Application of blockchain for secure data transmission in distributed state estimation

S. Asefi, Y. Madhwal, Y. Yanovich, and E. Gryazina

***Abstract*— The application of renewable energy sources in the power grid increases the necessity of tracking the system's state, especially in smart grids, where there is a bidirectional transfer of data and power. The complexity of coupling between communication and the electrical infrastructure in a smart grid will create a higher chance for security breaches. Increasing the state estimation accuracy will help the smart grid operator efficiently manage the system. The paper proposes an integration of distributed state estimation with a blockchain-designed communication platform. Additionally, the asynchronous manner for data transmission, which is more likely to happen in the real world, has been considered as the second task of this research. Finally, a detailed analysis of the blockchain-based application in distributed state estimation is provided. The numerical analysis shows that the proposed method meets real-world performance requirements and brings high security and reliability to the distributed state estimation process.**

***Index Terms*— Blockchain, Distributed algorithms, Optimization, Power system control, Smart contract, State estimation**

I. Introduction

POWER grid has faced different challenges due to the increasing utilization of the distributed energy sources and the non-stop escalating level of energy demand [1]. Hence, state estimation (SE) plays an essential role in justifying and regulating system operator decisions like economic dispatch, load frequency control, electricity markets, and load forecasting. It is to be noted that advanced SE can improve monitoring and controlling the power grid in case of a contingency. Especially for the smart grids in which bidirectional transfer of electrical energy and system/consumer data increases the complexity [2], [3]. Such a system can be divided into two integrated parts, i.e., physical equipment of a traditional power system (Physical part) and telecommunication equipment (Cyber part). Combining these two parts will lead to a cyber-physical power system (CPPS) [4].

A. Power system state estimation

Although SE is highly comparable to the conventional load flow, it considers the unpredictable errors that might originate due to unexpected system changes, meters or communication system errors, inaccuracy in equipment calibration, planned manipulation from a malicious attacker, etc. [3], [5]. Additionally, conventional load flow analysis does not consider redundancy and imprecision of the system's measurement data, whereas SE considers the mentioned features [5].

Considering a brief background of the evolution of the SE method and its application in power system, it is worth noting that as soon as Schweppe pointed out the application of SE in power system, it attracted industrial communities' attention [6]. However, they did not apply the basic weighted least squares (WLS) method proposed by him at the beginning but utilized two different methods, developed by Dopazo [7], and Larson [8]. However, after a while revised version of Schweppe's method was admitted, and those two methods were excluded from industrial applications [9]. Taking into account the sparsity of the gain matrix, different researchers made several attempts to slightly improve the WLS estimator [10]. Also, SE-related issues like ill-conditioning appeared afterwards, and several methods such as the inclusion of zero injection power within constraints of SE were proposed to overcome these issues [2], [11], [12]. Schweppe et al. proposed applying non-quadratic estimators for bad data detection within the early years. Later on, there were plenty of studies on methods for identifying bad data, such as application of least absolute value [13]. It is to be noted that from the early stages of utilizing SE, the mentioned areas and problems have been an active research area for the power systems, operations and control research community.

Growth of the power system due to increase in the level of needed electricity consumption and propagation of the communication technology, bring in several problems assigned with power system operation, especially centralized SE (CSE) such as *Expansion of power system continent-wise*, *Policy and privacy*, *Dimension of the grid*, *Communication bottleneck*, *Data size* and *Security/Reliability*, to name a few.

Expansion of the power grid over continents makes an interconnected system such that these continents can be affected by contingencies in other ones [14]. Although, in some regional expansion cases, e.g., the case with regional transmission organizations (RTOs) in Europe, operators are using HVDC technology for power transfer which is also another research area for considering hybrid HVDC/AC SE so that

S. Asefi and E. Gryazina are with center for energy science and technology (CEST), Skolkovo institute of science and technology (Skoltech), Moscow, Russia (e-mail: sajjad.asefi@skoltech.ru), (e-mail: e.gryazina@skoltech.ru).

Y. Madhwal and Y. Yanovich are with center of computational and data science and engineering (CDISE), Skolkovo institute of science and technology (Skoltech), Moscow, Russia (e-mail: yash.madhwal@skoltech.ru), (e-mail: y.yanovich@skoltech.ru).

This work was carried out as a part of the AMPaC Megagrant project supported by The Ministry of Education and Science of Russian Federation, Grant Agreement No 075-10-2021-067, Grant identification code 000000S707521QJX0002.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2021.3134135, IEEE Transactions on Control of Network Systems

they can meet the characteristics of the new network regarding Supervisory Control and Data Acquisition (SCADA) system [15]. Vulnerability and inflexibility of CSE make it unsuitable for a multi-area (or multi RTO) estimator from policy and privacy point of view [14]. The grid's high dimension is another challenge that affects the computational difficulty [16], [17]. Having only one central control unit, extensive network parameters and measurement unit's information, which needs to be transferred to this unit, may result in communication bottlenecks [18], [19]. Another problem that has attracted the researcher's attention, especially in smart grids, is that the size and the speed of receiving data (so called big data) from measurement units might be infeasible to be stored and processed [3], [20]. Moreover, in most of the literature, it is assumed that the central node is secure, though it can be the most vulnerable, insecure, and unreliable point in a network and prone to a single point of failure [3], [21].

B. Power system distributed state estimation

One way to overcome CSE issues would be implementing the distributed state estimation (DSE). In DSE, the power system will be divided into several smaller areas or subsystems, and the SE process will take place concurrently in each area. A low amount of information exchange at borders of the areas is required so that each area reaches convergence, i.e., the distributed network reaches a similar solution as the centralized one. The amount of information that must be exchanged depends on the method applied. In [22], a detailed comparison of the recent DSE methods regarding indices such as convergence rate and information exchange has been made, which clearly confirms that each method varies from one another considering information transfer between areas.

The DSE algorithms can be classified into two categories, having a global control center, i.e., hierarchical DSE [23]–[25] or fully distributed [19], [22], [26]. Both of them are successful in reaching to an acceptable solution compared to centralized algorithms. Alternating direction method of multipliers (ADMM) [27] that are in the category of distributed optimization [14], have been very popular recently. In [28], a fully decentralized adaptive SE scheme has been presented for the power system via applying the network gossiping method. The method enables collaboration between areas to solve the global problem; however, there is still a significant performance error in comparison to CSE. Authors in [29] presented a DSE for wide area monitoring system, which does not need local observability of all areas. In [30], a new multi-area SE method is discussed that utilizes a central coordinator; however, there is no need to exchange topology information between areas or from areas to the central coordinator. The proposed approach in [31] is a new hierarchical multi-area power system SE, which shares the sensitivity function of local estimators instead of boundary measurements or state estimates. As stated by the authors in [31], the approach reduces the information exchange, as well as increases convergence speed. In [21], the authors have provided an ADMM based DSE. Also, in [32] and [19], a DSE process using matrix splitting method for DC and AC SE, respectively. For more details, we refer to [33] that presents a brief review of multi-area SE.

It is to be noted that mostly in the literature, the transmission system has been a matter of concern, which we have followed the same approach. To solve AC SE via centralized method or some of the distribution methods, such as matrix splitting or ADMM, would need linearization of the problem using Newton's method. However, by applying the decomposition method [14] and the available solvers, there would be no further need for linearization of the problem.

