Power Line Monitoring-based Consensus Algorithm for Performance Enhancement of Energy Blockchain applications in Smart Grid 2.0

Charithri Yapa, *Student Member, IEEE,* Chamitha De Alwis, *Senior Member, IEEE,* Uditha Wijewardhana, *Member, IEEE,* Madhusanka Liyanage, *Senior member, IEEE,* and Janaka Ekanayake *Fellow, IEEE*

***Abstract*—Energy blockchain applications are becoming inevitable with the transformation of electricity distribution networks into the decentralized Smart Grid 2.0 architecture. The scalability of the blockchain platform plays a key role in catering to the increasing number of nodes connected due to consumer-turned-prosumers being integrated into the distribution grid in a distributed manner. Hence, this study aims to optimize blockchain utilization for Smart Grid 2.0 applications through a novel consensus mechanism, which eliminates the requirement for performing additional complex computations to mine a new block. The algorithm utilizes the grid monitoring process through the existing smart meters, and thus has been capable of reducing the energy footprint for block mining to a fraction of that of the legacy Proof-of-Work algorithm, and reducing the block creation time by $\sim< 60\%$. The proposed Power Line Monitoring-based Consensus Mechanism (PLMC) algorithm is validated using the Process Analysis Toolkit (PAT). In addition, data collected while monitoring the network for block mining is utilized for power quality measurement purposes.**

***Index Terms*—Blockchain, Consensus Algorithm, Energy-efficient Consensus Mechanism, Formal Model Verification, Power Quality detection, Process Analysis Toolkit, Smart Contracts**

I. Introduction

THE next generation of smart grids, also known as Smart Grid 2.0 (SG 2.0) improves the capability of integrating renewable energy generation through distributed generation sources such as solar Photo Voltaic (PV) and wind, Peer-to-Peer (P2P) trading between prosumers who have excess self-generated energy with consumers in the neighbourhood, and facilitate the growing market for Electric Vehicles (EVs) and the charging stations, to cater the increasing electricity demand [1]. The popularity of SG 2.0 has led to a rapid increase in the number of renewable energy installations integrating with the network [2]. Furthermore, massive numbers of renewable integration is envisaged, willing to contribute to cater to the demand through their excess generation. This requires strong monitoring and regulatory procedures to minimize the degrading of the power quality delivered to the consumer, with the rapidly increasing number of grid interactions [3]. Ensuring power quality standards in a decentralized grid is challenging without a costly, trusted intermediary node. Monitored power quality data can be used as reputation scores in P2P energy trading, supply-demand management, and energy transfers, influencing selection processes. Reputation-based mechanisms also support dynamic pricing and competitive rewards, crucial with increasing grid interconnections, ensuring fair execution based on delivered power quality [2].

Enhanced communication capabilities for this distributed architecture are enabled through the Internet, which acts as an overlay to the smart grid. The decentralized operation of SG 2.0 is enabled through blockchain, which is one of the widely used Distributed Ledger Technologies (DLTs) [4]. The inherent immutable, transparent, distributed, and pseudonymous nature of this technology has enabled P2P energy trading, microgrid operations, energy data management, and overall control of the SG 2.0 to be regulated autonomously and without the intervention of a third-party [2]. Further, the blockchain platform addresses the challenge of securing data in a decentralized environment, against the increasing number of cyber attacks.

Blockchain's role in future smart grids raises concerns about scalability, defined by transaction throughput and latency. The consensus algorithm used to determine the miner who adds the next block to the sequence has constraints, due to the existing algorithms such as Proof-of-Work and Proof-of-Stake, which involve heavy computations and assessment of previous work. Thus, enhancing scalability involves increasing throughput (transactions per second) while reducing latency; Ethereum 1.0 handles 25 TPS compared to Ethereum 2.0's shift to over 1,000,000 TPS with Proof-of-Stake. This scalability is crucial for managing the increasing transaction volume in smart grid operations. Further, the widely used consensus algorithms are energy-intensive and complex, creating limitations for stakeholders with lower processing capabilities onboard [5].

Hence, a consensus algorithm, which also delivers useful outputs, while selecting the next block makes it more application-oriented and user-friendly. This enables better participation among nodes and improves the fairness of the process. The study introduces a novel consensus algorithm tailored for Smart Grid 2.0's blockchain applications, addressing overlooked optimization aspects like latency, throughput, energy usage in consensus, and computational demands for mining. Further, the block mining process generates data, which can be stored and analysed to detect power quality degradation of the SG 2.0. It identifies a gap in the literature – a lack of

Charithri Yapa and Uditha Wijerwadhana are with University of Sri Jayewardenepura, Gangodawila, Sri Lanka.
E-mail: charithriyapa@sjp.ac.lk, uditha@sjp.ac.lk

Chamitha De Alwis is with the School Of Computer Science And Technology, University of Bedfordshire, United Kingdom.
E-mail: Chamitha.DeAlwis@beds.ac.uk

Madhusanka Liyanage is with the University College, Dublin, Ireland.
E-mail: madhusanka@ucd.ie

Janaka Ekanayake is with University of Peradeniya and School of Engineering, Cardiff University, United Kingdom.
E-mail: ekanayakej@eng.pdn.ac.lk, ekanayakej@cardiff.ac.uk

Manuscript received

focus on optimizing key blockchain parameters for efficient operation in energy markets. By doing so, it contributes to the development of efficient and scalable blockchain-based energy markets, a critical component of future SG2.0. The key contributions of this study are summarized below.

- Propose an application-based, user friendly, and low energy consuming consensus algorithm: Power Line Monitoring-based Consensus (PLMC), which will be utilized in Peer-to-Peer energy markets integrated with blockchain to collect real-time powering monitoring information.
- Integrate the energy monitoring process, which is a primary task of the smart grid with the block mining process to eliminate additional work being performed/ hardware requirements and to reduce the energy footprint.
- Control the block creation time in the block mining process with regular metering functions of the smart grid instead of complex problem-solving mechanisms in legacy consensus mechanisms.
- Propose further a user incentive scheme, in addition to the traditional block mining rewards, to motivate the collection of power quality data. This additional fee will be paid if a power quality violation is detected using the data monitored and stored by the node while mining the block.

The rest of the paper is organized as follows: Section II elaborates on the preliminaries related to Smart Grid 2.0 and blockchain consensus mechanisms while discussing the existing work and the motivation for this study. Section III discusses the stakeholders of the proposed PLMC algorithm and elaborates on the algorithms along with the process flow. Section IV presents the results of the formal verification of the model, developed using the Process Analysis Toolkit (PAT). Section V and VI present the simulation and implementation results obtained from different tests carried out related to PLMC respectively. Finally, Section VII compares the proposed algorithm with the existing work while Section VIII summarizes the overall operation of the novel consensus mechanism.

