Integration of Distributed Ledger Technology and Modern Smart Grids: An Outlook

Mikhail Komarov†, Markova Margarita†, Aleksandr Ometov‡
† Graduate School of Business, National Research University Higher School of Economics, Moscow, Russia
‡ Faculty of Information Technology and Communication Sciences, Tampere University, Tampere, Finland
Authors' emails: mkomarov@hse.ru (✉), mkmarkova@edu.hse.ru, aleksandr.ometov@tuni.fi

***Abstract*—Today, the evolution of electrical grid systems is pacing towards interconnected Smart Grids mainly driven by governmental activities worldwide. This step brings additional challenges from the data storage perspective since conventional centralized systems may not handle the growing data volumes arriving from various sources. Thus, new distributed solutions must be introduced to allow flexible and on-the-fly enablers to such tremendous data flows. One of the potential candidates is integrating Blockchain-powered Distributed Ledger Technology (DLT) to achieve an immutable record of manipulating electricity from production to end-user delivery. In this paper, we study the relation of said diverse technological components inter-operation, related challenges, and solutions proposed by research and federal regulators. Based on the literature review, we draft the recommendation for the wide-scale architecture of the future combined solution.**

***Index Terms*—Smart Grids; Distributed ledger technology; Distributed information systems; Electricity supply industry**

I. Introduction

Over the past few years, Distributed Ledger Technology (DLT) has been applied in an increasing number of industries, which is due to greater maturity of the technology, universal digitalization, the emergence of new models of implementation [1]. It resulted in the emergence of a new concept known as Blockchain-as-a-Service (BaaS), allowing for more flexible handling of growth in the number of transactions of various types [2].

One of the well-progressing DLT applications is related to the monitoring of various resources' distribution and consumption [3]. The concept of applying Blockchain technology in Smart Grids is attractive for several reasons. The Blockchain already entered the stage of "Blockchain complete" in 2020, and, in the next three years, it is expected that it will be adopted in most industries according to Gartner's forecasts [4]. Therefore, now is the most appropriate time for the development and early-stage integration implementation of Blockchain solutions.

Historically, one of the main reasons for the inaccurate calculation of electricity consumption was insufficient automation of accounting: errors appeared due to contradictory data of the controller [5]. Today, the government proposes introducing new technologies to eliminate the human factor in the data collection process. Replacing an employee with an electronic device in this process will not exclude all errors, which means that the problem is not completely solved.

After 2020, smart meters are expected to be installed broadly, and the transition to such gadgets will be mandatory in some countries. The frequent problem of implementing smart Internet of Things (IoT) devices is related to safety problems and technical errors [6], [7]. The objective of this study will be to highlight the issues associated with the introduction of smart meters.

In this work, the focus will be on the activities of enterprises providing public utilities, namely those engaged in the electricity market. The object of this study is the industry of the Russian electric power industry. The subject of the study is the interoperation of modern concepts and technologies such as Smart Grid, DLT, IoT, Internet-of-Energy (IoE), Internet-of-Measurement (IoM), and Blockchain. The main focus would be given to the Electricity Market of the Russian Federation as an example of an extremely broad and complicated ecosystem.

The rest of the paper is organized as follows. First, Section II provides a state-of-the-art on Smart Grid development process from governmental and research perspectives. Next, Section III outlines the applicability of Blockchain/DLT to Smart Grid-related data storage and processing tasks. Further, Section IV describes the model for the use of BaaS for Smart Grid. Future perspective is given in Section V. The last section provides a summary of this work.

II. Background on Smart Grid

The energy market of the Russian Federation is represented by companies with different roles: power producers, power suppliers, distribution companies, and grid companies. Generating companies produce electricity using one of the following methods: fuel combustion, hydrogeneration, conversion of nuclear energy, generation utilizing wind, and solar plants.

Most generating companies use fuel-based generators: gas (about 50%) or coal (about 15%)[1]. Among them are both energy import operators and energy export operators, such as Inter-RAO. Generating companies can sell energy independently, but power is often supplied to the wholesale market of electricity and capacity. Wholesale Electricity and Capacity Market – the sphere of electric energy and capacity

[1]The main market players are RusHydro, Inter-RAO, Eurosibenergo, OGK-2, Irkutskenergo.

circulation in Russia under the Unified Energy System of Russia. Buyers in this market are sales companies and sometimes large industrial enterprises. Suppliers are electricity importers, generating companies as well as grid companies. The interaction of electric power market objects is given in Fig. 1.

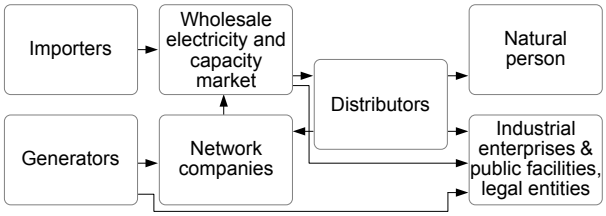

Fig. 1. Electricity market segments interaction scheme

National and regional network companies are mainly state companies, e.g., Federal Grid Company (FGC) and Rossetti Holding. The role of FGC is to transmit energy through the Unified National Electric Grid, while Rosset is the operator of power transmission lines, substations, and transformers. The two companies are interconnected: Rosset owns 80.13% of FGC shares, while PJSC Rosset is owned by the state (88.04% of shares). [8]

The components of electricity cost differ in the wholesale and retail electricity markets. The cost of electricity as a commodity is composed of electricity, logistics, and power balance – the balance of production and consumption of electricity, which is important for the reliability of energy supply. Additional components of the cost on the wholesale electricity market are the cost of balancing the electricity production plan (reduction and increase in the generation of power plants, the planned volume of fuel – market participants submit consumption forecasts to the exchange and based on this load of power plants and electricity exchange prices are calculated, as well as the costs of concluding bilateral agreements.