C. Blockchain

Blockchain (BC) is a peer-to-peer distributed ledger technology that stores data on multiple servers globally. In 2008, Satoshi Nakamoto's whitepaper on Bitcoin [34] pioneered the use of BC technology in financial application [35]. BC technology was primarily used in the financial domain, so as to providing trustfulness and secure environment without central authority where digital assets like cryptocurrency can be prevented from double-spending attacks [36], [37]. Since then, the technology's potential has moved beyond financial domains to different sectors like supply chain management, healthcare, etc. [38]–[42].

BC is a distributed ledger of chronologically generated blocks containing cryptography linked blocks to the previous block forming a chain. Any modification to the previous existing block will be reflected on every subsequent block, making it secure and immutable to modification. If an attacker changes data on any of the previous blocks, the following block's data will also change, and the ledger can be compared with another copy to track the point at which the data was manipulated and later rectified. In cryptocurrency, it is computationally hard to take control over the BC network because the attacker will require 51% of the network's computing power, i.e., it will be difficult for an attacker to fork from a past block and mine blocks faster, surpassing current (honest chain) block height. This will create double spending, which computationally hard [43]. BC-based applications can provide security, trust, economic, and auditability [44].

Since Bitcoin, many alternative cryptocurrencies (altcoins) have emerged. Ethereum [45] is the most popular cryptocurrency after Bitcoin, which provides an open-source platform to develop BC-based decentralized applications (DApps). DApps are application programs that runs on decentralized BC applications using Ethereum Virtual Machine (EVM). For example, smart contracts can specify the functionality and condition, under which circumstances payment can occur between two individuals. These conditions are programmed and deployed on the BC, and individuals can abide by these conditions and transact in a secure environment without intermediaries. EVM is one big computer that is made of small individual computers located globally. These computers are nodes connected, having a copy of the Ethereum BC. The transactions are broadcasted to the network via a node which is replicated across the network. For feasibility demonstration of BC for secure data transmission, we have developed a prototype on the Ethereum platform using truffle framework [46] which can be deployed on local machines. We have created a smart contract, specified

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCNS.2021.3134135, IEEE Transactions on Control of Network Systems

conditions and deployed it on a BC network running on local devices.

Aside from financial applications of BC, it has been developed in other fields. For example, in [47], the authors propose a BC based method to preserve security of the spectrum sharing between aerial (unmanned aerial vehicle as a component of next generation cellular network) and terrestrial communication systems. Application of BC in the smart grid mainly has been investigated in the area of power markets, i.e., the issues related to the secure energy transactions [1]. In [48], a proof of concept (PoC) for decentralized energy trade using BC has been proposed, to enable peer to peer energy transactions. A BC based platform for solar energy trade amongst prosumers has been implemented in laboratory scale in [49]. However, a few works have been applied BC in power system for security purposes, [50], [51]. These studies consider storing system wide measurement data in each measurement, which seems inefficient due to low memory of measurement units and time delay caused by encryption/decryption of the data.

Three main security features for the data in a smart grid are *Confidentiality*, *integrity* and *availability*, which they refer to occasions when the data are accessible only to authorized users, the data are trustworthy in any operational circumstances, and the data are promptly and reliably available, respectively [52]. Cyberattacks, such as the denial of service (DoS) or false data injection (FDI), aim to deteriorate such properties. Noting the case when a central control unit gets compromised, all data can either get lost or controlled by the attackers (same case happened in Ukraine's cyber-attack [53]), and one of the potential solutions could be a distributed control scheme. However, the distributed grid can also be subjected to a cyber-attack, i.e., attack to measurement units, to control centers, to communication line between control centers and measurement units, to communication line between control centers (i.e., between areas). Due to the mentioned BC properties, in this paper an integration of DSE with BC has been proposed to eliminate such an opportunity for the attackers while information transfer occurs between areas.

The work in this paper is inspired by [3]. However, we have considered static SE, whereas they have considered dynamic SE. Dynamic SE refers to estimating the dynamic variables of the system (machine/dynamic load/distributed energy resources' dynamic variables), and static SE (which already applicable in energy management system) hands out the algebraic variables of the system, i.e., voltage magnitude (v) and phase angle (θ) for each bus [54]. The second one is that in [3], the DC approximation of the power system has been considered while here the AC, SE has been studied. The third difference is considering the asynchronous behaviour of the information transfer within the power network that has not been provided in [3]. And finally, detailed analysis and design of BC aided data transmission for DSE.

Beyond the numerous features of this research, the main contributions of this work can be summarized as follows:

- Implementation of BC based DSE method, which requires low data transfer and provides high accuracy.
- Application of a new technology (i.e., BC) to increase the data transfer security in the power system.
- Consideration of asynchronous and delayed data transfer that might happen within the DSE.
- Analysis and open-source code implementation for the design of BC aided data transmission in DSE.

The rest of the paper is organized as follows. In the second section, we present the modelling of SE, BC and designed system architecture. In the third section, the problem formulation is presented. The fourth section provides the graphical and numerical performance analysis. Finally, in the section V the research work is concluded.

II. System model

In this section, the mathematical equations governing the DSE problem is presented. Decomposition method has been selected to solve DSE problem [14]. Later on, BC architecture and asynchronous data transfer are discussed.

A. Distributed state estimation

Given the noisy measurements and network parameters available in the power system, SE's role is to infer the state of the system. This study's measurements are considered as power flows, power injections and voltage magnitudes. In order to model the power network, considering the set of the measurements as z, the vector of errors associated with these measurements as e and the set of nonlinear physical equations governing the power system that relates the state variables to the measurements as $f(x)$, we can state the following equation [2]:

$$z = f(x) + e. \tag{1}$$

It is noted that state variables, x, in this study are considered as voltage magnitudes and phase angles for each bus in the network, taking into account the phase angle of slack bus (bus number one) as zero. Taking into account two assumptions for e, that these errors are mutually independent and follow a normal distribution function, one can use the maximum likelihood method and get the following optimization problem:

$$\min \sum_{i=1}^{m} W_i (z_i - f_i(x))^2, \tag{2}$$

where residual of i^{th} measurement is defined as $r_i = z_i - f_i(x)$ and W_i is the weighting factor to each measurement (inverse of the squared measurement variance, i.e., $W_i = \sigma_i^{-2}$). In DC SE, the f function would be approximated by a linear function. However, in AC SE, we would need to use Newton's method to linearize the problem and then solve it iteratively.

Without loosing generality, to apply DSE via decomposition method the network would be divided into N areas (or control centers), and the formulation represented in (2) should be separated for each area. Therefore the formulation of the optimization problem for each area can be represented as follows:

$$\min \sum_{i=1}^{m_N} W_{N,i} (z_{N,i} - f_{N,i}(x_N))^2, \tag{3}$$

where $z_{N,i}$ is the measurements inside area N, m_N is the number of measurements in area N, $W_{N,i}$ is the weighting factor corresponding to the measurement $z_{N,i}$ and $f_{N,i}$ is the equation related to this measurement. x_N represents the set of state variables inside the N^{th} area, plus the set of auxiliary variables. The idea of auxiliary variables is to provide a consensus for the solution and it is due to the power line connections between areas. This will lead to the need for information transfer within the borders of these interconnected areas. In section III, we will discuss the formulation of DSE and auxiliary variables in more details.