II. Preliminaries

This section provides an overall understanding on the basic concepts related to power quality of smart grids and blockchain consensus mechanisms, while emphasizing their importance in the context of the envisaged grid architecture.

A. Blockchain

Blockchain organizes blocks containing transactions in chronological order and is shared among nodes for transparency. The applications are widely adopted across finance, healthcare, supply chain, agriculture, energy, and transportation sectors. Each block is linked to the preceding one via a unique hash, ensuring security and immutability by detecting any alterations. Its features enable authority delegation among stakeholders without the need for a third party, leveraging Public Key Infrastructure (PKI) to verify user validity and maintain data privacy through pseudo-identities, without revealing personal information [4], [2].

B. Blockchain consensus mechanism

Consensus, is crucial in blockchain, which involves adding validated blocks upon agreement by all nodes. It relies on a block header containing Merkle tree roots, previous block hashes, and timestamps. Blockchain implementations for Smart Grids utilize the existing, widely adapted consensus mechanisms to assess a miner's contribution to approve and add proposed blocks. These include Proof-of-Work, Proof-of-Stake, Practical Byzantine Fault Tolerance, and Proof-of-Authority [6].

Proof-of-Work (PoW): The winning miner is selected by successfully solving a complex cryptographic puzzle. The miner has to determine the nonce, which will ultimately generate the block hash with the stipulated number of leading zeros, also referred to as the difficulty level [7].

Proof-of-Stake (PoS): The miner possessing the highest cryptographic stake among the peers will be selected to add a new block [5].

Proof-of-Authority (PoAu): A pre-determined validator proposes the next block keeping their identity at stake [6].

Practical Byzantine Fault Tolerance (PBFT): A pre-defined authority proposes the new block, which is accepted by the rest blockchain nodes through a communication process comprising of three phases; pre-prepare, prepare, and commit [6].

Proof-of-Solution (PoSo), Proof-of-Search (PoSe): The complex cryptographic puzzle in PoW is replaced with an optimization problem to eliminate the meaningless computations performed by the miners [8], [9], [10].

C. Limitations of the existing blockchain consensus algorithms

The PoW incorporates a complex cryptographic hashing-based puzzle, for which mining nodes are required to possess the computational capabilities to perform these additional tasks [7]. This is experienced to be costly as well as energy intensive. In contrast, algorithms such as PoS, PoAu, and PBFT pledge their stake or reputation obtained through past mining instances to secure the opportunity to create the next block. In such an instance, the stake/reputation is earned by initiating from the PoW. Further, PoAu and PBFT rely on a single validator/authorizer in the consensus process, which contradicts the delegation that is envisaged [6].

D. Power quality of Smart Grid 2.0

The main concern of smart grid operations is the impact on the power quality delivered to the consumer. The presence of switching devices and the intermittent nature of renewable generation, which is the predominant source in smart grids have raised negative consequences on the power quality. Consumers experience malfunctioning of their equipment and loss of reliability of the power supply are observed as consequences of degraded power quality [3].

Continuous monitoring of the smart grid to identify the degradation of the power quality due to high penetration of renewable generation makes it possible to deploy measures and restore the desired conditions. This enables a power supply with a clean waveform at all ends of the power network. Network monitoring to improve power quality standards, as well as adherence to the desirable limits, could both be rewarded to encourage both prosumer and consumer participation.

E. Related Work

Currently implemented blockchain-based solutions for P2P energy trading markets are focused on achieving decentralized operations with the luxury of trust, integrity, security, anonymity, and being free of third-party influence. Hence, they mostly adopt blockchain platforms, which originated from the finance domain.

Real-world blockchain-integrated P2P markets include the very first implementation, the Brooklyn microgrid where energy transfers occur within a confined neighbourhood [11]. Later this concept was extended to many other implementations, facilitating the trading of excess solar energy generation [12] in a broader geographical area. All these have been implemented based on legacy blockchain platforms, which incorporate the PoW and PoS consensus mechanisms. This has created issues due to high latency leading to low throughput, hence scalability concerns. In addition, the energy footprint of the PoW consensus algorithms is proven to be high. Apart from PoW, PoS is gaining attention due to its considerably lower energy consumption. Ethereum, a widely used platform for energy blockchain applications is also switching to PoS from PoW [5]. However, PoS requires previously accumulated stake in terms of crypto, earned through mining rewards for performing a given task, which mostly incorporates complex puzzle solving such as PoW. A modified version of PoS is proposed by Solarcoin [13], where the stake is earned by every MWh of solar energy produced by the stakeholder, which is identified as a sustainable and fair initiative.

As a solution for having to solve a complex computational task to reach consensus in PoW mechanism, several studies have proposed alternative algorithms to eliminate the additional work performed by the miners. Studies presented in [10], [9] propose Proof-of-Solution (PoSo) consensus algorithm, focusing on energy blockchain applications, where the mathematical puzzle has been replaced with an optimization problem in energy trading or an energy dispatch problem, respectively. The former proposes a novel algorithm for P2P energy trading, which is capable of maximizing social welfare in a decentralized manner while considering physical network constraints. A similar PoSo algorithm is proposed in [14], which aims at replacing the additional task with a useful work such as training a machine learning model and utilizing the submitted model updates as Work Stake tokens to be used in PoS consensus mechanism. Furthermore, the Proof-of-Search (PoS) consensus algorithm has been proposed by several studies including [8] and [15], where the mathematical puzzle involved with PoW is replaced with an optimization problem offered by a client, and the winning miner is selected based on the optimal solution provided by the nodes. A reputation-based algorithm, named Proof-of-Energy (PoE) is proposed in [16], which is a simplified version of PoS to select the validator based on the best self-consumption patterns. A Consumption-Production Function (CPF) determines the number of units produced by renewable generation and the amount consumed, including those from energy storage. The validator of the next block will be the prosumer who is capable of producing all the energy units that he consumes, through a renewable source. This, however, has not addressed the issue of centralized operation as a malicious validator can jeopardize the system. Comparing the proposed algorithms with the legacy PoW counterpart, it can be observed that the additional work required has been replaced with a useful output. However, solving an optimization problem efficiently will require additional hardware components that can be identified as a limitation of the above proposed algorithms.