In the case of retail sales of electric power, apart from the cost price, transportation, and capacity regulation, there are surcharges to pay for the work of the sales company and payment for losses in the networks. The object with a special status in the wholesale and retail market is a guaranteed supplier. A participant with this status following the legislation of the Russian Federation [9] is obliged to conclude an energy supply contract with any individual or legal entity whose energy receiving devices are in its area of activity. The guaranteeing supplier shall sell on the retail market electric energy or power purchased by it on the wholesale market, i.e., an energy sales organization. The status extends to a certain territory according to the register. The largest organizations: JSC “Mosenergosbyt”, JSC “Petroelectrosbyt”, JSC “Gazprom energosbyt Tyumen” [8]. Guaranteeing supplier is obliged to organize the collection and reception of metering devices and provide billing to the consumer, including using the conventional Internet network [10].

However, guaranteeing suppliers will be responsible for ensuring commercial accounting only in the apartment and residential buildings, and accounting for consumers purchasing energy in retail markets will be provided by network organizations [9]. Thus, the losses related to errors from smart meters will be attributed not only to the guaranteeing suppliers but also to the grid companies, which will lead to an increase in tariffs on the retail market as well: sales margins will increase, and on the wholesale market – the tariffs for electricity transmission will raise.

A. Intellectual systems of power metering

The experience of the different countries confirms advantages of the technological advancement: decrease in the cost of the electric power, a potential reduction of gas emissions is noted by researchers in U.S. [11], decrease in nontechnical losses was revealed in Lebanon [12], prevention of theft in South Africa [13]. All over the world, there is a tendency to introduce IoT devices. That is already a common phenomenon: Austin Energy, one of the famous energy suppliers in the U.S., installed more than 260,000 smart meters to consumers in 2008. Smart meters are a long-established technology in Europe: In Italy, [14], Sweden [15], and others.

Today, the Russian system that provides electricity accounting is an automated system of commercial electricity accounting. It consists of components that can be divided into three levels. The first level includes metering devices, a link, at present, the most frequent is the RS-485 interface and processing center.

Nonetheless, Smart Grid corresponding to the concept of the IoE is introduced [16]. Sensors are being placed at the stage of energy generation, which allows collecting the programmed amount of data and use them for forecasting, adaptation to weather conditions. In addition, the implemented Smart Grid technologies imply the collection of information that allows predicting electricity consumption and electricity prices.

Further, the development of the IoT and IoE concepts has led to adopting a law regulating changes in electricity accounting. “The Internet of Electricity is a network of generation, transmission, distribution of energy, enhanced by digital control, monitoring and telecommunication capabilities” [16]. The system built in the concept of IoT should be transactional, intellectual, sustainable, and flexible.

The benefits are achieved using the IoT devices: all kinds of sensors and actuators connected to intelligent networks. For the system of smart metering, the following definition has appeared in Russian legislation (translated): “intelligent system of electric energy (power) metering – a set of functionally combined components and devices designed for the remote collection, processing, transmission of electric energy metering devices’ readings, providing for information exchange, storage of electric energy metering devices’ readings, which does not affect the measurement results performed by electric energy metering devices, as well as the provision of information on measurement results, quantity and other parameters of electric energy following the rules for providing access to the

minimum set of functions of intelligent systems of electric energy (power) metering, approved by the Government of the Russian Federation" [9].

Thus, the smart metering system includes the smart meters directly and the components responsible for remote access, storage, and information exchange. This definition relates to the Internet of Energy (IoE) concept, which involves two-way automated information flow and the accumulation of data from sensors.

However, another aspect of the concept is to realize the potential of data, such as using information for predictive analysis.

A certain minimum set of functions of the intelligent accounting system is [17]: transfer of measurement results; providing information on electricity parameters; possibility to suspend or limit the power supply; determination of the date, time of day, days of the week to apply differentiated tariffs; transfer of data on recorded events by the meter; transfer of additional data; notification of possible incorrect measurements in cases of technical failures, magnetic fields, tampering indicators triggered.

These components do not affect the measurement results in any way. In other words, the measurement results are not supposed to be continuously checked for obvious emissions, anomalies, and technical errors. Measuring instruments must provide at the point of measurement [17]:

- measuring electricity with an accuracy 1.0+ class;
- measurement capability using transformation coefficients;
- time tracking with an error of no more than 5 seconds per day, ability to synchronize with the exact time;
- electricity measurement and calculation (class S measurement error);
- consumption displays;
- power outage and restart upon request of a smart system;
- indication of the opening of seals, the influence of magnetic fields, various kinds of technical failures, infringement of parameters of quality of power supply;
- communication channel organization via RS-485 interface, optical and digital Ethernet;
- protecting information through access control, integrity, event logging;
- logging of events: recording of unsuccessful identification, unauthorized violation of information integrity, and other deviations from the norm;
- self-diagnostic capability;
- possibility to organize secure information exchange, use of protocols approved by local standards.

In the case of using IoT devices, the legislation specifies the requirements for protecting information in the intelligent system of electricity accounting. Information protection is assumed in all system components at the stages of collection, transmission, and storage. The information in the system gets under [18] and [19], e.g., for system protection, the following tools should be used: authentication and identification in each of the components of the intelligent accounting system; information reserving; physical protection of information from exposure; cryptographic protection; data access rights management.

First, the smart meter has the possibility of communication. There are three major ways to transfer information for smart meters: using GPRS, NB-IoT, LPWAN, or Wi-Fi (IEEE 802.11 family) technologies [20], [21]. Depending on communication technology, different controllers are used. The controller connects to the meter using wires and then uses wireless communication technology to transfer data. GPRS controllers have built-in SIM cards. They are energy efficient and work well where cellular communication is well caught. LPWAN controllers use technologies specifically designed for the Internet of things, less energy-consuming, but special towers to receive this signal are less. To use the Wi-Fi controller requires Wi-Fi communication in the house but combines the advantages of previous controllers. The communication scheme is as shown in Fig. 2.

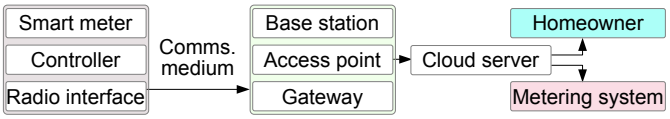

Fig. 2. Communication scheme for smart controllers

Notably, manufacturers of smart meters do not use a unified standard protocol for data transfer yet. The most broadly adopted one is ANSI C12.18 with low cost of equipment and availability of authentication, but with low speed of data transmission; IEC 61107 also with low data rate and the problem of non-regulated compliance with types of data measurements; M-BUS with similar issues [22]; OSGP – a promising protocol, but also growing trend of using TCP/IP technologies. There is also a standardized (IEEE 802.15.4.) Zigbee protocol is broadly utilized for the application [23] and a closed XNB, which may become a standard for smart electricity meters [24].