B. Blockchain Architecture

BC is a digital ledger of transactions distributed across the network of computer systems, with atomic changes to the database. The integrity and tamper-resistance of the transaction logs are assured because of the cryptographic hash linked among the blocks. BC is usually assumed to be decentralized architecture maintained by individual parties. Each node of the network owns a copy of the BC. Each BC block contains transactions, and every time a new transaction occurs on the BC, it is broadcasted to all nodes and added to a block along with other transactions waiting to get committed in a block. This technology has developed over the last decade and can be categorised as private, public or consortium BC, each further divided by permissioned or permissionless. As shown in Fig. 1, every new block N generated at time T contains information from the previous $N-1$ block generated at time T', where $T > T'$.

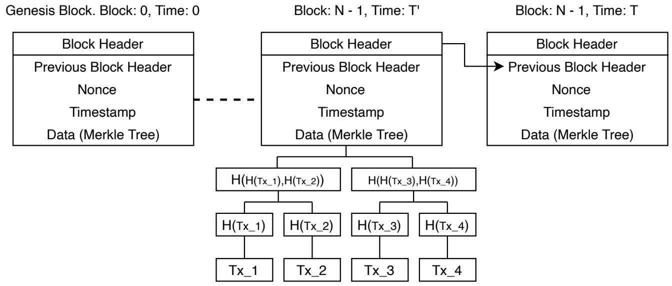

Fig. 1. Data organization in blockchain

1) Consensus algorithm for decentralized ledger: BC is a peer-to-peer network of nodes that functions individually without any central authority. Each node of the network can function individually, i.e., update ledger (creating and adding a block to the BC) and broadcast new block to the other nodes of the network using the gossip protocol [28]. The nodes verify the broadcasted block's validity, and have to either accept or reject the proposed block, thus reaching a consensus. In distributed ledger technology, there exists a fundamental problem of reaching consensus. Majority of the BC projects use any of the three most common consensus algorithms, i.e., proof of work (PoW), proof of stake (PoS), and Byzantine fault tolerant. Similar to Bitcoin, Ethereum uses a PoW consensus algorithm. In December 2020, Ethereum 2.0 was launched, which uses PoS consensus. In PoW BCs, block creators (which are called miners) are rewarded with mining rewards along with transaction fees included in the block. This mining reward is the incentives for using computation power and electricity in finding the correct nonce within the target range.

Miners have to perform computation by running a hash of block's content and incrementing a nonce until it produces a value less than the target. Nonce is an integer that starts from 1 and increments until it produces a hash of block's content less than specific target value [34]. Generating a hash on an arbitrary size input is a one-way function that produces a fixed output length [55], i.e., given input, we can generate an output of fixed-length, but not vice versa. The hash function used is cryptographically secure and with brute force there exists a potential solution with complexity of $O(2^n)$ for $H(m) = H(m')$, where H is a SHA function [56] on an input m and m' and $m \neq m'$. This means that for a fixed output length on n, for example, $n = 256$ in the case of SHA256, the probability of success is $k/2^n$, where k is a number of queries [57].

2) Ethereum Architecture: A computer (node) can be a full node or light node [58] running an instance of the Ethereum BC. A full node stores the entire BC data and can serve any request. It verifies all blocks and states and can propose a new block to append on the ongoing chain. Light node stores only the header of the chain and can verify the validity of the state roots' data in a block header. To interact with the DApp, clients should interact with the BC by running a full node by itself and using ethereum clients, like Geth, OpenEthereum, etc., to interact with the network. Ethereum BC has grown and consumes a significant storage amount and can be difficult to run a full node. Therefore, via a third-party platform like Infura, Alchemy, etc., [59], [60] provides application programming interface (API) to interact with ethereum BC feasible.

Ethereum comprises two main components:

- *Database:* All activities on the network are recorded on the BC in the form of a transaction. Sending cryptocurrency from one address to another is recorded in a transaction with valid signatures and broadcasted to the network where other nodes commit to a block after verification. PoW consensus algorithms make sure that all the nodes in the network have the same BC data as all the valid transaction data. The data are stored in the form of a Merkle Patricia Tree. There are two types of addresses in Ethereum, Externally Owned Account (EOA), controlled by private keys and Contract Address, controlled by contract code. When a smart contract code is compiled and deployed from EOA, a contract address is created, and bytecode is stored in it.
- *Code:* The smart contract is stored on the BC in a contract address in the form of code, known as byte code. The codes in contract addresses execute contract when a transaction is sent from EOA to contract addresses.

For each transaction on the Ethereum BC, there is a fee known as Gas for executing transactions. Once a transaction is added to the block, the transaction fee goes to the miner as a reward for using computational resources. Gas is a unit to measure computation difficulty in Ethereum Virtual Machine (EVM). Gas is charged only when data are modified on the BC, i.e., reading and accessing data are not chargeable. Once the sender signs a transaction and broadcasts it, the Ethereum protocol debts gas fees in a fraction of ethers from the Ethereum account, lack of required gas amount will not allow the transaction to be execute. If there are no fees, attackers can flood the node's memory pool with bogus transactions, causing distributed DoS attacks. Gas is not fixed for the transaction but it is variable and depends on the computational difficulty of a smart contract. The sender of the transaction pays gas, and the miner who mines a block receives gas. Miner receives all the transaction gas that he includes in the block along with the block generation reward. Miners set the price of gas based on the computational power of the network required to process transactions and smart contract.

Since ether is not stable in value but sees daily change, therefore gas is a relative price converted to ethers based on the load on the network. In a congested network, the gas price will increase for each unit of gas. So there is a gas price, i.e., how many units of ether are transactor willing to pay for one gas unit. Each opcode in Ethereum has a cost. The total cost of the contract is the summation of all the opcodes [61].

The EVM is a virtual stack embedded within each full Ethereum node that allows anyone to execute arbitrary bytecodes and plays a crucial role in the consensus engine of the Ethereum system. It allows anyone to execute arbitrary code in a trustless environment in which the outcome of execution can be guaranteed and is entirely deterministic. When you install and start the Geth, parity or any other client, the EVM is started, and it starts syncing, validating and executing transactions. The EVM is Turing complete, i.e., capable of performing any algorithm.

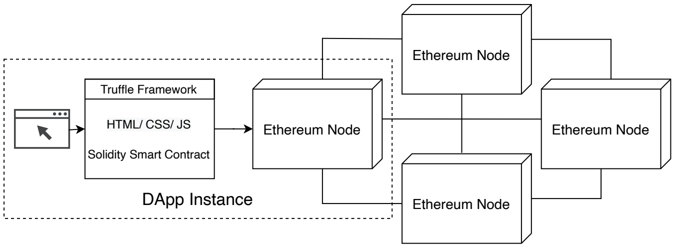

Fig. 2. Ethereum network structure

3) Data Verification: Before broadcasting the data that contains the formation of the transaction to other nodes in the network, the data should be signed using the private key. A signature is required to prove that the sender of the data are genuine and not an imposter who signed the message without the private key. BC uses asymmetric cryptography based on public key infrastructure. Like a physical signature, digital signatures are used to authenticate electronically a document's contents like pdf, emails, etc. [62].