Moreover, a study conducted in [6] compares the block creation time of three existing, widely used consensus algorithms in P2P energy trading through a double auction mechanism. The comparison is made between PoW, PoAu, and PBFT algorithms. Further, the total auction time is calculated for a double-auction transaction using each of the consensus mechanisms for blockchain recording. The study revealed that PoAu results in the least block creation time. However, both PoAu and PBFT algorithms rely on a centralized authority /validator, which hinders the third-party-free operation expected from the envisaged smart grids.

The requirement of power quality monitoring is emphasized in the study presented in [3], where it investigates the impact of solar Photovoltaic (PV) integration on the voltage profile of the distribution line and derives a generalized approach to model the voltage variations across the line. This highlights the requirement of continuous monitoring of the envisaged SG 2.0 network integrating numerous solar PV connections, hence an ideal application to be utilized in designing a novel consensus algorithm for energy blockchain. To address the identified drawbacks, this study hence, focuses on designing a consensus mechanism, which can be deployed using existing network hardware components, while delivering a useful output for the grid operations.

III. The proposed Power Line Monitoring-based Consensus (PLMC) Algorithm

An overview of the system architecture and the related process sequence is elaborated in the following sections.

A. System Architecture

This section presents the stakeholders of the proposed algorithm, the deployment of blockchain nodes, and the process related to reaching a consensus upon a proposed block.

1) Stakeholders

The stakeholders involved in the proposed block mining process include smart meters owned by prosumers and consumers connected to the distribution network and non-smart grid IoT sensors used for measuring, which are geographically dispersed. Prosumers engage in trading their excess generation with consumers in the neighbourhood. The non-smart grid sensors are independent nodes of the network and their functionality is restricted to obtaining measurement data from the SG 2.0 and analyzing them. However, unlike in the conventional Smart Grid, the Distribution System Operator doesn't own the meters, enabling heterogeneity and preventing 51% attacks due to the monopoly in the ownership of electrical assets. The high-level view of the stakeholders is given in Fig. 1.

2) Deployment of blockchain nodes

The smart meters and the IoT sensors utilized for monitoring purposes should have a notch filter installed, which can extract

information from high frequency signals captured. Since most of the smart meters/sensors available in the market can be easily modified to integrate the filtering facility, the proposed monitoring system can be implemented as a public blockchain. Prosumer and consumer smart meters that have less computational capabilities will be serving as half nodes, which are restricted to the mining operation and cannot participate in key generation and distribution. Meanwhile, the non-smart grid IoT sensor nodes with high processing power will serve as full nodes and have the capability of generating the key as well as participating in the mining process.

3) Power line monitoring to deploy the consensus mechanism

Smart meters/ IoT sensors continuously obtain voltage and current measurements from the electricity grid and the collected data is stored in an offchain platform such as Inter-Planetary File System (IPFS) to reduce the space requirement of the blockchain. This regular grid operation is utilized to implement a blockchain consensus mechanism in the proposed study.

4) Reaching consensus using PLMC algorithm

During a session, a selected full node transmits a secret message modulated onto the carrier of a known frequency. The node to transmit the secret is randomly selected executing an algorithm, on a smart contract. This eliminates the bias associated with the physical distance of the receiving node from the transmitter and ensures decentralization with security. The carrier frequency is selected from the range that is utilized for Narrow-Band Power Line Communication (NB-PLC). This minimizes the interference with the normal grid operations by distorting the power frequency waveform, which is proven by applications in Power Line Communication (PLC). Further, the use of a known frequency enables the smart meters to be pre-configured to filter out the high-frequency component at the entry point of the consumer installation. Moreover, it is assumed that harmonic limiters are installed at the boundaries of the smart grid, to prevent from these high-frequency signals being propagated into the rest of the electricity grid.

A session is initiated between the creation of two consecutive blocks, where mining nodes are expected to perform a precise measuring process of voltage and current to capture the transmitted secret, acting as the key for this session. Upon verifying the creation of a new block, the session expires and a randomly selected node transmits a new secret, during the next session key. Simultaneously, the transmitter broadcasts the hash of the secret as an encrypted message using an existing network (5G and beyond) for verification purposes.

Miners monitor the smart grid to capture the transmitted secret while retrieving the encrypted message through a known communication channel. The first miner, who successfully reveals the session key (secret) that can decrypt the broadcasted message will propose the next block. The rest of the miners will try to verify the winner by using a copy of the encrypted message, captured by themselves. The process of adding the next block earns a reward to the winning miner.

B. Process sequence of the PLMC algorithm

The proposed PLMC algorithm comprises four phases in the process of reaching a consensus. This includes the transmission of the secret, capturing, block generation, and validation. Fig. 1 represents a high-level deployment view of the proposed architecture.

1) Broadcasting the secret

A randomly generated number is used as a session key, which is then modulated onto the power line carrier and transmitted across the network. Further, the encrypted message, which is the hash of the secret used for the verification purpose is broadcasted through a known channel such as 5G. This process is deployed according to pseudo-code given in Algorithm 1.

Algorithm 1 Transmitting Information

```
Generate a random number as the secret to be used as the session key.
Calculate H ← hash of the secret
Encrypt H with the session key to generate the encrypted message for verification.
for t = T_0 to t = T_0 + T ← session time do
    Transmit the secret modulated to a carrier signal of a pre-defined frequency.
    Broadcast the encrypted message through a known channel.
    if Block != verified then
        Re-transmit the secret with an interval of ΔT between two transmissions.
    end if
end for
```

2) Recovering the secret

A miner will capture the secret by monitoring the power line using a smart meter or an IoT sensor. The observed signal will be demodulated and processed to extract the secret. Miners will continuously monitor the power line until they capture the secret accurately. A reward is offered for mining the next block in the blockchain, which encourages miners to monitor the power network through the hardware available to them. The monitored data is stored in an external database such as the IPFS and the hash of it is added as a pointer to the block that is generated. This data can be retrieved by the blockchain from the off-chain database, when necessary.

3) Block generation

The winning miner creates the next block to be added to the blockchain by including the smart grid energy trading data and a pointer to the hash of the monitored data. The block header contains the version, timestamp, hash of the session key, H (SECRET), hashes of the previous block, and the Merkle root. Further, the winning miner broadcasts the retrieved session key and the message H, digitally signed with his private key, among other miners of the network, for verification purposes. The structure of the block is given in Fig. 1.

4) Verification

Once the winning node proposes a new block, the verification phase is initiated. All other miners in the network will perform the authentication of the signature, to verify the sender. Next, they retrieve the encrypted message using the shared session key. This enables them to compare the hash of the session key with the decrypted message to verify the solution. This allows the winning node to claim victory by retrieving the correct session key. The process flow of verifying the winning node is given as a pseudo-code in Algorithm 2.

