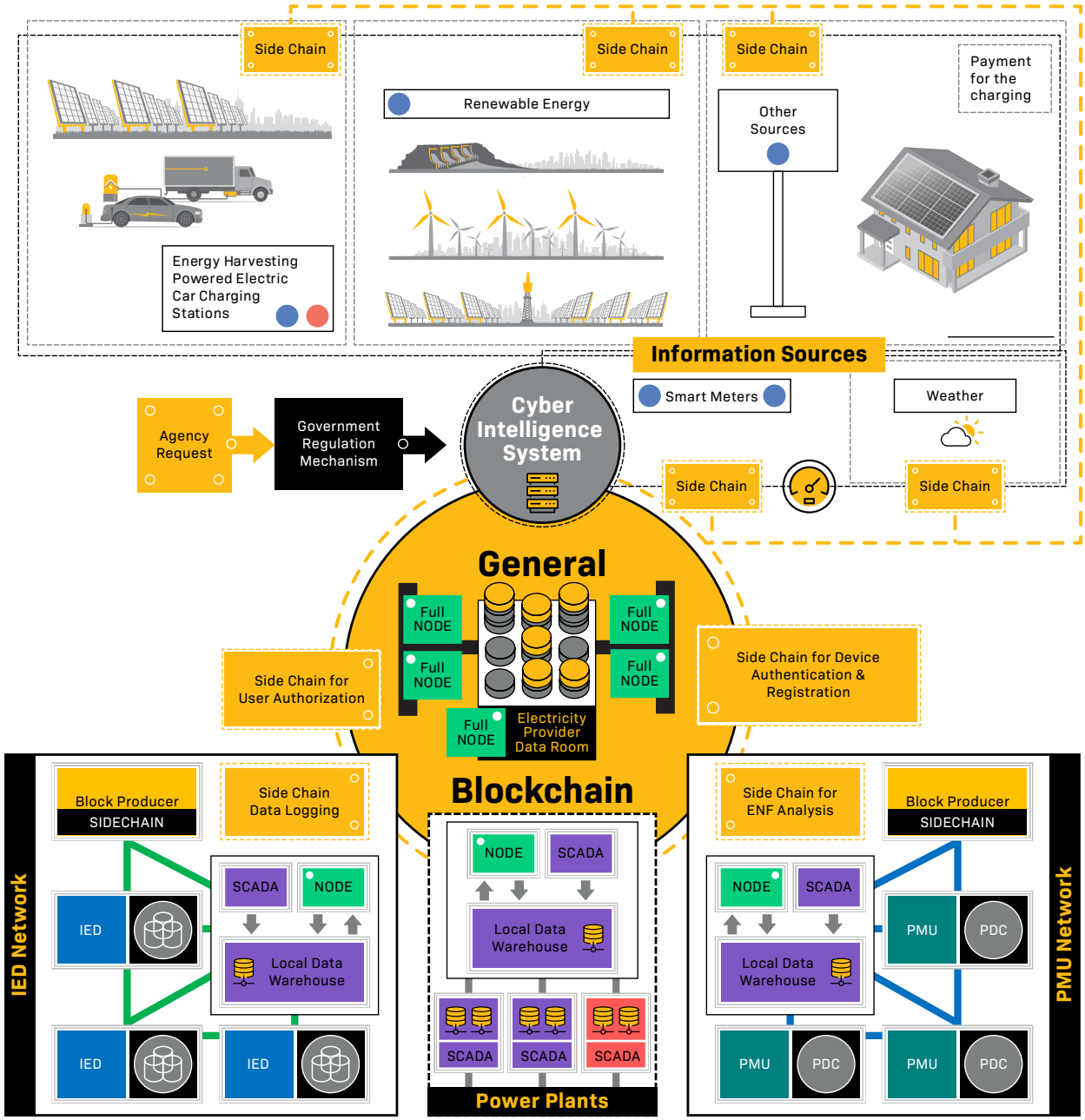

Figure 2. A Decentralized Smart Energy Transaction Platform on Blockchain

a transaction that is transmitted to the full node of its network segment, which forms transactions in the block and sends it to the main blockchain.