In the BC network, each node has its pair of public and private keys, and the public key is shared with all the other nodes. Owning a private key is equivalent to owning or controlling a node associated with its public key and accessing the activities restricted to it.

To sign a message (or data), a function is calculated using the private key of the document's sender. The recipient's using the public key of the sender, can verify if the document is correct and not tampered.

C. Asynchronous data transfer

The combination of renewable energy sources and information and communication technology (ICT) changes the power system's nature from a physical system to a CPPS [4]. Therefore, the physical part consists of a power grid, and the cyber part comprises a control and computation layer. The physical layer consists of physical elements such as generators, transmission lines, transformers, etc. On the other hand, the cyber layer is responsible for computation, analysis and assessment of the power grid, and includes elements such as sensors, communication medium, control system, etc. [4]. A CPPS encounters different types of cyberattacks, such as DoS and FDI. However, latency attack has the potential to be considered as a new type of attack in the area of the power system, while it is already well-known for wireless network community [63]. The power system undergoes a time delay of several milliseconds, while increasing this latency or time delay maliciously may lead to the power system instability [63]. Although the application of distributed methods and implementation of a BC based communication network may dissolve the issue, still there would be a chance that the latency happens for the system. To study such a case, we have considered a delay in data transfer between areas in a randomized manner. In other words, at some iterations, an area randomly (based on uniform probability distribution) will be selected so as not to update its state variables. The comparison of the DSE results with and without delay is presented in section IV.

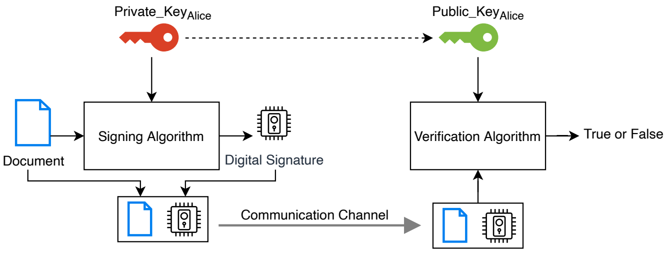

Fig. 3. Data verification using private and public key

III. Problem formulation

Suppose that we have divided the power system into N areas, having z_N measurements composed of power injection, power flow and voltage magnitude. Considering x_k as the state variables related to area k and $\tilde{x}_l$ as the auxiliary variables estimated by area k related to its neighboring area l, one can rewrite (3) into the following equation:

$$\min_{x_k} \; f_k(x_k) + \sum_{l \in \Lambda_k} f_{kl}(x_k, \tilde{x}_l), \tag{4}$$

where Λ_k indicates the set of all neighboring areas of k^{th} area. It is clear that (4) is composed of two statements. The first statement is related to the measurements that the physical equation for calculating them only requires the state variables inside the area and can be written as follows:

$$\begin{aligned} f_k(x_k) = {} & \textstyle\sum_{i \in \Lambda_k^v} W_{k,i}^v (v_{k,i}^m - v_{k,i})^2 \\ & + \sum_{i \in \Lambda_k^P} W_{k,i}^P (P_{k,i}^m - P_{k,i}(.))^2 + \sum_{i \in \Lambda_k^Q} W_{k,i}^Q (Q_{k,i}^m - Q_{k,i}(.))^2 \\ & + \sum_{(i,j) \in \Lambda_k^{PF}} W_{k,ij}^{PF} (P_{k,ij}^m - P_{k,ij}(.))^2 + \sum_{(i,j) \in \Lambda_k^{QF}} W_{k,ij}^{QF} (Q_{k,ij}^m - Q_{k,ij}(.))^2, \end{aligned} \tag{5}$$

where i and j are arbitrary buses; Λ_k^v, Λ_k^P, Λ_k^Q, Λ_k^{PF} and Λ_k^{QF} indicate the set of voltage, active power injection, reactive power injection, active power flow and reactive power flow measurements in area k, respectively; $W_{(.)}^{(.)}$ weighting factor for the measurements; $P_{(.)}^m$, $Q_{(.)}^m$ and $v_{(.)}^m$ are the active power injection or power flow, reactive power injection or power flow and voltage observed measurements, respectively; While $P_{(.)}$, $Q_{(.)}$ and $v_{(.)}$ are the physical equations of these measurements. These physical equations governing the power system are provided in appendix.

The second statement of (4), is related to the measurements in k that need to receive state values regarding the buses in connection with the neighboring area l. It is to be noted that, for calculation of the physical equations regarding these measurements, we use the auxiliary variables:

$$\begin{aligned} f_{kl}(x_k,\tilde{x}_l)=&\textstyle\sum_{i\in\Lambda_{kl}^P} W_{kl,i}^P(P_{kl,i}^m-P_{kl,i}(.))^2 \\ &+\sum_{i\in\Lambda_{kl}^Q} W_{kl,i}^Q(Q_{kl,i}^m-Q_{kl,i}(.))^2+\sum_{(i,j)\in\Lambda_{kl}^{PF}} W_{kl,ij}^{PF}(P_{kl,ij}^m-P_{kl,ij}(.))^2 \\ &+\sum_{(i,j)\in\Lambda_{kl}^{QF}} W_{kl,ij}^{QF}(Q_{kl,ij}^m-Q_{kl,ij}(.))^2+\sum_{i\in\Lambda_{kl}} W_{k,i}^{\tilde{v}}(v_{l,i}-\tilde{v}_{l,i})^2 \\ &+\sum_{i\in\Lambda_{kl}} W_{k,i}^{\tilde{\theta}}(\theta_{l,i}-\tilde{\theta}_{l,i})^2, \end{aligned} \tag{6}$$

where $\tilde{\theta}_{(.)}$ and $\tilde{v}_{(.)}$ are the auxiliary variables. It is worth noting that the last two statements in (6) are utilized to provide a consensus for this minimization function.

A. Proposed Blockchain Solution

Building DSE's data transmission architecture based on BC provides a security feature of the technology to transfer data among system areas. BC integration can ensure honesty in the system as the transaction's sender can only sign each transaction.

A PoC is developed on the Ethereum test network and deployed using Truffle framework and Ganache. Ethereum provides tools to build smart contracts and decentralized applications without any downtime or any third-party interference. Truffle Suite is a BCs development environment, testing framework, and asset pipeline using the EVM. Ganache [64] is a personal BC for Ethereum and Corda based distributed application development. Utilizing Ganache and Truffle, the entire DApp can be developed in a safe and deterministic environment. The code repository containing open source prototype is available in [65].

The EVM has separate storage areas:

- All contracts have state variables, and the state variables are stored on the BC, i.e., the data are recorded into the BC itself. When the contract executes some code, it can access all the previously stored data in its storage area.
- Memory holds temporary values and only exists in the calling function and has less gas price because the stored memory gets erased between calls. Gas price increases with the size of memory scaling quadratically. Though, comparatively cheaper than storage.
- The stack holds small local variables, and here the computations happen. This data can only hold a limited amount of values up to 1024 small local variables.
- Logs store data in an indexed structure with mapping, and with filters, specific data can be accessed. Logs are inaccessible to contract but are mainly used for events that occur on the BC.