5) Adding the new block to the blockchain

Upon verification, the winning miner will add the proposed block to the blockchain.

6) Database for power quality data

Besides recovering the secret, smart meters collect a significant amount of measurements in the process. Measurement data is

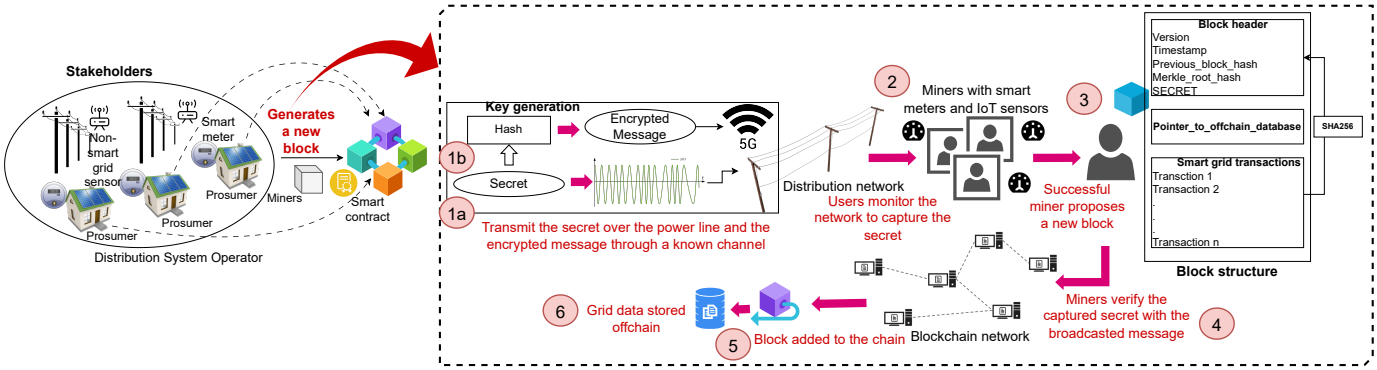


Fig. 1: High-level overview of the proposed consensus algorithm

Algorithm 2 Verification

Input: Digitally signed session key, signature
Output: Key is verified or key is not verified
1: ECDSA signature verification.
2: $H' \leftarrow$ hash of the session key shared by the winner node.
3: Obtain $H \leftarrow$ by decrypting the message using the session key.
4: **if** $H' == H$ **then**
5: Key is verified.
6: **else**
7: Key is not verified.
8: **end if**

stored locally by each node until the next block is created. Following the selection of a winner, the node adds a pointer to these data in the generated block. Off-chain platforms (e.g., IPFS) are utilized to avoid excessive growth of the main chain. Further, the miner can obtain an additional reward if power quality violations are detected based on their measured data. Further, the stored data can be analysed to identify the consumption/production patterns of the prosumer and assign a reputation score based on the behaviour. A multi-factor reputation scoring scheme is essential to enhance trust in a decentralized architecture of SG 2.0 with minimal centralized authority [17].

C. Increasing Mining Difficulty

Every consensus algorithm should have a mechanism to vary the block generation time, also referred to as the difficulty [7]. In the case of PLMC, the difficulty is determined through how easily the secret can be retrieved from the power network. This is affected mainly by the characteristics of the shared secret, transmission channel, and transmitter and receiver. The impact of some selected factors are given in Table I and further analysed in Section V.

The propagation channel, which is the power line distorts the signal with additive noise and increases the difficulty level. The studies given in [18], [19], [20] have identified the best mathematical models to represent the additive noise in power line communication. Even though, noise is commonly simulated using the Additive White Gaussian Noise (AWGN) model, the above studies have shown that its accuracy is less in the context of power line communication. Therefore, the noise is best represented using Bernoulli-Gaussian, Middleton Class A, and Poisson-Gaussian models. The effects of each noise variant are elaborated in Section V. The technique used to modulate the secret to a carrier signal plays a vital role in the recovery probability of the secret at the receiving end. Studies focusing on power line communication have indicated that Phase Shift Key (PSK) techniques perform well over Amplitude Shift Key (ASK) and Frequency Shift Key (FSK) modulation. Thus, this study has evaluated the impact of Binary Phase Shift Key (BPSK) and Quadrature Phase Shift Key (QPSK), which are the widely adopted PSK modulation techniques in power line communication [18].

TABLE I: Impact of factors upon the difficulty of retrieving the secret

Factor		Effect
Secret	Length ↑	Increase
	Sharing Frequency ↑	Decrease
Channel	Noise ↑	Increase
	Attenuation ↑	Increase
	Fading ↑	Increase
Transmitter/Receiver	Modulation	PSK - Increase, ASK, FSK - Decrease
	Coupling loss ↑	Increase
	Error correction ↑	Decrease

IV. Formal Verification of the Proposed Consensus Algorithm

The process flow of the proposed PLMC algorithm can be illustrated in a state transition diagram as shown in Fig. 2.

Formal methods were used to ensure accuracy and verify the model of the proposed consensus mechanism. Among the available model-checking tools, the Process Analysis Toolkit (PAT) is an efficient technique, which models the process flows of the system in terms of state transitions [21]. PAT develops the system model using a sub-language of Communicating Sequential Processes (CSP), CSP#, which allows importing C# libraries to simulate customized data structures and a variety of user-defined functions. It allows the modelling of multiple, complex processes simultaneously and the pro-

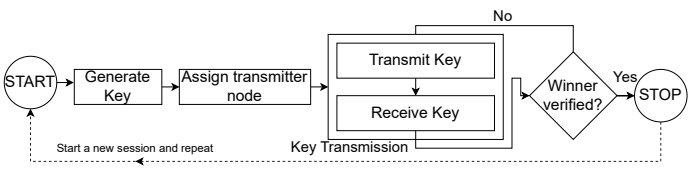


Fig. 2: State sequence of the proposed consensus mechanism

gramme generates a state transition diagram by analysing all possible changes of states. Further, it is capable of verifying the reachability of pre-defined conditions. This is achieved by the automatic transition between states and interleaving the logic conditions defined by the user [22].

A. Formal model

The states of the process illustrated in Fig. 2 are modelled using user defined functions written in CSP#, simulating a blockchain network with N mining nodes. At the beginning of each session, a new key is generated using the $GenerateKey()$ function. A node is selected as the transmitter for the session key using the $AgssinKey()$ phase. The states of repeated key transmission and receiving of the key by N-1 nodes are modelled through the $KeyTransmission()$ state, where channels between each and every node in the network are pre-defined. This process is run concurrently until a winner has been selected. These user-defined functions are modelled with the integration of C# libraries, as CSP# language only supports basic functionalities. The state transition is defined by the following equation.