Another component of the smart metering system that needs to be considered is data management systems. Simultaneously, telemetry data in the automated system of commercial energy accounting are controlled by systems such as SCADA. SCADA systems provide data exchange with controllers, information processing and can be integrated with external applications. The Smart Grid concept uses not only SCADA but also MDM systems that perform various functions:

- control and design of installation of smart meters;
- monitoring of meter procurement and implementation;
- counter setting – remote and automatic;
- data analysis.

Smart meter data analytics should include outlier diagnostics in the data, detection of poor-quality data, calculation of power losses due to nontechnical reasons (only smart meters provide such data), load profiling. Predictive techniques and analysis of electricity consumers are also expected to be used. The results of the consumption analysis can be used to manage the provision of services to consumers

and benefit-generating companies. The main techniques of smart meter data analysis are machine learning, time series analysis, the use of dimensional reduction methods (PCA, multidimensional scaling), deep understanding, and others.

B. Major Smart Grid Integration Challenges

Implementation of the Smart Grid concept is a promising but controversial way to modernize the power industry. A Smart Grid contains data that is confidential and affects the well-being and comfort of users. In addition, it will have an impact on the economy – forecasts based on telemetry data affect the market supply of electricity. The holistic view of the Smart Grid is provided in Fig. 3 for a better understanding of the following discussion [25].

From the perspective of the electricity consumer, it is very important to trust the data provided by billing systems. Due to the Smart Grid of consumers, the following aspects are of concern. The complexity of the system. A smart network combines many devices connected to the Internet, increasing the number of points of vulnerability of the system, thus increasing the number of potential attacks. Distortion of data by the consumer himself. Users tend to intentionally corrupt devices to change readings, which may affect the Smart Network components associated with a compromised device [26]. Attacks on data management systems, e.g., MDM system may suffer from various types of attack threats such as viruses, various malicious programs [27]. Nonetheless, some patterns of electricity consumption can tell which electrical appliances the consumer uses. Thus, targeted attacks on data privacy should also be considered [28].

Moreover, system availability is important, being critical for implementing built-in algorithms of protection against attacks. DoS attacks are aimed at interfering with the communication processes of system components, blocking the system, or overloading it, which can also cause a failure or complete inaccessibility of the system. In this attack, the attacker does not need to access the network levels protected utilizing authentication and identification, but only to the communication channel. Attackers jam the channel, which leads to serious consequences for power generators or other devices connected to the system. DoS attacks can be carried out at different levels – at the transport, network, application levels.

Continuous functioning of the system is necessary for a smart network, short interruptions may lead to significant changes in the structure of supply and demand. The problem arose in Denmark [29], and researchers report that interruptions in data transmission within the system, the temporary unavailability of the system, which displayed credit information on electricity consumption, led to panic among consumers. The problem affected more than a hundred thousand people, which significantly changed the demand. It also affected other components: the web portal could not cope with the number of customers who decided to pay for electricity urgently.

The attacks on data integrity were aimed at unauthorized data changes and changes in data exchange. One type of such attack, for example, is spoofing – the attacker connects to the network and, by manipulating MAC addresses or other identifiers, is embedded in the system and transmits distorted information or signals. In addition to causing damage to the system, the attacker can also target customer personal information, consumption information and change the tags of smart devices displayed in the event log.

The security of two-way communication of information between network components is another aspect, which leads to new points of vulnerability of the system. An attack by a person in the middle is also possible in smart networks and poses a threat. This attack is related to information integrity and confidentiality: data encryption keys, passwords, logins can be intercepted. All components require the use of identification and authentication tools. Smart meters are vulnerable to the unauthorized reading of information, gaining control over the meter, cloning the meter. Connecting to interfaces using malware can be used to change the information in a smart network.

These vulnerabilities have been confirmed in various contests, e.g., PHDAYs (international hackathon) participants implemented a successful DoS attack, changed readings on electric meters, controlled controllers, adjusted transformation ratio, etc. Vulnerabilities exist in every element of the system, but most of them are in the device of smart meters. Requirements for the use of security features are poorly executed. Although passwords are set on most devices, they can be easily intercepted, for example, by queries to the configuration script.

In addition, Smart Grid components are electrical devices that also suffer from magnetic field effects, voltage unbalance, which leads to technical failures and losses in the Smart Grid. The most vulnerable are transformers, intelligent system devices. Physical impact on these elements, disruptions due to weather conditions can also be considered a threat to the integrity of information.

Even in the absence of extreme exposure, smart meters can overestimate readings by 582% or understate by 32% [30]. These results were obtained from experiments by Dutch scientists. Within six months, experiments were carried out on the most popular meter models. They were connected to various electrical consuming devices, and readings were checked against a control device. The result observed significant deviations from the norm, although the meters were produced according to a certain accuracy class.

The quality of data provided by smart meters suffers, leading to the following problems [31]:

- duplicates data occur;
- produces data omissions, incorrect encoding;
- significant excesses of permissible measurement errors occur;
- data compromised by a cyberattack;
- data is reset to zero;
- produces emissions in the data;