B. System Overview

The proposed BC solution focuses on establishing a secure architecture of transferring arbitrary data for every iteration among the DSE areas based on the established connections on the BC. Fig. 4 shows the main participating entities of the system:

- *DSE areas*: The control center at each area is responsible for receiving data and then, calculate SE and after that send data to another area.
- *Auditor*: Provides public key infrastructure [66] to all DSE areas and is responsible for maintaining smart contracts on the BC and can establish or demolish connection between two areas. In other words, only the auditor can establish communication between two or more than two areas by sending a transaction to the smart contract address that sets communication to *true* between areas on the smart contract. Auditor is like a supervising body of the infrastructure of the DSE network. Although, it is responsible for deploying contracts on the blockchain, the DSE areas can communicate, i.e., transfer date, with each other via smart contract without interference from the auditor. If any issues arise on the BC, the auditor can resolve this issue with the BC. The DSE data transactions are independent, and the auditor is not involved.

C. System Design

On the BC, two contracts are deployed. First, to establish/demolish connection between the areas. Second, to transfer data per iteration between the areas within the established connection. The following section describes the details.

1) Establishing/Demolishing Connection:

The auditor manages the connections between areas through algorithm 1. The smart contract emit event upon each connection change to inform all the areas.

2) Data Transfer:

Algorithm 2 smart contracts listens to all the transaction call of the first deployed smart contract and as per update the state of the connections of this smart contract. This algorithm takes four parameters i.e., *sender*, *receiver*, *iteration* and *payload*. Each area in our case study has a different data payload size (i.e., state variables which needs to be transferred). With each iteration, data are passed as arrays of float integers as string type because it is impossible to pass a negative number in a smart contract. With each transaction of the iteration, the transaction event is emitted and notified to the receiving area, who can process the data off-chain as peruse.

D. Security

This architecture provides security because each transaction requires a transaction signature. The connection can only be established by the smart contract owner as there is a specific check-in of the smart contract that requires signature

Algorithm 1 Establish/Demolish area Connection

```
Input: address_deployer, address_from, address_to
    Initialization: $connection(from, to) \leftarrow bool$
if ($msg.sender \neq address\_deployer$) then
    from ← address from
    to ← address to
    if ($from \neq to$) then
        if ($connection(from, to) \neq True$) then
            Set connection(from,to) ← True
        else
            Revert and show error ”Connection exist”
        end if
    else
        Revert and show error ”No Self Connection”
    end if
else
    Revert and show error ”Only Owner Access”
end if
```

Algorithm 2 Data Transfer

```
Import: ‘Establishing Demolishing Connections’
Input: address_sender, address_to, interation_number,
    data_String
if ($msg.sender \neq address\_sender$) then
    if ($connection(from, to) = True$) then
        Call function to transact these values on blockchain
        Notify transaction in the network
        Apply the transferred data in the current iteration for
        state estimation
    else
        Revert and show error ”No Connection”
    end if
else
    Revert and show error ”Only msg.senders”
end if
```

verification. Signature is created using the private key, and address generation also requires a private key. Therefore, losing the private key, especially by the auditor, i.e., controller of the architecture, can compromise the whole system.

IV. Simulation Results and Discussion

In this section, the test case (i.e., IEEE 14 bus system [67]) results are presente utilizing the proposed method. The system has been divided into four areas and Fig. 4 shows the topology of the studied test case.

In this research, AC SE has been considered, where the state variables would be voltage magnitudes and phase angles at each bus. The number of state variables and measurements are 27 and 41, respectively. The weighting factor for all measurement units has been considered equal to 10^4. In order to solve (4), MATLAB (version *R2018b*) solver (Sequential quadratic programming) has been applied and for initiation of the optimization process the initial value for state variables have been set to flat start, i.e., voltage magnitude of “1” and phase angle value of “0”. Moreover, the bus number one has been selected as the slack bus with phase angle zero. To evaluate the prototype’s performance, the smart contract was deployed on a local BC server and interacted with the python application. The experiments were performed on a computer with memory 16 GB 2400 MHz DDR4, Intel Core i9 running @2,3GHz.

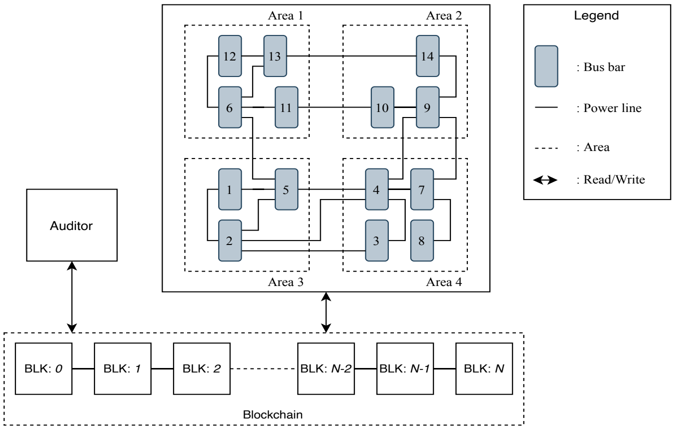

Fig. 4. Distributed topology of the IEEE 14 bus system [32] integrated with blockchain

As mentioned before, we have considered two different cases. The data transfer between areas are simultaneously in the first case and with latency (time delay) in the second case. The graphical and numerical results of both cases are presented.

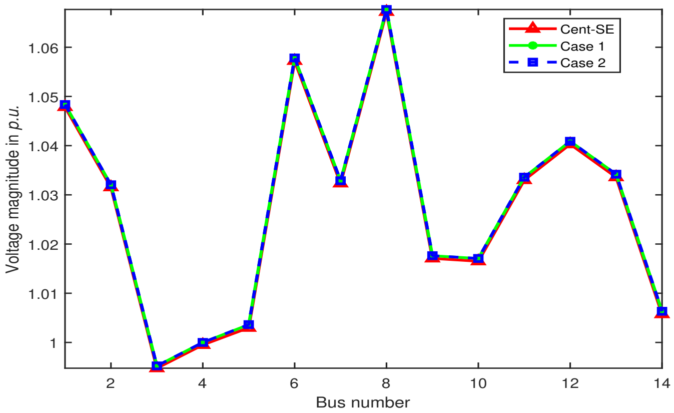

Fig. 5. IEEE 14 bus system voltage magnitude for centralized (Cent-SE) and distributed state estimation interacting with blockchain (case 1 and case 2)

Fig. 5 and Fig. 6 represent the comparison of centralized and distributed estimated voltage magnitude and voltage phase angle for IEEE 14 bus test system interacting with BC. The distributed method has succeeded to reach the centralized values in both cases.

Fig. 7 shows the distributed method objective value during the IEEE 14 bus system’s optimization procedure. As proposed in [22], we have considered the state variables convergence rate as convergence criterion. It means that the difference between obtained state variables of two successive iterations are measured at each area and if the value is below the specified threshold (it has been set to 10^{-6} [22]), the optimization stops. It is clear that in case 2, where there is a delay in data transmission, the number of optimization iteration increases.