PLMC() = GenerateKey(); AssignKey(); KeyTransmission(); KeyTransmission() = (||x:{1..(N-1)}@((TransmitKey(x)|| ReceiveKey(x) || IncrementCycle(x)))); KeyTransmission();

In CSP#, process A running in parallel with process B is denoted by $A||B$.

B. Formal verification

The developed PAT model is then validated against a predefined set of properties as given below. The number of nodes is set as $N = 6$ and the secret length as 6 bits. The proposed consensus protocol is verified against three critical properties, which include the ability to reach consensus, fork probability, and the deadlock-free condition. Further, each of the above conditions is validated for the operation of the blockchain with malicious nodes. Therefore, the security aspect of the proposed blockchain consensus mechanism can be evaluated using the PAT model checker. For this study, we have selected four scenarios where the number of malicious nodes present in the blockchain is varied. These are defined in the PAT model respectively as, I) With no malicious miners, II) With minority malicious miners, III) With 50% malicious miners, and IV) With majority malicious miners.

1) Reaching consensus

The property of every miner node agreeing on the same block to be added to the blockchain is verified by defining how the winner is selected based on the capturing of the secret. Assertions (A1, A2, A3, A4) are defined for the selected four scenarios to verify the reach of consensus condition.

2) Fork probability

In the real working scenario, the longest chain, which has earned the most trust will be selected as the legitimate version and all the participating nodes update their ledgers, accordingly. To ensure that in the proposed consensus algorithm the forking probability is minimized, user-defined conditions (A5, A6, A7, A8) were verified, which ensure that all nodes have reported the same proposed block in their version of the blockchain.

3) Deadlock-freeness

PAT model checker facilitates checking of the system behaviour where the execution of the next step depends on the activity of a certain node in the network, hence a deadlock occurs. The proposed consensus mechanism was validated for the deadlock-free property of it, defined through assertions (A9, A10, A11, A12).

The results obtained from the test carried out are summarized in Table II.

According to the results obtained, the following conclusions could be made regarding the proposed consensus mechanism.

A1-A4: The system reaches a consensus, regardless of the presence of the malicious nodes. This is mainly due to the independent operation of the miner nodes during the process. However, it is preferred to have less malicious nodes present in the network.

A5-A8: The model does not exhibit blockchain fork under all four scenarios.

A9-A12: Model does not result in a deadlock situation irrespective of the operation of the malicious nodes.

V. Simulation Results

Simulation models were developed to evaluate how 1) length of the secret, 2) channel noise and 3) the modulation technique used to transmit the secret across the power line affect the recovery probability of the secret, which determines the difficulty level of the consensus algorithm. Further, the developed model is utilized to calculate the end-to-end delay associated with the proposed consensus mechanism. The following sections explain the details of the simulation setup developed and the analysis of the obtained results.

A. Assessing the difficulty of revealing the shared secret

The simulation model was developed using MATLAB, to replicate PLC using the Orthogonal Frequency-Division Multiplexing (OFDM) technique. OFDM is one of the Spread Spectrum Techniques (SST) that can be used to minimize the Inter-Symbol Interference (ISS) caused by multi-path fading, which is commonly observed in PLC [18]. OFDM spreads a narrow band signal across a wide spectrum and the developed simulation model utilizes 64 sub carriers. Out of these 64, 48 are used for data transmission and the remaining channels are used as guard bands and pilot sub carriers. Each subcarrier waveform is modulated using BPSK or QPSK scheme. BPSK and QPSK are the widely used modulation techniques in the context of PLC, thus adopted in this study to analyze the impact of the channel characteristics on the difficulty of retrieving the secret. The high-level overview of the simulation setup is given in Fig. 3.

The developed model analyzes the impact of the 1) length of the secret, 2) channel noise, and 3) modulation scheme

TABLE II: Results for verification of security and trust properties using PAT model checker

Assertion	Consensus	No fork	Deadlock-free
No_malicious_miners	A1:Yes	A5:Yes	A9:Yes
Minority_malicious_miners	A2:Yes	A6:Yes	A10:Yes
Half_malicious_miners	A3:Yes	A7:Yes	A11:Yes
Majority_malicious_miners	A4:Yes	A8:Yes	A12:Yes

used, on the probability of retrieving the secret. Simulations were performed for 1000 random key transmission-receiving scenarios and the key recovery probability is obtained for the energy per bit to noise power spectral density ratio ($\frac{E_b}{N_0}$) varied from 0 to 25, and the average results are shown in Fig. 4.

1) Impact of the length of the shared secret

As the length of the secret (L) increases, it was observed that the probability of key recovery reduces. Since more bits have to be captured while monitoring the power line to reconstruct the secret, the key recovery probability is observed to be reducing.

2) Impact of channel noise

Previous studies on PLC have analysed the interference of noise on the data transmission, which has identified two components namely, background noise and impulse noise [18]. The former is considered to remain stationary for a longer period while the latter has a time-varying nature. Background noise is widely represented using a Gaussian model while the impulse noise exhibits a non-Gaussian nature. The cumulative impact of noise on the symbols transmitted through OFDM is approximated as given in Eq. 1.

$$S_k = s_k \times h_k + nG_k + nI_k \quad k = 0, 1, 2, ...N-1 \tag{1}$$

where, S_k represents the noise added OFDM symbol s_k, while nG_k, nI_k denote the background noise and impulse noise, respectively. The former is represented using a Gaussian form and the latter is modelled as described in the section followed.

Several statistical models have been derived to represent the interference of impulse noise and this study utilizes three widely used models. They are namely, Bernoulli-Gaussian, Middleton Class A, and Poisson-Gaussian models, which describe the noise in a more realistic way in OFDM-based power line communication systems.

Below given are the Probability Density Functions (PDFs) of each statistical model used for this analysis.

The sequence of the Bernoulli-Gaussian (BG) model, for $\alpha > 1$ comprises independent and identically distributed random variables with a Probability Density Function (PDF) given by Eq. 2 [19].

$$P(v_i) = U_i w_i + \alpha(1 - U_i)w_i \tag{2}$$

in which, U_i is the Bernoulli random variable with $P(U_i = 1) = p$ and W_i is the Gaussian variable with zero mean and variance σ^2.

The Middleton Class-A noise model is defined by the PDF given by Eq. 3 [20].