Light Node stores data only of its site, sometimes it stores partially, because the annual volume is about 60 TB. The examples of light nodes are Phasor Measurement Units (PMU), Intelligent Electronic Devices (IED), local substations, unit operator stations, etc.

- Side chains

We use side chains to break the entire network into sections, thereby reducing the amount of information for storage. Each network of the same devices with the SCADA system has its own sidechain (data/logs) and store data about user login registration, device registration in the network, device events, and device data.

- Energy Core

Energy core is a set of software for controlling transactions and storing information. It performs the functions of receiving and validating transactions and then forms an encrypted block signed by a private key, which is sent to all the same nodes for confirmation and storage in their data warehouse. It also detects and connects to similar network nodes, thereby forming a decentralized information energy platform, which is also a decentralized virtual machine, which enables you to manage network nodes based on smart contracts, and in turn, creates an environment for distributed hardware and

Table 2. A summary of applications, challenges and open issues in Smart Grid forensic

Level of network	Assets	Applications	Challenges
Power plant	Advanced Interrupting Switch Controllable/ Regulating Inverter Distribution Automation SCADA Loading Monitor Phase Angle Regulating Transformer	Metering (event logging, data logging, user's authorization, devices authentication) Disaster forensics (equipment failure, equipment health sensor) Tracking cryptocurrency payments (energy charges) Decentralized application (equipment management) ECore software (full nodes)	Privacy of personal information Secure data collection and storage Data storage and processing cost (partially) Scalability Lack of live analysis tools
Transmission System	FACTS Device Fault Current Limiter Microgrid Controller Phasor Measurement Technology SCADA	Metering (event logging, data logging, user's authorization, devices authentication) Equipment health sensor Decentralized application (equipment management) Light Nodes Obtaining pattern database for old ENF recordings GPS spoofing attacks Signal processing for audio and video recordings (partially)	Scalable data collection Sophisticated data processing Event logging hardware for highly critical assets (similar to flight data recorders) Data collection during severe disasters Smart Grid control under communication system failure or damage Event logging hardware for highly critical assets (similar to flight data recorders)
Home	Advanced Metering Infrastructure (AMI)/Smart Meters Smart Appliances and Equipment Customer EMS/Display/Portal	Metering (event logging, data logging, user's authorization, devices authentication, equipment health sensor) Decentralized application (equipment management; invoice payment) Light node	
Network	RTU Distribution Management System	IEC 61158	User's access by private key Access only for authenticated devices The data stored on all devices

applications. At the moment, there is a big challenge for computer forensics, when it is necessary to obtain the data from the operating equipment since their disconnection from the network affects the power and safety; thus, the further investigation becomes impossible.

The blockchain will provide real-time management and research capabilities that will speed up the process of investigating cyber-crimes and failures during natural disasters, acts of cyber-terrorism, and computer fraud.

Each element of this infrastructure, including the blockchain nodes as well as the Smart Grid components, are a potential source of information. Below, there are some examples of items mentioned in general scheme (see Fig. 1) and their possible use for cyber- or disaster forensics.

- Intelligent Electronic Devices (IED)

IEDs are microprocessor-based tools used for the protection, automation, and control and

monitoring the power system hardware. They sense voltage, current, or frequency anomalies, or raise/lower voltage levels in order to maintain the desired level [25].

- Charging stations

Information from charging station allows parties to find out the duration of the charge (the time the object stays at a certain point), information about the connected car, payment history, etc. It also keeps usage logs and provides possible notifications about hacking, abnormal activity of the charging station, etc.

- Smart counters

Smart meters and IEDs provide granular energy/demand data. This information allows utilities to interpolate behaviors, work schedules, occupancy rate (how many people live in a home), types of equipment at a home, heating/cooling systems, etc. Investigation of incidents with theft of electricity, as it mentioned in [17] may indicate certain crimes, such as the cultivation of marijuana.

- Phasor measurement units (PMU)

PMU can measure phase, amplitude, frequency, and Rate of Change of Frequency of voltage and current waveforms. Besides their wide use in power systems for protection purposes, they also can be used for several tasks related to the injection of photovoltaic power into the grid [26].