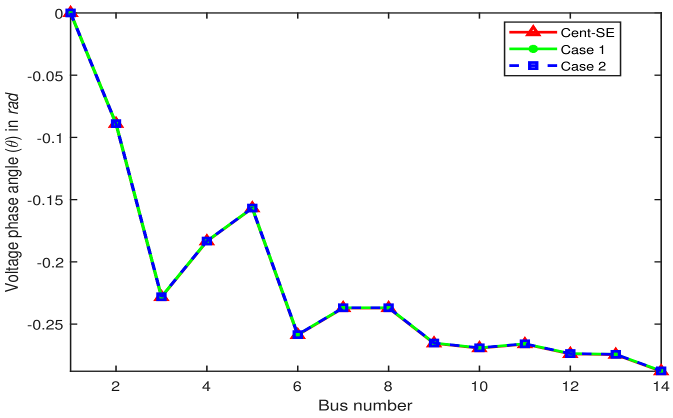

Fig. 6. IEEE 14 bus system voltage phase angle for centralized (Cent-SE) and distributed state estimation interacting with blockchain (case 1 and case 2)

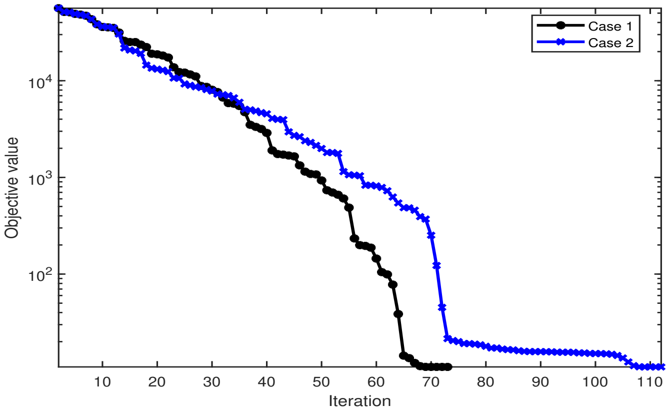

Fig. 7. Distributed method objective value during iteration for case 1 and case 2

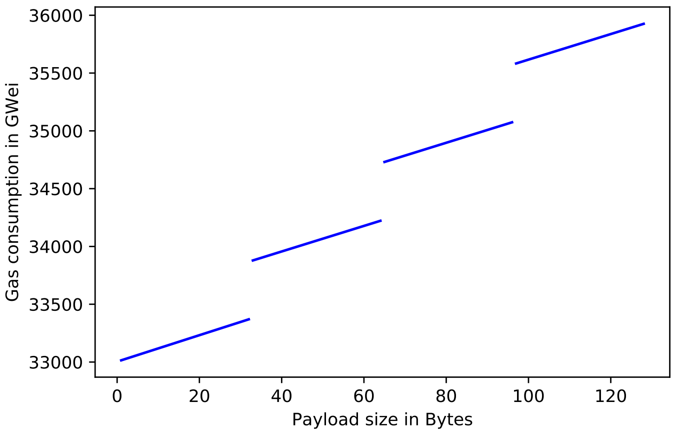

Fig. 8. Gas consumption in Gwei to transfer bytes with payload size

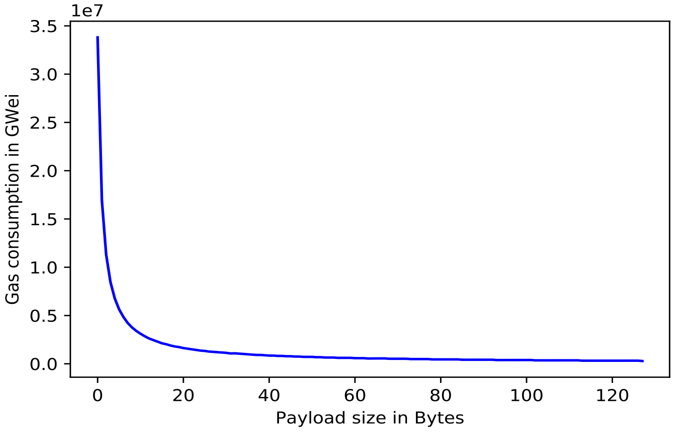

Fig. 9. Gas consumption to transfer 1024 bytes per payload size in Bytes

The numerical results of the comparison between CSE and DSE are presented in table I. The iteration number and objective value of both centralized and distributed are presented. As mentioned in section II, the objective value for CSE is obtained using (1) and applying Newton's method. However, for DSE, after solving the optimization problem stated in (4) for all areas, we gathered the state variables and placed these state variables into (1). The objective values are obtained by substituting the DSE state variables into (1).

TABLE I
NUMERICAL RESULTS OF COMPARING CENTRALIZED AND DISTRIBUTED METHOD FOR CASE 1 AND CASE 2

	Iteration		**Objective**		**Objective**	**Distributed**
	CSE	DSE	CSE	DSE	**error**	**objective**
case 1	6	73	11.5568	11.6801	1.0559 %	10.9951
case 2	6	112	11.5568	11.6804	1.0582 %	10.9951

As shown in the table, the factual error between these values is approximately 1 percent. The necessity of considering objective value is due to the fact that one of the methods to specify measurement anomalies, so-called *bad data*, is to compare objective value with the chi-square value [2]. So, considering measurement residuals distributed method matches the centralized to a great extent as well.

The last column of table I is devoted to the DSE objective value, which is slightly different from the centralized objective value. This slight difference is quite apparent, and it is due to the application of the auxiliary variables. In other words, applying auxiliary variables in (6) is the main reason leading to a better objective value. There might be a method to utilize the benefit of applying these auxiliary values to improve SE results further, but it is beyond the scope of the paper.

Fig. 8 shows the result of the experiment to check the gas consumption, amount of gas used to execute a transaction, with respect to the transaction payload size in bytes of different values in a transaction, i.e., in a hexadecimal value and used to check how it will influence the processing time. Different value precision results in different payload sizes. We executed 128 transactions of payload size one and bytes of size k from 1 to 128. In EVM, a one-word is a maximum of 32 bytes. Zero bytes pad each payload up to the closest factor of 32 bytes and processed as a sequence of 32 bytes words. Most of the operation consumption goes to cryptographic signature checks by the nodes. Gas consumption varies with different byte sizes, and we can see a significant shift for each consecutive 32 bytes, but within each set, the gas fees increased linearly with an increment of a byte.

Fig. 9 indicates the optimization of the transfer procedure where several transactions can be concatenated as one string, i.e., bulk data transfer. This would result in less number of transaction to transfer the same amount data without spending extra gas for each execution. For the experiment, we measured the gas consumption to transfer 1024 bytes per 2^{k-1} bytes where $k \in \{1, \ldots, 8\}$, with increase on payload size, the gas consumption reduces for computation at nodes.

V. Conclusion

Blockchain technology has attracted research and industrial communities' attention due to its diverse and novel characteristics. Needless to say that the future power grids, so-called smart grids, can benefit from these features in different industrial divisions. In this regard, we tried to point out blockchain application in smart grids' main sector, i.e., the state estimator. State estimation plays a vital role in regulating system operator decisions such as contingency analysis, electricity market and load forecasting in energy system management.

In this work, we have proposed a combination of distributed state estimation and a blockchain designed communication platform for secure data transmission and increasing the system's reliability. Application of the smart contract concept would lead to improving the security of the overall system. Moreover, the robustness of the method against the data transmission latency has been analysed.

As mentioned before, we introduced a scheme for the combination of state estimation with blockchain in a distributed transmission system. Therefore, implementing such a combination for the distribution system, in which the applications of renewable energy sources are increasing exponentially, can be a future direction. Another research direction for the future can be introducing multi-signature that will make this architecture more secure. Additionally, economical analysis for BC's implementation in the power system would be of interest to research and the industrial community and can be considered as another future direction for this study.