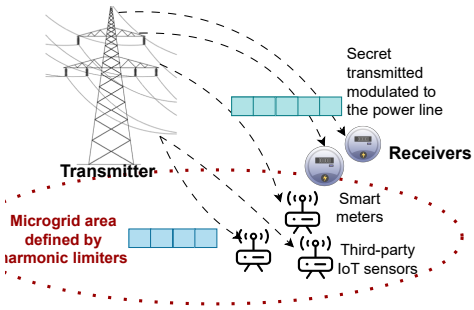


Fig. 3: Simulation setup

$$P(v_i) = \sum_{m=0}^{\infty} \frac{A^m e^{-A}}{m!} N(v_i, 0, \sigma_m^2) \tag{3}$$

where, A represents the impulse index, m being the impulse number and $N(v_i, 0, \sigma_m^2)$ is the Gaussian noise with 0 mean and σ_m^2 variance. $\sigma_m^2 = \sigma_I^2 \frac{m}{A} + \sigma_g^2$, in which σ_I^2 and σ_g^2 defines the variances in impulse and Gaussian noise, respectively.

In the Poisson-Gaussian noise model the amplitude is represented using the Gaussian PDF with 0 mean and σ_g^2 variance with the arrival of the impulses being modelled according to the Poisson distribution as in Eq 4 [18].

$$P(m) = e^{-\lambda} \frac{\lambda^m}{m!} \tag{4}$$

According to the obtained results, a higher secret recovery rate is observed under Poisson-Gaussian channel conditions.

3) Impact of the modulation scheme

The BPSK modulation scheme encodes a single bit per symbol while QPSK achieves this in two bits. Hence, QPSK transmits twice the data rate for a given bandwidth, compared to BPSK and this leads to a higher recovery probability of the transmitted signal at the receiver end.

B. End-to-end delay

Time accumulated for transmission and receiving of the secret through power line monitoring, block generation, and verification of the winner is considered as the end-to-end delay of the proposed consensus algorithm.

OFDM-based QPSK symbol transmission interfered with Poisson-Gaussian noise is used to capture the power line characteristics. The OFDM symbol duration is set as $2240\,\mu s$ following the standards PRIME, G3-PLC, IEEE 1901.2, and ITU-T G.hnem, which govern Narrow-Band power line communication. The secret is re-transmitted every $200ms$ to ensure that a miner with a smart meter or an IoT sensor is capable of capturing the secret within the block generation time. The process of adding generating the new block and the verification of that by the rest of the miners was modeled using Java on Eclipse IDE. Fig. 5 illustrates the variations in the delay for 25 iterations, for ($\frac{E_b}{N_0}$) of 0, 2dB, 4dB, and 8dB.

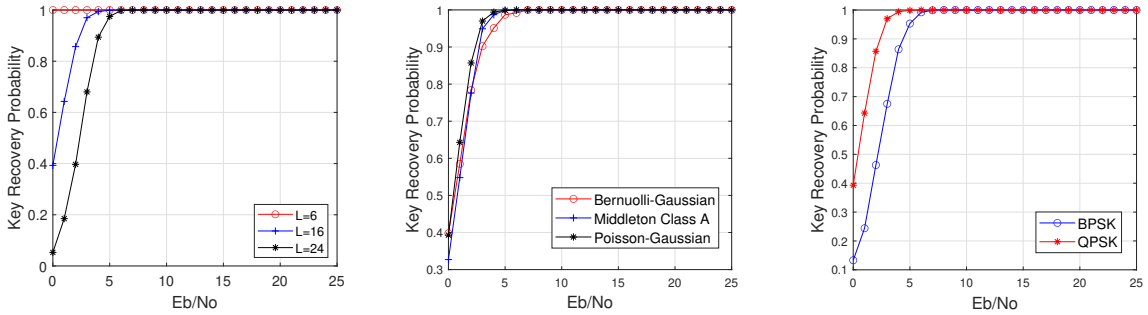
The lowest average end-to-end delay is observed to be 0.1s when the ($\frac{E_b}{N_0}$) is 8 dB, which indicates less noise in the channel.

VI. Implementation Results

A comparison of the proposed PLMC with the currently utilized algorithms is given in the below sections, to evaluate the former's performance concerning energy usage and block sealing time.

A. Comparison of the energy usage

Proof-of-Work is considered to be one of the most energy-intensive consensus mechanisms as it involves intense usage of resources to solve a complex problem within the shortest possible time. As the difficulty level increases, solving the puzzle becomes challenging and the miners tend to pool their resources to achieve better computational capabilities. Proposed PLMC however, utilizes the power line monitoring process for the consensus mechanism, where the secret is captured while receiving measurements through the smart meter. Hence, the proposed mechanism incorporates a less complex hashing function, while creating the next block. The



(a) Key length (b) Channel noise (c) Modulation technique

Fig. 4: Variation of the key recovery probability with channel and key characteristics

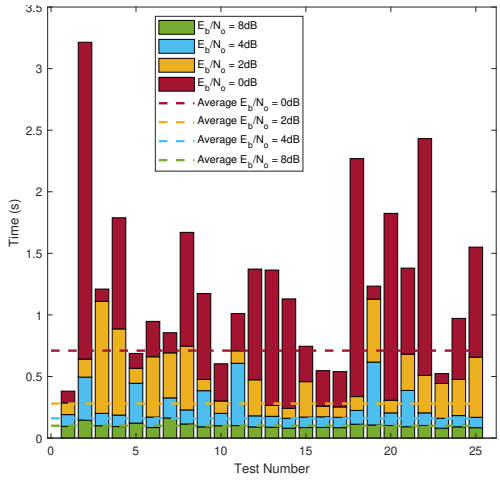


Fig. 5: End-to-end delay for varying $\frac{E_b}{N_0}$

latter approach is less energy intensive in terms of computation since, it obtains the hash of the parameters of the block header, including the version, timestamp, previous block hash, and the Merkle root hash.

The energy consumption during the hash computation is measured through JoularJX, which is a Java-based tool facilitating power monitoring at source code level [23]. This tool is used to measure the energy consumed to calculate the hash by a single node in the block generation process, for both PoW and proposed PLMC.

For comparison, the difficulty level of the PoW algorithm is selected to be six leading zeros in a 32-bit nonce, while the PLMC transmits a six-bit secret. Both the consensus algorithms use SHA-256 as the hashing function. Results of the energy measurements obtained from the simulation are given in Table III.

Since the PoW algorithm has to run multiple, recursive calculations until the target number of leading zeros is achieved, it exhibits a higher energy consumption for the execution of the operations. PLMC, in contracts, consumes less energy as it directly calculates the hash of the block, with the captured secret.