- Phasor Data Conscentrators

PDCs receive and synchronize phase data from multiple PMUs to produce real-time data streams. A PDC can exchange phasor data with PDCs at other locations. Both PDC and PMU data can be used by forensic specialists for Electric Network Frequency analysis. They compare frequency changes in background mains hum in the recording with long-term high-precision historical data. It can identify when the record was created and help detect any edits in the recording.

B. System deployment

In parallel with the SCADA system, the light node (network node) is installed at the object, and the local data storage is deployed. Physically, the Light Node is a separate computing device.

Devices on a network site transmit information (make a transaction) to the SCADA system, in turn; SCADA stores the data in its local storage.

The node, working in parallel with the SCADA system, is already working directly with the data warehouse, to increase the security of the system as a whole.

To ensure the authenticity (the device is valid/data is not substituted) transactions, they are produced according to the ZKP protocol. Transactions are collected in a block and sent to the general blockchain.

To register new devices on the network, one shared Sidechain is required (if you do it on each network segment, it will be inconvenient to process data in the future). Authentication of new devices on the network can be done using the Bloom filter [27].

Registration of operator access also has its own separate side chain. All sites are included in one blockchain (denoted as General in Fig. 2).

Nodes are located in settlements. The network is formed of at least three nodes, each in a separate city. The more nodes, the higher the decentralization, and as a result, the greater the reliability.

The blocks formed by the Sidechains are included in the general blockchain, which stores the complete chain of blocks of all sections. Blocks can be created not only by network sections but also by operators.

For example, information from smart meters, charging stations of electric cars, weather information from the regions. Requests for information may be in service of the investigation of cyber incidents, the tracking of criminals, or the investigation of system failures during disasters. To perform a more accurate forensic investigation, more decentralized and/or fully distributed Smart Grid networks are required. In this case, the blockchain ensures the security, validity of the data and access to the old records.

VI. CONCLUSION AND FUTURE WORK

The use of the blockchain will allow us to create a single shared information space for investigating incidents in the Smart Grid. To perform this there are some necessary conditions: data should

be valid (impossible to replace), all network devices should be authenticated (this device will generate this data), all attacks must be very expensive for an attacker, and the information environment should be as transparent as possible.

Finally, since blockchain already has some proven applications in the financial industry, we hope that there is a high potential for it to be similarly adopted in Smart Grids. This technology is still in its early stage and suffers from immaturity, problems with scalability, and transaction processing delays and trust issues. However, it can still benefit both Smart Grids and cyber forensic agencies. Currently, we are

developing a decentralized platform on Ethereum that utilizes blockchain technology as well as non-traditional cyber-forensics methods to provide access to Smart Grid resources. We are studying other blockchain solutions and frameworks (e.g. Exonum, Stellar, etc.) that may also be good for our platform.

References

[1] C. Eid, P. Codani, Y. Perez, J. Reneses, and R. Hakvoort.—Managing electric flexibility from Distributed Energy Resources: A review of incentives for market design || *Renewable and Sustainable Energy Reviews*, 2016, vol. 64, pp. 237–247.

[2] Y. Kabalci.—A Survey on Smart Metering and Smart Communication || *Renewable and Sustainable Energy Reviews*, 2016, vol. 57, pp. 302–318.

[3] K. Kok.—The PowerMatcher: Smart Coordination for the Smart Electricity Grid || SIKS Dissertation Series, No. 2013–17, Dutch Research School for Information and Knowledge Systems, TNO, The Netherlands, 2013. Available: http://dare.ubvu.vu.nl/handle/1871/43567.

[4] C. Stöcker.—Software Defined Digital Grid on a P2P Network — On Systems of Autonomous Energy Cells || 2018. Available: https://medium.com/cstoecker/softwaredefined-digital-grid-on-a-p2p-network-cdd17c9017e4.

[5] M. Merz.—Potential of the Blockchain Technology in Energy Trading || In Blockchain technology Introduction for business and IT managers. Berlin, Boston: De Gruyter Oldenbourg, 2016. Available: https://www.ponton.de/downloads/mm/Potential-of-the-Blockchain-Technology-in-Energy-Trading_Merz_2016.en.pdf.

[6] C. Zhang, J. Wu, C. Long, and M. Cheng.—Review of Existing Peer-to-Peer Energy Trading Projects || *Energy Procedia*, vol. 105, No. Supplement C, 2017, pp. 2563–2568.