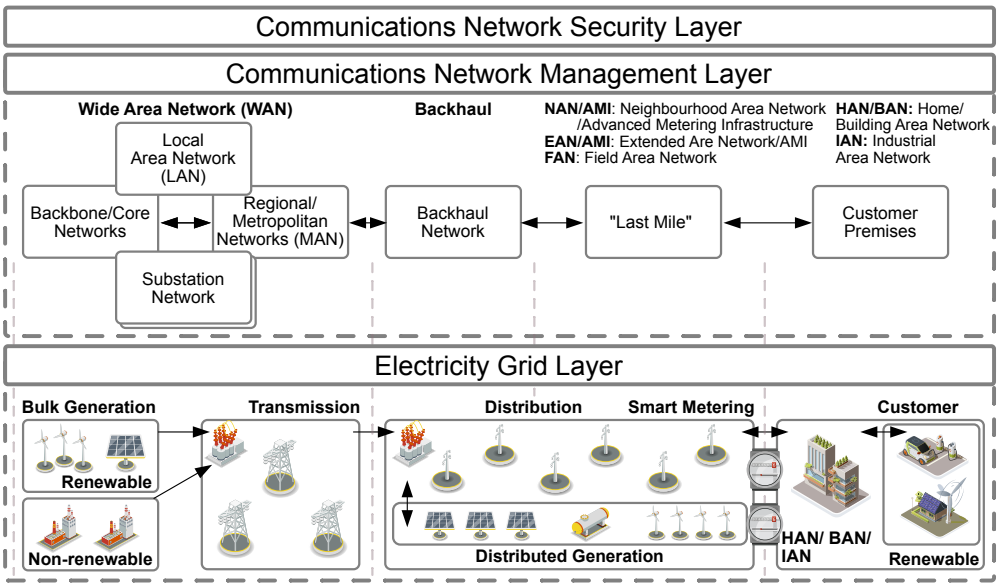

Fig. 3. Smart Grid communications model

- timestamps and other synchronized data are distorted;
- failed data anonymization.

Thus, the reliability of data can be affected by problems arising at the level of intelligent devices: cyber-attacks on sensors and other elements, physical attacks, failures in the application of different settings, the same hacker attacks, communication failures; at the level of data management – wrong prediction methods, inefficient processing, data preparation, database distortions will lead to bad decisions in the industry; at the level of integration with other systems – new nodes of vulnerabilities and attacks.

C. Existing Smart Grid solutions for the listed challenges

The Smart Grid is a mature concept in many developed countries, so various solutions aim to protect different aspects of information. These solutions can be classified by information security components: integrity, availability, confidentiality.

From the information security point of view, solutions aimed at counteracting DoS attacks are offered. Traffic analysis is used to detect such attacks. [32]. Researchers' work suggests analyzing flow entropy, signal strength, measuring sensor response time, paying attention to the number of undelivered (damaged) data packets, detecting DoS attack patterns.

If a DoS attack has been detected at one of the Smart Grid layers, then measures are taken to limit the negative impact on the system: malicious traffic is blocked the DoS attack patterns can see that; the allowed data flow is limited for all participants in the network; spam packets are detected and removed, thus reducing the load on the channel; attempts are made to isolate the part of the network into which the attacker has penetrated; traffic is redirected for filtering. These methods are used in DoS attacks at the network layer. Frequency Hopping Spread Spectrum algorithms are effective in physical layer attacks, especially in ZigBee technologies [33].

When ensuring the confidentiality of information, solutions focus on two issues: encrypting the data so that the attacker does not disclose personal data (in the case of static data storage) and keeping the data confidential when aggregated, i.e., when attacking the direct transfer of data. In the first case, public-key encryption, symmetric key encryption is used. The authentication and identification mechanisms provide part of the confidentiality. Here the methods used involve secret-info asymmetry, time asymmetry, and their combination [34].

Data aggregation also uses different encryption schemes, with the focus of research on encryption methods and the complete aggregation scheme – other encryption methods can be used together at various stages of data aggregation. Effective techniques are suggested in Li et al. [35] the main aspect of which was Paillier's additive homomorphism encryption scheme. Further, the proposed work was continued by the researchers Garcia and Jacobs [36], Zhang et al. [37], Chen et al. [38], who proposed the concepts of additive secret sharing, super-increasing sequence, and Chinese Remainder theorem and fault tolerance, respectively. All these methods are aimed at protecting against external attacks. The problem of internal attacks was discussed in and He et al. [39].

Another solution that will improve the Smart Grid even during the construction phase is the use of simulations. You can simulate all the usage examples and check step by step whether the network is designed correctly from the beginning. They simulate system load, check power layer, cyber layer – MDM systems, servers, a communication network. Also, cyber-attacks at all levels of the system are simulated. Useful simulators – DigSilent, EuroStag, ObjectStab, Cymdist. For simulations are offered frameworks – SCADASim, OMNET++, Inspire, Matlab/Simulink. [40]

After all, many protocols and standards in the field of cybersecurity were developed by the IEEE, IEC, and others [41], see Table I.

TABLE I
MAIN PROTOCOLS AND STANDARDS USED IN SMART GRIDS

Protocol/ Standard	Details
IEC 60870-5D	ata transfer protocols
IEC 61850	Standards and requirements for data transmission systems
IEC 62056	Standards for electricity metering data exchange
IEC 62351	Data security protocols
IEEE 1686	Data security standards for Intelligent Electronic Devices
IEEE 1815	Standards for Electric Powering Systems
KS X 4600-1	Power Line Communication standards
NISTIR 7628	Grid cyber security framework
NERC	Cybersecurity framework (Critical Infrastructure Protocol)
ZigBee	Data transferring throw ad-hoc digital radio networks protocols

In addition to methods specifically designed for Smart Grids, widely applicable cybersecurity models will also be effective [42]:

1) Establishing a virtual private network: This is used to secure data exchange between two network points. It uses encryption and encapsulation.
2) Locking a gateway: gateways collect critical data and provide an interface between substation automation systems and external connections. You should also use encryption or VPN here.
3) Use transparent firewalls: they will help detect the threat and detect the attack.
4) Configure ACL (router access control list) – prevents unauthorized access to the network, allows you to filter data.

Regarding the safety and reliability of the data, Blockchain technology also must be considered. This work hypothesizes that it can cover most aspects: resistance to DoS attacks, resistance to errors, the impossibility of fraud, and confidentiality.

III. BLOCKCHAIN TECHNOLOGY FOR SMART GRIDS

Historically, Blockchain was the first fully implemented and efficient example of DLT technology currently used for reliable and irreversible data storage [43]. The most well-known example is the Directional Acyclic Graph (DAG), which involves using distributed storage in a non-linear manner in contrast to linear Blockchain structure [44]. Each new block is added to the chain, and this is the only type of database change. This conversion gives the output a unique string of data that cannot be converted backward. Therefore, the openness of the entered data (it increases the level of trust to the placed information) could be achieved; cryptographic data protection; mathematical guarantees of low vulnerability to hacker attacks; the immutability of data; decentralization; resistance to censorship; the ability to conduct transactions without intermediaries.