TABLE III: Comparison of energy consumption

Consensus algorithm	Energy consumption (J)
Proof-of-Work	1584
Proof-of-Stake	29.8
PLMC	0.18

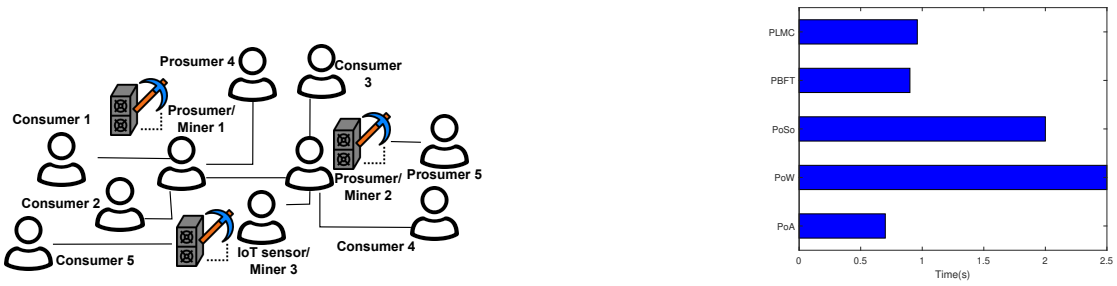
B. Comparison between the block creation time

This section aims at emulating a study conducted in [6] to compare consensus algorithms used by different blockchain architectures in the context of P2P energy trading with a double auction mechanism. The study has selected three widely used consensus mechanisms, namely PoW, PoAu, and PBFT, and aims to find the most scalable and efficient algorithm.

Among the criteria investigated, Block Sealing Time (BST) is a critical parameter, which is the time taken to commit a new block to the blockchain. A setup with 10 nodes (prosumers and consumers) has been utilized for the analysis in [6]. We emulated this setup to incorporate the proposed PLMC consensus algorithm as given in Fig. 6a and measured the time taken to commit a block to the blockchain.

For comparison, tests were performed on a machine equipped with a 2.9 GHz CPU, 16 GB of RAM, and Ubuntu 18.04 LTS operating on a virtual machine [6]. To emulate the study in [6], the network comprises 10 nodes, out of which 3 are miners and the remainder are prosumers/consumers. It is assumed that every miner will be transmitting a part of the secret and each miner has to capture all these components to complete the task. Hence, this incorporates a waiting time of $200ms$ for each node, which is the time between two adjacent transmissions. Apart from this, the time taken for capturing the secrets, block generation, and verification time delays are also included in the BST of the proposed algorithm. The BST has averaged over 100 test simulations and the results are plotted in Fig. 6b against those given in [6] for comparison. Further, the block sealing time of PLMC is compared against that of Proof-of-Solution (PoSo) by using the test results presented in [24]. The study proposes to direct the computations made to create blocks to optimization algorithms.

From the obtained results it is evident that PoW associates the highest BST as the time taken to calculate the correct nonce cannot be predicted. PoSo, which is an optimized version of PoW has been capable of reducing the block creation time significantly compared to its legacy counterpart. However, solving as optimization problem is an additional computation task, which requires dedicated hardware and software infrastructure.



(a) Experimental setup

(b) Block sealing time for a network of 10 nodes

Fig. 6: Experimental validation of proposed consensus mechanism (PLMC)

TABLE IV: Comparison with existing work

Feature	PoW [11]	PoS[13]	PoSo[10]	PoSe[9]	PBFT[8]	PoE[16]	*Ours*
P2P trading applications	✓	✓	✓	✓	✓	✓	✓
Usable work performed	✗	✗	✓	✓	✗	-	✓
Consensus deployed using available hardware	✗	-	✗	✗	-	✓	✓
Lesser computation involved	✗	-	✗	✗	✗	✗	✓
Supports Power quality monitoring	✗	✗	✓	✓	✗	✗	✓
Low energy footprint	✗	✓	✗	✗	✗	✗	✓
Easily customized to vary the difficulty level	✗	✗	✗	✗	✗	✗	✓
Does not rely on a validator selected	✓	✗	-	-	✗	✗	✓

PoAu and PBFT consensus mechanisms exhibit slightly less BST compared to the proposed algorithm. However, the former two involve a centralized entity for the execution of the consensus mechanism thus, conflicts with the primary objective of achieving a decentralized smart grid architecture. Therefore, the proposed PLMC offers better advantages over existing algorithms in terms of block creation time while preserving the decentralized operation structure.

VII. Discussion

This section presents a concise comparison between the existing consensus mechanisms utilized in energy blockchain applications and the proposed, in terms of their features and performance.

A. Feature comparison of existing work in blockchain consensus for energy applications

Table IV summarizes the features of the existing proposals/implementations and illustrates a comparison with the proposed work.

However, the security consideration of the proposed PLMC algorithm has not been extensively analysed in this study as the main focus is on performance optimization. Creation of a consortium by the mining nodes may pose security vulnerabilities, as the smart grid increases in its scale. Further, connecting large number of heterogeneous metering devices, owned by the user might lead to meter tampering, Denial of Service attack and generative-AI based attacks. Enhancing the security of the proposed consensus algorithm is to be explored as a future extension of the work carried out in this study.

B. Assessing the performance against existing consensus mechanisms

Measuring the performance of blockchain involves assessing key metrics: latency, transaction throughput, security bound, and communication complexity. These metrics are influenced significantly by the consensus mechanism utilized. Table V includes a breakdown of the different consensus mechanisms and their performance based on the total number of nodes (N) and the number of malicious nodes (f) present in the network.

1) Latency

PBFT exhibits a high latency due to its communication process between all nodes participating in the consensus at the pre-prepare, prepare and commit stages. Meanwhile, PoW and its variants PoSo, PoSe exhibit a high latency due to the puzzle-solving involved in the consensus process. The proposed PLMC exhibits a low latency as it incorporates the power line monitoring process, which aligns with the regular operation of the miners and does not associate an additional work.

2) Transaction throughput

Transaction throughput refers to the rate at which transactions are processed within a system, typically measured as the number of transactions processed per second (TPS). Due to its complex hash puzzles, PoW, PoSo and PoSe have limited transaction throughput. The voting-based consensus mechanisms including PoAu and PBFT exhibit a high transaction throughput. Meanwhile, the proposed PLMC mechanism, which utilizes power line monitoring, is less computationally demanding compared to PoW. However, the verification might take some time hence, can be identified as a low-to-medium transaction throughput.