Appendix

Measurement units that have been considered in this study are composed of voltage measurement, real power injection, reactive power injection, real power flow, reactive power flow. In this section physical equations governing the power system are provided.

A. Active and reactive power injection and power flow (inside area k)

$$P_{k,i}(.) = \sum_{i=1}^{n} v_{k,i} v_{k,j} (G_{ij}\cos\theta_{k,ij} + B_{ij}\sin\theta_{k,ij}),$$

$$Q_{k,i}(.) = \sum_{i=1}^{n} v_{k,i} v_{k,j} (G_{ij}\sin\theta_{k,ij} - B_{ij}\cos\theta_{k,ij}),$$

$$P_{k,ij}(.) = v_{k,i} v_{k,j} (G_{ij}\cos\theta_{k,ij} + B_{ij}\sin\theta_{k,ij}) - \; G_{ij} v_{k,i}^2,$$

$$Q_{k,ij}(.) = v_{k,i} v_{k,j} (G_{ij}\sin\theta_{k,ij} - B_{ij}\cos\theta_{k,ij}) + v_{k,i}^2 \left(B_{ij} - \frac{b_{ij}^s}{2} \right),$$

where G_{ij} and B_{ij} is the real and imaginary part of the element in the i^{th} row and j^{th} column of the network admittance matrix, respectively; and $\frac{b_{ij}^s}{2}$ is the shunt suseptance considering the π equivalent mode of the line.

B. Active and reactive power injection and power flow (between area k and area l)

The equations between areas would be the same as inside areas, but the only difference would be the value of state variables. If the state variable is for the neighboring area we should use the auxiliary variables. For example, if the j^{th} bus is for the neighboring area, we should use $\tilde{v}$ and $\tilde{\theta}$.

Acknowledgments

The reported study was funded by RFBR according to the research project № 20-37-90128.

References

[1] A. S. Musleh, G. Yao, and S. Muyeen, "Blockchain applications in smart grid–review and frameworks," *IEEE Access*, vol. 7, pp. 86 746–86 757, 2019.

[2] A. Gomez-Exposito, A. J. Conejo, and C. Canizares, *Electric energy systems: analysis and operation*. CRC press, 2018.

[3] 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.

[4] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151 019–151 064, 2020.

[5] F. C. Schweppe and J. Wildes, "Power system static-state estimation, part i: Exact model," *IEEE Transactions on Power Apparatus and systems*, no. 1, pp. 120–125, 1970.

[6] F. F. Wu, "Power system state estimation: a survey," *International Journal of Electrical Power & Energy Systems*, vol. 12, no. 2, pp. 80–87, 1990.

[7] J. Dopazo, O. Klitin, G. Stagg, and L. Van Slyck, "State calculation of power systems from line flow measurements," *IEEE transactions on power Apparatus and Systems*, no. 7, pp. 1698–1708, 1970.

[8] R. E. Larson, W. F. Tinney, and J. Peschon, "State estimation in power systems part i: Theory and feasibility," *IEEE Transactions on Power Apparatus and Systems*, no. 3, pp. 345–352, 1970.

[9] J. Allemong, L. Radu, and A. Sasson, "A fast and reliable state estimation algorithm for aep's new control center," *IEEE Transactions on Power Apparatus and systems*, no. 4, pp. 933–944, 1982.

[10] t. A. Garcia, A. Monticelli, and P. Abreu, "Fast decoupled state estimation and bad data processing," *IEEE Transactions on Power apparatus and Systems*, no. 5, pp. 1645–1652, 1979.

[11] F. Aschmoneit, N. Peterson, and E. Adrian, "State estimation with equality constraints," in *Tenth PICA Conference Proceedings*, 1977, pp. 427–430.

[12] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[13] M. Irving, R. Owen, and M. Sterling, "Power-system state estimation using linear programming," in *Proceedings of the Institution of Electrical Engineers*, vol. 125, no. 9. IET, 1978, pp. 879–885.

[14] A. J. Conejo, S. de la Torre, and M. Canas, "An optimization approach to multiarea state estimation," *IEEE Transactions on Power Systems*, vol. 22, no. 1, pp. 213–221, 2007.

[15] M. Ayiad, H. Leite, and H. Martins, "State estimation for hybrid vsc based hvdc/ac transmission networks," *Energies*, vol. 13, no. 18, p. 4932, 2020.

[16] M. Pau, F. Ponci, A. Monti, S. Sulis, C. Muscas, and P. A. Pegoraro, "An efficient and accurate solution for distribution system state estimation with multiarea architecture," *IEEE Transactions on Instrumentation and Measurement*, vol. 66, no. 5, pp. 910–919, 2017.

[17] C. Xu and A. Abur, "Robust linear state estimation for large multi-area power grids," in *2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2016, pp. 1–5.

[18] T. Zhang, P. Yuan, Y. Du, W. Zhang, and J. Chen, "Robust distributed state estimation of active distribution networks considering communication failures," *International Journal of Electrical Power & Energy Systems*, vol. 118, p. 105732, 2020.

[19] A. Minot, Y. M. Lu, and N. Li, "A distributed gauss-newton method for power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3804–3815, 2015.

[20] M. Rostami and S. Lotfifard, “Distributed dynamic state estimation of power systems,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3395–3404, 2017.

[21] V. Kekatos and G. B. Giannakis, “Distributed robust power system state estimation,” *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1617–1626, 2012.

[22] S. Asefi, S. Parsegov, and E. Gryazina, “Distributed state estimation: a novel stopping criterion,” *arXiv preprint arXiv:2012.00647*, 2020.

[23] G. N. Korres, “A distributed multiarea state estimation,” *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 73–84, 2010.

[24] W. Jiang, V. Vittal, and G. T. Heydt, “Diakoptic state estimation using phasor measurement units,” *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1580–1589, 2008.

[25] L. Zhao and A. Abur, “Multi area state estimation using synchronized phasor measurements,” *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 611–617, 2005.

[26] D. Marelli, B. Ninness, and M. Fu, “Distributed weighted least-squares estimation for power networks,” *IFAC-PapersOnLine*, vol. 48, no. 28, pp. 562–567, 2015.

[27] S. Boyd, N. Parikh, and E. Chu, *Distributed optimization and statistical learning via the alternating direction method of multipliers*. Now Publishers Inc, 2011.

[28] X. Li and A. Scaglione, “Robust decentralized state estimation and tracking for power systems via network gossiping,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1184–1194, 2013.

[29] L. Xie, D.-H. Choi, S. Kar, and H. V. Poor, “Fully distributed state estimation for wide-area monitoring systems,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1154–1169, 2012.

[30] A. Sharma, S. Srivastava, and S. Chakrabarti, “Multi area state estimation using area slack bus angle adjustment with minimal data exchange,” in *2013 IEEE Power & Energy Society General Meeting*. IEEE, 2013, pp. 1–5.

[31] Y. Guo, L. Tong, W. Wu, H. Sun, and B. Zhang, “Hierarchical multi-area state estimation via sensitivity function exchanges,” *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 442–453, 2016.

[32] A. Minot and N. Li, “A fully distributed state estimation using matrix splitting methods,” in *2015 American Control Conference (ACC)*. IEEE, 2015, pp. 2488–2493.