The benefits of this technology are promising to reduce the vulnerability of the Smart Grid. Due to the properties of Blockchain, researchers distinguish the following advantages in the context of Smart Grid [45]–[47]: ensuring cyber protection of information; the system requires reduced transaction value (by excluding intermediaries from interactions); additional control; introduction of new generators; and use of smart contracts (automation of contract execution).

The first area of the Blockchain application is to ensure cybersecurity in the system – for example, a cyber-secure trading platform for power transactions. Blockchain allows the operation of a distributed P2P system [48].

The 4-level Smart Grid system described in [49] assumes three baseline levels. Core network, the upper level, brings together the controlling participants of the system: energy companies, system operators, guaranteeing suppliers, management companies that use SCADA systems. The WAN is the link between the Core Network and NAN. The NAN layer connects electricity producers and consumers directly for different interactions. HAN binds IoT devices.

Also, an advantage of Blockchain technology is that it has proven itself in protecting the Smart Grid from false data injection attacks – attacks common for electricity grids. [50]. The management company has the public and secret key as well as a smart account. Consumption data is encrypted first on the smart meter side. Then the data is decrypted in the Blockchain system for verification. If the data has been successfully decrypted with the public key, it is uncompromised. Then the information is encrypted on the public key of the management company: this ensures that only the management company has access to the data. This ensures that the data remains confidential.

IV. THE USE OF BLOCKCHAIN-AS-A-SERVICE MODEL

Blockchain is a very complex technology with high development costs, and in addition to the increased computing power, the concept of Blockchain-as-a-Service is the most suitable implementation option for many companies. Blockchain as a service means that the company deploys a Blockchain solution for its purposes with the vendor's help: that is, the vendor provides technical, software, technical support, etc. Of course, the decision to request a BaaS provider must be carefully weighed: the expected costs are compared to the expected profit.

In terms of costs, on the one hand, everything is similar to any other software: the client pays the provider for the deployment, maintenance, technical support. On the other hand, the fee is directly proportional to the leased computing resources (e.g., Blockchain peer node from Amazon Cloud). If you still want to build your solution, you can use Blockchain platforms such as Ethereum, Hyperledger, etc. This will not reduce the cost of development too much but will allow you to customize the solution more sensitively for your company. It is also worth assessing the risks associated with staff training, technological risks.

For an approximate understanding of the cost of deploying a blockchain, let us turn to BaaS presented by Amazon, as it has a clear billing system. Suppose a network with two members who want to make a deal. Each has a node with 10 G.B. of memory and records 10 M.B. of data per hour. That's the total cost for an hour: Membership for 2 participants: 0.6 USD; Cost of 2 nodes: 0.068 USD; Cost of data storage (2 by 10 GB): 0.003 USD; Data recording (2 by 10 MB) 0.002 USD. Total: 0.673 USD [51].

From the point of expected advantages, it is necessary first to determine: what problem is supposed to be solved with the help of a blockchain. If to sum up, BaaS clients receive an unchangeable register of information. This is used to prevent losses due to fraud in the industry, human factors, technical failures. The concepts of tracking and smart contracts are also widely used in various industries. Thus, to assess the effect of the Blockchain application, it is necessary to evaluate the value of information that will be improved by the Blockchain technology (in terms of integrity, completeness, relevance, integrity, reliability).

Once the goal has been defined and necessary to implement a Blockchain rather than some simpler solution, the question of how to choose a Blockchain vendor arises. Today there are several major players in the BaaS market: IBM, Microsoft Azure, Oracle, Amazon, Alibaba, Baidu, Huawei [52]. Most of these vendors offer quite flexible tools for developing Blockchain applications (for example, Microsoft Azure). The most popular Blockchain deployment frameworks are Hyperledger Fabric, Corda, Ethereum, Ant Blockchain. In most of the solutions, you will find high-performance IAM capabilities and tools for node management.

In general, the offers are different in:

- Price (here, you need to consider all aspects and do not get caught on hidden payments);
- Platform stability level;
- Development tools (the more elements are customizable, the higher the risk of error);
- Level of security and encryption;
- Speed and ease of deployment;
- Proposed consensus mechanisms.

In most cases, the company already has a certain software architecture with which it works. BaaS must provide integration with the required systems. First, it is worth assessing large Blockchain solution vendors by these criteria. However, we should not forget that there are other narrowly focused solutions as well.

Blockchain as a service has prospects for implementation in many industries: healthcare, logistics, real estate, intellectual property protection. In all companies and services, where it is possible to present transactions, it is possible to deliver the Blockchain benefits. In this case, the company will not need to hire an expensive team to develop and support software but can focus on business. This will increase trust between suppliers and customers, reduce the number of paper documents, and increase the speed of interaction. The Blockchain protects against fraud, forgery, and counterfeiting. Cases are particularly interesting in areas where fraud can cost human life. For example, DHL uses BaaS to prevent substitution of pharmaceuticals, this company turns to the vendor Accenture, which in their case is best suited for collaboration.

Blockchain as a service may well change the usual way of industry. One of the key concepts offered together with Blockchain nodes' deployment is Smart Contracts with the most widely-known platform – Ethereum. The most straightforward way to explain the future of Smart Contracts in our domain is to register information about the movement of goods using IoT devices, be visible to all network users, and not be substituted at any stage of delivery.

Thus, BaaS is a promising opportunity to take advantage of Blockchain technology in its industry without development. Solutions in the market are quite productive and applicable. By trusting vendors, you potentially save time, money, nerves at the Blockchain development stages. Fan base and community may be another option for you to consider. The more people use the solution: the easier it will be to deal with the errors that occur: and when implementing such a rather complex concept as Blockchain, they are likely to occur.

A. Related consensus algorithms

BaaS solutions allow not only to use a solution fully developed and configured by the vendor and configure your Blockchain itself only using frameworks. This solution will be more suitable in considering all the nuances of the application described in the work. When building a complete solution for areas in which the Blockchain 3.0 concept is being developed, the possibility of customization is necessary.