[7] M. Mihaylov, I. Razo-Zapata, R. Radulescu, and A. Nowe.—Boosting the Renewable Energy Economy with NRGcoin || Atlantis Press, 2016. Available: http://www.atlantispress.com/php/paper-details.php?id=25860387.

[8] E. Ela, M. Milligan, A. Bloom, A. Botterud, A. Townsend, T. Levin, B. A. Frew.—Wholesale Electricity Market Design with Increasing Levels of Renewable Generation: Incentivizing Flexibility in System Operations || *The Electricity Journal*, 2016, vol. 29, pp. 51–60.

[9] Z. Mrabet, N. Kaabouch, H. Ghazi and H. Ghazi.—Cyber-security in Smart Grid: Survey and challenges || *Computers & Electrical Engineering*, 2018, vol. 67, pp. 469–482.

[10] N. Z. Aitzhan and D. Svetinovic.—Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams || *IEEE Transactions on Dependable and Secure Computing*, 2016, vol. PP, No. 99, pp. 1–1.

[11] H. T. Nguyen, S. Battula, R. R. Takkala, Z. Wang, and L. S. Tesfatsion.—Transactive Energy Design for Integrated Transmission and Distribution Systems || Iowa State University, Department of Economics, Tech. Rep. 201802280800001000, Feb. 2018. Available: https://ideas.repec.org/p/isu/genstf/201802280800001000.html.

[12] N. Schwieters, J. van Hoof, D. Etheridge, and A. von Perfall.—Blockchain — an opportunity for energy producers and consumers || PwC, Tech. Rep. Available: https://www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf.

[13] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt.—A blockchain-based Smart Grid: towards sustainable local energy markets || Computer Science — Research and Development, 2017, pp. 1–8, Available: https://link.springer.com/article/10.1007/s00450-017-0360-9.

[14] Blockchain Consortium Aims to Create an 'Energy eBay' || Greentech Media. Available: https://www.greentechmedia.com/articles/read/blockchain-consortium-aims-tocreate-an-energy-ebay.

[15] WePower — blockchain-based green energy trading platform. Available: https://wepower.network/.

[16] F. Hawlitschek, B. Notheisen, and T. Teubner,—The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy || Electronic Commerce Research and Applications. Available: https://www.sciencedirect.com/science/article/pii/S1567422318300292.

[17] M. Erol-Kantarci and H. Mouftah.—Smart Grid forensic science: applications, challenges, and open issues || *IEEE Communications Magazine*, 2013, vol. 51(1), pp. 68–74.

[18] R. K. Knake.—A cyberattack on the U.S. power grid, 2017.

[19] ENSIA, Distributed Ledger technology & Cybersecurity, ENSIA, Tech. Rep., 2016. Available: https://www.enisa.europa.eu/publications/blockchain-security/at_download/fullReport.

[20] F. Restuccia, S. D'Oro and T. Melodia.—Securing the Internet of Things: New Perspectives and Research Challenges || arXiv: 1803.05022 [cs], 2018, arXiv: 1803.05022.

[21] K. Zetter.—Inside the cunning, unprecedented hack of Ukraine's power grid, 2016. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[22] C. Cohen.—Forensics and Bitcoin || Forensic Focus. Available: https://articles.forensicfocus.com/2015/01/16/.forensics-bitcoin/.

[23] A. Beres, B. Genge, I. Kiss.—A brief survey on Smart Grid data analysis in the cloud || Proceedia Technology, 2015, vol. 19, pp. 858–865.

[24] Bitfury Group. On Blockchain Auditability, 2016. Available: https://bitfury.com/content/downloads/bitfury_white_paper_on_blockchain_auditability.pdf (accessed on 15 November 2018).

[25] Intelligent electronic device. Available: https://en.wikipedia.org/wiki/Intelligent_electronic_device.

[26] S. Vergura, M. Carpentieri.—Phase Coherence Index, HHT and Wavelet Analysis to Extract Features from Active and Passive Distribution Networks || Applied Sciences, 2018, vol. 8(1), p. 71.

[27] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du and Y. Ma.—Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities || *IEEE Communications Magazine*, 2018, vol. 56(7), pp. 82–88.