[33] A. Gómez-Expósito, A. de la Villa Jaén, C. Gómez-Quiles, P. Rousseaux, and T. Van Cutsem, “A taxonomy of multi-area state estimation methods,” *Electric Power Systems Research*, vol. 81, no. 4, pp. 1060–1069, 2011.

[34] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *www.bitcoin.org*, pp. 1–9, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[35] P. Vigna and M. J. Casey, *The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order*. St. Martin’s Press, 2015.

[36] I. Eyal, “Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities,” *Computer*, vol. 50, no. 9, pp. 38–49, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/8048646/

[37] G. W. Peters and E. Panayi, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money,” in *Banking Beyond Banks and Money*. Springer, Cham, 2016, pp. 239–278.

[38] Y. Madhwal and P. Panfilov, “Blockchain And Supply Chain Management: Aircrafts’ Parts’ Business Case,” in *Annals of DAAAM and Proceedings of the International DAAAM Symposium*, 2017, pp. 1051–1056.

[39] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, “TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains,” in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 7 2019, pp. 184–193. [Online]. Available: https://ieeexplore.ieee.org/document/8946187/

[40] N. Alzahrani and N. Bulusu, “Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain,” in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock’18*. New York, New York, USA: ACM Press, 2018, pp. 30–35.

[41] D. Korepanova, S. Kruglik, Y. Madhwal, T. Myaldzin, I. Prokhorov, I. Shiyanov, S. Vorobyov, and Y. Yanovich, “Blockchain-Based Solution to Prevent Postage Stamps Fraud,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 5 2019, pp. 171–175. [Online]. Available: https://ieeexplore.ieee.org/document/8751495/

[42] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, E. Izumchenko, A. Aliper, K. Romantsov, A. Zhebrak, I. O. Ogu, and A. Zhavoronkov, “Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare,” *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, 1 2018. [Online]. Available: http://www.oncotarget.com/fulltext/22345

[43] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and A. Mohaisen, “Exploring the Attack Surface of Blockchain: A Systematic Overview,” 4 2019. [Online]. Available: http://arxiv.org/abs/1904.03487

[44] M. Choe, “LONDONCOIN: THE ULTIMATE CRYPTOCURRENCY.” [Online]. Available: https://coinmarketcap.com/

[45] Buterin and Vitalik, “Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform,” *Etherum*, no. January, pp. 1–36, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[46] “Truffle Suite - Your Ethereum Swiss Army Knife,” 2018. [Online]. Available: http://truffleframework.com/

[47] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, “Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator’s perspective,” *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, 2019.

[48] 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*, vol. 15, no. 5, pp. 840–852, 2016.

[49] M. Pipattanasomporn, M. Kuzlu, and S. Rahman, “A blockchain-based platform for exchange of solar energy: Laboratory-scale implementation,” in *2018 International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE)*. IEEE, 2018, pp. 1–9.

[50] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, “Distributed blockchain-based data protection framework for modern power systems against cyber attacks,” *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2018.

[51] Z. Dong, F. Luo, and G. Liang, “Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems,” *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 5, pp. 958–967, 2018.

[52] A. M. Mohan, N. Meskin, and H. Mehrjerdi, “A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems,” *Energies*, vol. 13, no. 15, p. 3860, 2020.

[53] D. U. Case, “Analysis of the cyber attack on the ukrainian power grid,” *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[54] J. Zhao, M. Netto, Z. Huang, S. Yu, A. Gomez-Exposito, S. Wang, I. Kamwa, S. Akhlaghi, L. Mili, V. Terzija *et al.*, “Roles of dynamic state estimation in power system modeling, monitoring and operation,” *IEEE Transactions on Power Systems*, 2020.

[55] S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” *Journal of Cryptology*, vol. 3, no. 2, pp. 99–111, 1 1991. [Online]. Available: https://link.springer.com/article/10.1007/BF00196791

[56] P. Jones and D. Eastlake, “US Secure Hash Algorithm 1 (SHA1),” September 2001.

[57] S. Gueron, S. Johnson, and J. Walker, “SHA-512/256 ,” 2011.

[58] “NODES AND CLIENTS.” [Online]. Available: https://ethereum.org/en/developers/docs/nodes-and-clients/

[59] “Infura: The foundation for decentralized applications.” [Online]. Available: https://infura.io/

[60] “Alchemy.” [Online]. Available: https://www.alchemyapi.io/

[61] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[62] Q. ShenTu and J. Yu, “A Blind-Mixing Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm,” *arxiv*, 2015.

[63] C. Chen, Y. Chen, K. Zhang, M. Ni, S. Wang, and R. Liang, “System redundancy enhancement of secondary frequency control under latency attacks,” *IEEE Transactions on Smart Grid*, 2020.

[64] “Ganache: ONE CLICK BLOCKCHAIN.” [Online]. Available: https://www.trufflesuite.com/ganache

[65] Y. Madhwal, “code repository,” 2020. [Online]. Available: https://github.com/yashmadhwal/secureDataTransmission

[66] U. Maurer, “Modelling a public-key infrastructure,” pp. 325–350, 1996.

[67] R. Christie, “Power systems test case archive. 14 bus power flow test case, 1993.”

Sajjad Asefi has received his B.Sc. degree at Guilan University, Iran (2015) and his M.Sc. degree at University of Mohaghegh Ardabili, Iran (2018), both in electrical engineering (power systems). Currently, he is a Ph.D. student in center for energy science and technology (CEST) at Skoltech, Moscow, Russia.

His focus of research at Skoltech is on distributed methods for power system optimization. His research interests include application of optimization in bulk power system, blockchain, demand side management, electric vehicles and renewable energy sources, cyber-security and state estimation.

Yash Madhwal is a Ph.D. student at Skolkovo Institue of Science and Technology (Skoltech), specializing in implementing blockchain technology in resolving supply chain problems. Yash has authored multiple scientific papers where he has built prototypes of the blockchain-based decentralized application (DApp), focusing on industrial problems, especially the supply chain. Yash is the Teaching assistant of the course ”Introduction to blockchain” and conducts technical seminars, showing the listeners methods to build blockchain applications. Additionally, he is invited as a guest lecturer to different universities to deliver an introductory lecture on blockchain technology and potential applications.

Yury Yanovich received the Ph.D. degree in probability theory and mathematical statistics from Institute for Information Transmission Problems, Moscow, Russia, in 2017 and Master (honors) and Bachelor (honors) Degrees in Applied Physics and Mathematics in Moscow Institute of Physics and Technology, Moscow, Russia, in 2012 and 2010 respectively.

Currently, he is a Research Scientist at Skolkovo Institute of Science and Technology, Moscow, Russia. Yury is an author of Exonum consensus protocol and is a lecturer of the “Introduction to Blockchain” course at top Russian universities since 2017. His interests include consensus protocols, privacy and security, parachains and applications.

Elena Gryazina received the Ph.D. degree from the Institute for Control Sciences Russian Academy of Sciences. She is currently an Assistant Professor at Skolkovo Institute of Science and Technology, Moscow, Russia.

Her research interests include convex and non-convex optimization with applications to energy systems engineering problems such as optimal power flow, decentralised state estimation, peer-to-peer energy market and energy efficient micro-climate control in buildings.