An important parameter of the implemented Blockchain is the consensus algorithm: it can vary significantly for different tasks and applications. The most known and used algorithms are as follows [44], [53]:

1) Proof-of-Work (PoW) is the most well-known consensus algorithm used in Bitcoin. The job is to calculate a hash suitable by parameters for adding a block to a chain in the fastest way [54]. Adding a block to a chain, i.e., conducting transactions, is rewarded, usually in the system's cryptology. Race of computation and increasing complexity of hash selection make race participants (miners) use more and more computational resources, which requires large energy costs. Adding a block reward provides an incentive to decentralize the system, but fewer and fewer competitive participants as the complexity grow. There is a vulnerability of a double-spending attack. However, a verification algorithm is implemented in bitcoin.
2) Proof-of-Stake (PoS) is a method popular because it eliminates the possibility of a double-spending attack and significantly reduces power consumption compared with the Proof-of-Work algorithm [55]. Here the participants with the largest balance of crypt-currency on the account are most likely to have the right to create

a block. There is a threat of network decentralization, as there is an additional incentive to get the largest share.

3) Proof-of-Authority is an algorithm that does not require any mining [56]. Blocks are added to the chain and checked by specific accounts approved by members. Transactions are automatically executed. This eliminates the need for cryptographic software, making it popular with Blockchain 3.0 solutions. However, the decentralization of such a system suffers.
4) Proof-of-Activity is another promising consensus algorithm that does not require heavy computation of the involved nodes but rather their involvement in the PoS-like operation of the system [7].

There are numerous other consensus algorithms, but those mentioned earlier may be the most promising from the Smart Grid perspective.

B. Measurements-related aspects

Existing concepts for the use of Blockchain in Smart Grids offer clear advantages in improving information quality. However, some application concepts do not consider that meters are often overestimated or underestimated for technical reasons. The reason for the divergent power generation and consumption data can be a change of data by the hacker, a program failure or physical impact, and a priori incorrect measurement of the energy performance of the meter, i.e., discrepancies with the measurement system. With the development of the Internet, it is possible to check and calibrate electronic measuring instruments via the Internet. This concept is being developed in Europe, the USA, and other countries and is IoM. Mobile working standards are used for calibration, which reduces the overall cost of moving measurement samples to the calibration laboratory.

Notably, remote calibration of electrical measurements is considered in [57]. Its implementation requires special software for remote control of the measurement system, measurement results, mobile working standard, calibrated measurement system, sensors for tracking foreign conditions, and the Internet channel. The calibration process allows selecting the values to be calibrated and considering uncertainties and errors inherent in electrical values. The measurement system not only passes the calibration test but can also be set up remotely.

Since data transmission is assumed, especially using the Internet, researchers are exploring ways to protect data. It is suggested that cryptographic transformations be used to protect data. In work [57] algorithms of encryption Blowfish (symmetric encryption key size 32-448 bits, block – 64 bits, number of rounds 16, the use of Feistel cipher) are proposed. The advantages of this protection method were determined as follows: simplicity of implementation, crypto stability. The efficiency of using this algorithm was proved experimentally.

Further development of the concept uses Blockchain technology to create a system for remote calibration of measurements [58]. The IoM involves the transfer of data from the system being calibrated to the calibration laboratory. The idea is to organize the transfer from one point to another without intermediaries by creating a system based on a blockchain. The data transmitted by the system being calibrated are collected in blocks, while asymmetric cryptographic protection is also applied. Each block is linked to another by adding information about the previous block and hashing. Next, data are added to these blocks for calibration. This way, the data is checked and delivered (distributed over the network). In addition, one can manage the confidentiality of data using the public key system – private key and additional encryption [59].

V. Future perspective outline and summary

By investigating aspects of the Blockchain application in such a critical area for society as energy, it is necessary to achieve maximum system stability and efficiency. The biggest issue of applying the latest Smart City concepts is the lack of public confidence in the reliability of technology, privacy and the lack of evidence that would give the public confidence in the reliability of the data [60].

In this regard, the most suitable practices for the energy sector have been analyzed, and their shortcomings found (Fig. 3). A comprehensive solution that combines the latest concepts should provide a system in which algorithms are implemented that make the industry the most transparent to the consumer. Besides, there will be mathematical grounds to consider the design reliable, maximally protected from hacker attacks, and provide reliable information.

Starting with the zero and first-level – smart generation, transmission, and metering of electricity – devices are introduced that allow the Internet measurement concept. At the same level, another Smart Grid member is added, a calibration laboratory from which the first level members can exchange data. A Blockchain-based network is built up between them, and the data is transmitted in encrypted form so that only the calibration lab can decipher the data. Adding a new participant will reduce the number of unmeasurable losses due to the devices' original mistaking. The first level aggregates information between participants in a cluster using symmetric encryption. Participants in the same group can be, for example, smart meters installed in the same house.

The next step is to bring the data to the second level, the data aggregation level. Data transfer is again based on Blockchain technology to ensure resistance to the interception of data and its change at this stage. At this level, data is fed into the information aggregators, which is the intermediate link in the system. Here, the data is stored securely, processed, and transmitted to the next architecture layer.

The last layer of the architecture is a Blockchain-based system that connects the customer with all other participants in the Smart Grid system. For the consumer, it is a kind of data showcase, and it must also provide the ability to make transactions for the purchase (payment) of electricity, i.e., to conduct the so-called smart contracts. At the same time, the system user must also be the controlling participants

of the system: electricity producers, management companies. Cryptographic transformations should ensure the delimitation of access rights to information.

Any Blockchain can be deployed with BaaS solutions depending on the customer's wishes. The Proof-of-Authority algorithm should be chosen as the consensus algorithm: this will simplify the system as much as possible since transactions must be done continuously regardless of external factors. The controlling participants of the system should automatically select the nodes of the system that create and add blocks to the Blockchain.

To summarize, the development of technology offers extensive opportunities for industry development. The prospects include increased resource efficiency, elimination of fraud and theft, more environmentally friendly production, and electricity consumption. However, to achieve a higher return on technology than the initial investment in implementation, it is necessary to understand the mechanisms of technology operation, the reasons, and evidence for its performance, the common difficulties encountered in its implementation, and the ways to address them.

In this paper, Blockchain technology was studied in applying in the electric power industry, i.e., Smart Grid.

Based on the study results, Blockchain technology has prospects for implementation at all levels of the Smart Grid concept, thus providing the entire system with cryptographic protection, the accuracy of measurements, and the inability to unauthorized change data.

The proposed architecture adds another control element, a separate company with no interest in data distortion. In this way, the data will become more reliable. At the same time, the beneficiaries of this implementation are both energy producers and consumers – the wrong measurement has a deviation in both directions.

With the increasing complexity of the technology, more and more costs are spent on development, testing, and bug fixing, but now there are opportunities to outsource development, thereby shifting the risks to solution vendors. Startups are specializing in Smart Grid and universal BaaS solutions. This makes Blockchain technology more accessible for implementation.

A further area of research may be the specific technical implementation of network blocks for Smart Grid levels. Each layer requires a personalized protection method, as it is exposed to different cyber-attacks and has various inherent vulnerabilities. Besides, an interesting direction is studying cryptographic protection algorithms – different encryption is different from common attacks.

ACKNOWLEDGEMENTS

The project group was funded by the Graduate School of Business National Research University Higher School of Economics.

REFERENCES

[1] S. Smetanin, et al., "Modeling of Distributed Ledgers: Challenges and Future Perspectives," in *Proc. of 22nd Conference on Business Informatics (CBI)*, vol. 1. IEEE, 2020, pp. 162–171.

[2] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "Blocksdn: Blockchain-as-a-Service for Software Defined Networking in Smart City Applications," *IEEE Network*, vol. 34, no. 2, pp. 83–91, 2020.

[3] M. Gorbunova, P. Masek, M. Komarov, and A. Ometov, "Distributed Ledger Technology: State-of-the-Art and Current Challenges," *Computer Science and Information Systems*, p. 37, 2021.

[4] Gartner. (2019) Top 10 Strategic Technology Trends for 2020. (accessed December 3, 2021). [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows

[5] X. Xia, Y. Xiao, and W. Liang, "SAI: A Suspicion Assessment-based Inspection Algorithm to Detect Malicious Users in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 361–374, 2019.

[6] R. Pirmagomedov, et al., "Applying Blockchain Technology for User Incentivization in mmWave-based Mesh Networks," *IEEE Access [Early Access]*, February 2020.

[7] K. Zhidanov, S. Bezzateev, A. Afanasyeva, M. Sayfullin, S. Vanurin, Y. Bardinova, and A. Ometov, "Blockchain Technology for Smartphones and Constrained IoT Devices: A Future Perspective and Implementation," in *Proc. of 21st Conference on Business Informatics (CBI)*, vol. 2. IEEE, 2019, pp. 20–27.

[8] BCS Express. (2019) How the Electricity Market Works in Russia. (accessed December 3, 2021). [Online]. Available: https://bcs-express.ru/novosti-i-analitika/kak-ustroen-rynok-elektroenergii-v-rossii

[9] "FZ 552: On Amendments to Certain Legislative Acts of the Russian Federation in Connection with the Development of Electricity (Power) Metering Systems in the Russian Federation," Law of the Russian Federation, 2018.

[10] J. Hosek, et al., "A SyMPHOnY of Integrated IoT Businesses: Closing the Gap between Availability and Adoption," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 156–164, 2017.

[11] J. D. Hmielowski, A. D. Boyd, G. Harvey, and J. Joo, "The Social Dimensions of Smart Meters in the United States: Demographics, Privacy, and Technology Readiness," *Energy Research & Social Science*, vol. 55, pp. 189–197, 2019.

[12] M. A. Akkawi, F. B. Chaaban, R. F. Olabi, and C. K. Lakkis, "Determination and Reduction of Utilities' Power System Losses using Advanced Metering Infrastructure-The Case of Lebanon," *Journal of Recent Trends in Electrical Power System*, vol. 2, no. 3, 2019.

[13] N. Shokoya and A. Raji, "Electricity Theft: A Reason to Deploy Smart Grid in South Africa," in *Proc. of International Conference on the Domestic Use of Energy (DUE)*. IEEE, 2019, pp. 96–101.

[14] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, "Smart meters for power grid—challenges, issues, advantages and status," in *Proc. of IEEE/PES Power Systems Conference and Exposition*. IEEE, 2011, pp. 1–7.

[15] A. Mannikoff and H. Nilsson, "Sweden—Reaching 100%'Smart Meters' July 1, 2009," in *Proc. of IEEE Power & Energy Society General Meeting*. IEEE, 2009, pp. 1–4.

[16] G. Nalbandyan and T. Khovalova, "The Concept Of Internet Of Energy In Russia: Drivers And Perspectives," *Strategic Decisions and Risk Management*, no. 3, pp. 60–65, 2018.

[17] "On Functioning of Retail Markets of Electric Energy, Full and (or) Partial Limitation of Electric Energy Consumption Regime," Resolution of the Government of the Russian Federation dated 04.05.2012 N 442 (ed. on 30.04.2020), 2012.

[18] "FZ 152: On Personal Data," Law of the Russian Federation, 2006.

[19] "FZ 187: About Safety of Critical Information Infrastructure of the Russian Federation," Law of the Russian Federation, 2017.

[20] Smart Meters. (2021) Technical Information on Smart Meters. (accessed December 3, 2021). [Online]. Available: https://www.smartme.co.uk

[21] P. Masek, et al., "A Perspective on Wireless M-BUS for Smart Electricity Grids," in *Proc. of 42nd International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, 2019, pp. 730–735.

[22] Masek, P. et al., "Communication Capabilities of Wireless M-BUS: Remote Metering within Smartgrid Infrastructure," in *Proc. of International Conference on Distributed Computer and Communication Networks*. Springer, 2018, pp. 31–42.

[23] C. Bekara, "Security Issues and Challenges for the IoT-based Smart Grid," *Procedia Computer Science*, vol. 34, pp. 532–537, 2014.

[24] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-Stream-based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study," *IEEE Systems journal*, vol. 9, no. 1, pp. 31–44, 2014.

[25] B. Gupta and T. Akhtar, "A Survey on Smart Power Grid: Frameworks, Tools, Security Issues, and Solutions," *Annals of Telecommunications*, vol. 72, no. 9, pp. 517–549, 2017.

[26] A. Agnihotri and S. Bhattacharya, "Unethical Consumer Behavior: The Role of Institutional and Socio-Cultural Factors," *Journal of Consumer Marketing*, 2019.

[27] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Newnes, 2013.

[28] S. Bindu, "Energy Storage Systems for Smart Meter Privacy: A Study of Public Perceptions," Master's thesis, Universitat Politècnica de Catalunya, 2019.

[29] M. R. Asghar and D. Miorandi, "A Holistic View of Security and Privacy Issues in Smart Grids," in *Proc. of International Workshop on Smart Grid Security*. Springer, 2012, pp. 58–71.

[30] F. Leferink, C. Keyer, and A. Melentjev, "Static Energy Meter Errors Caused by Conducted Electromagnetic Interference," *IEEE Electromagnetic Compatibility Magazine*, vol. 5, no. 4, pp. 49–55, 2016.

[31] M. Ge, S. Chren, B. Rossi, and T. Pitner, "Data Quality Management Framework for Smart Grid Systems," in *Proc. of International Conference on Business Information Systems*. Springer, 2019, pp. 299–310.

[32] S. Shapsough, et al., "Smart Grid Cyber Security: Challenges and Solutions," in *Proc. of International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*. IEEE, 2015, pp. 170–175.

[33] D. von Oheimb, "IT Security Architecture Approaches for Smart Metering and Smart Grid," in *Proc. of International Workshop on Smart Grid Security*. Springer, 2012, pp. 1–25.

[34] E. Vahedi, M. Bayat, M. R. Pakravan, and M. R. Aref, "A Secure ECC-based Privacy Preserving Data Aggregation Scheme for Smart Grids," *Computer Networks*, vol. 129, pp. 28–36, 2017.

[35] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *2010 first IEEE international conference on smart grid communications*. IEEE, 2010, pp. 327–332.

[36] F. D. Garcia and B. Jacobs, "Privacy-Friendly Energy-Metering via Homomorphic Encryption," in *Proc. of International Workshop on Security and Trust Management*. Springer, 2010, pp. 226–238.

[37] J. Zhang, L. Liu, Y. Cui, and Z. Chen, "SP2DAS: Self-Certified PKC-based Privacy-Preserving Data Aggregation Scheme in Smart Grid," *International Journal of Distributed Sensor Networks*, vol. 9, no. 1, p. 457325, 2013.

[38] L. Chen, R. Lu, and Z. Cao, "PDAFT: A Privacy-Preserving Data Aggregation Scheme with Fault Tolerance for Smart Grid Communications," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1122–1132, 2015.

[39] D. He, N. Kumar, and J.-H. Lee, "Privacy-Preserving Data Aggregation Scheme Against Internal Attackers in Smart Grids," *Wireless Networks*, vol. 22, no. 2, pp. 491–502, 2016.

[40] R. Liu and A. Srivastava, "Integrated Simulation to Analyze the Impact of Cyber-Attacks on the Power Grid," in *Proc. of Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*. IEEE, 2015, pp. 1–6.

[41] Y. Wang, B. Zhang, W. Lin, and T. Zhang, "Smart Grid Information Security–A Research on Standards," in *Proc. of International Conference on Advanced Power System Automation and Protection*, vol. 2. IEEE, 2011, pp. 1188–1194.

[42] K. Bhat, V. Sundarraj, S. Sinha, and A. Kaul, *IEEE Cyber Security for the Smart Grid*. IEEE, 2013.

[43] S. Smetanin, et al., "Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective," *Sensors*, vol. 20, no. 12, p. 3358, 2020.

[44] A. Ometov, et al., "An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends," *IEEE Access*, vol. 8, pp. 103 994–104 015, 2020.

[45] S. Khalid, A. Maqbool, T. Rana, and A. Naheed, "A Blockchain-Based Solution to Control Power Losses in Pakistan," *Arabian Journal for Science and Engineering*, pp. 1–11, 2020.

[46] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-Security in Smart Grid: Survey and Challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.

[47] X. Chen, et al., "A Blockchain-Based Privacy-Preserving Scheme for Smart Grids," in *Proc. of 2nd International Conference on Blockchain Technology*, 2020, pp. 120–124.

[48] M. M. Esfahani and O. A. Mohammed, "Secure Blockchain-based Energy Transaction Framework in Smart Power Systems," in *Proc. of 44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2018, pp. 260–264.

[49] Z. Guan, et al., "Privacy-Preserving and Efficient Aggregation based on Blockchain for Power Grid Communications in Smart Communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[50] M. N. Kurt, Y. Yılmaz, and X. Wang, "Secure Distributed Dynamic State Estimation in Wide-Area Smart Grids," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 800–815, 2019.

[51] Amazon Web Services. (2021) AWS Blockchain. (accessed December 3, 2021). [Online]. Available: https://aws.amazon.com/ru/blockchain/

[52] 101 Blockchains. (2021) Blockchain as a Service: Enterprise-Grade BaaS Solutions. (accessed December 3, 2021). [Online]. Available: https://101blockchains.com/blockchain-as-a-service/

[53] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on Private Blockchain Consensus Algorithms," in *Proc. of 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*. IEEE, 2019, pp. 1–6.

[54] S. Nakamoto, "PBitcoin: A Peer-to-Peer Electronic Cash System," Manubot, Tech. Rep., 2019.

[55] S. King and S. Nadal, "PPCOIN: Peer-to-Peer Crypto-Currency with Proof-of-Stake," *Self-published paper*, vol. 19, p. 1, 2012.

[56] S. De Angelis, et al., "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain," 2018.

[57] O. N. Velichko and R. V. Gurin, "Organization of Remote Calibration of Measuring Instruments of Electrical Quantities," *Georesource Engineering*, vol. 49, no. 2, p. 113, 2014.

[58] D. Peters, J. Wetzlich, F. Thiel, and J.-P. Seifert, "Blockchain Applications for Legal Metrology," in *Proc. pf IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. IEEE, 2018, pp. 1–6.

[59] Y. Bardinova, et al., "Measurements of Mobile Blockchain Execution Impact on Smartphone Battery," *Data*, vol. 5, no. 3, p. 66, 2020.

[60] C. Milchram, G. Van de Kaa, N. Doorn, and R. Künneke, "Moral Values as Factors for Social Acceptance of Smart Grid Technologies," *Sustainability*, vol. 10, no. 8, p. 2703, 2018.