3) Security Bound

The security threshold of a consensus mechanism is determined by the maximum number of faulty nodes it can tolerate. PoW and its variants observes a security bound of $2f + 1$, indicating it is susceptible to 51% attacks. PBFT allows $1/3$ of the nodes to be faulty, hence security bound is calculated as $3f + 1$. The proposed PLMC has a security bound similar to PoW, which is $2f + 1$.

4) Communication Complexity

This refers to the number of communications being executed between the transmitter and receiver. PoW and the variants

TABLE V: Comparative analysis of performance among widely used consensus mechanisms

Consensus Mechanism	Latency	Transaction throughput	Security bound	Communication complexity
PoW	High	Low	$2f+1$	$2N$
PBFT	High	High	$3f+1$	$2N^2+N$
PoSo [25], [26]	High	High	$3f+1$	$2N^2+N$
PoSe [25], [26]	High	High	$3f+1$	$2N^2+N$
Ours(PLMC)	Low	LowMedium	$2f+1$	$2N$

require N number of communications to broadcast the client request to miner nodes and another N to communicate the winning miner for verification by others. PBFT requires communication among each node in pre-prepare, prepare and commit, hence accounts for $2N^2+N$. The proposed PLMC has a communication complexity similar to PoW, with a total of $2N$ broadcasts for client requests and verifying the winner miner.

VIII. Conclusion

This study aims to develop a dedicated consensus mechanism for blockchain-integrated smart grid applications to overcome the drawbacks of the legacy systems. The PLMC utilizes the integrated function of continuous grid monitoring through smart devices to develop the consensus protocol, eliminating the resource requirement for additional work performed in the existing alternatives. Moreover, its energy footprint is observed to be a fraction of the exhaustive PoW consensus protocol. Further, the proposed solution has the capability of adding a new block to the sequence within the same time frame as in PoAu and PBFT, while reducing 60% of the computation time of PoW. PLMC is a prospective candidate for energy blockchain applications as it is difficult to capture the secret but easy to verify, which will facilitate the expanding operations of the future smart grids.

Acknowledgment

This work has been partially supported by the Science Foundation Ireland under CONNECT phase 2 (Grant no. 13/RC/2077_P2) project and Science and Technology Human Resource Development Project, Ministry of Higher Education, Sri Lanka, funded by the Asian Development Bank (Grant No. R3/SJ/14).

References

[1] "Chapter 9 - roadmap from smart grid to internet of energy concept," in *From Smart Grid to Internet of Energy*, E. Kabalci and Y. Kabalci, Eds. Academic Press, 2019, pp. 335–349.

[2] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for Future Smart Grid: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 18–43, 2021.

[3] D. Almeida, S. Abeysinghe, M. P. Ekanayake, R. I. Godaliyadda, J. Ekanayake, and J. Pasupuleti, "Generalized Approach to Assess and Characterise the Impact of Solar PV on LV Networks," *International Journal of Electrical Power & Energy Systems*, vol. 121, p. 106058, 2020.

[4] "Survey on Blockchain for Future Smart grids: Technical Aspects, Applications, Integration Challenges and Future Research," *Energy Reports*, vol. 7, pp. 6530–6564, 2021.

[5] Ethereum.org, "Proof-of-Stake (PoS)," 2023, accessed on March, 14 2023. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[6] T. Machacek, M. Biswal, and S. Misra, "Proof of X: Experimental Insights on Blockchain Consensus Algorithms in Energy Markets," in *2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2021, pp. 1–5.

[7] S. Nakamoto, "Bitcoin Whitepaper," *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[8] F. Bizzaro, M. Conti, and M. S. Pini, "Proof of Evolution: Leveraging Blockchain Mining for a Cooperative Execution of Genetic Algorithms," in *2020 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2020, pp. 450–455.

[9] S. Chen, H. Mi, J. Ping, Z. Yan, Z. Shen, X. Liu, N. Zhang, Q. Xia, and C. Kang, "A Blockchain Consensus Mechanism that uses Proof of Solution to Optimize Energy Dispatch and Trading," *Nature Energy*, vol. 7, no. 6, pp. 495–502, 2022.

[10] Z. Guo, B. Qin, Z. Guan, Y. Wang, H. Zheng, and Q. Wu, "A High-Efficiency and Incentive-Compatible Peer-to-Peer Energy Trading Mechanism," *IEEE Transactions on Smart Grid*, 2023.

[11] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing Microgrid Energy Markets: A Case Study: The Brooklyn Microgrid," *Applied energy*, vol. 210, pp. 870–880, 2018.

[12] G. Kim, J. Park, and J. Ryou, "A Study on Utilization of Blockchain for Electricity Trading in Microgrid," in *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*. IEEE, 2018, pp. 743–746.

[13] Solarcoin.org, "SolarCoin," 2021, accessed on March, 14 2023. [Online]. Available: https://solarcoin.org/

[14] M. Kiran, A. P. Patil, H. Premkumar, P. Hegde, and P. R. Kumar, "Proof of Solution: Implementation of Work History as Stake in Blockchain Applications," in *2021 IEEE 18th India Council International Conference (INDICON)*. IEEE, 2021, pp. 1–6.

[15] N. Shibata, "Proof-of-Search: Combining Blockchain Consensus Formation with Solving Optimization Problems," *IEEE Access*, vol. 7, pp. 172 994–173 006, 2019.

[16] P. Siano, G. De Marco, A. Rolán, and V. Loia, "A Survey and Evaluation of the Potentials of Distributed Ledger Technology for Peer-to-Peer Transactive Energy Exchanges in Local Energy Markets," *IEEE Systems Journal*, vol. 13, no. 3, pp. 3454–3466, 2019.

[17] C. Yapa, C. De Alwis, M. Liyanage, and J. Ekanayake, "Utilization of a Blockchainized Reputation Management Service for Performance Enhancement of Smart Grid 2.0 Applications," *Journal of Industrial Information Integration*, vol. 39, p. 100580, 2024.

[18] K. Al-Mawali, "Techniques for broadband power line communications: impulsive noise mitigation and adaptive modulation," Ph.D. dissertation, RMIT University, 2011.

[19] L. Di Bert, P. Caldera, D. Schwingshackl, and A. M. Tonello, "On noise modeling for power line communications," in *2011 IEEE International Symposium on Power Line Communications and Its Applications*. IEEE, 2011, pp. 283–288.

[20] C.-Y. Chen and M.-C. Chiu, "Parameter estimation of impulsive noise for channel coded communication systems," *IET Communications*, vol. 15, no. 3, pp. 445–452, 2021.

[21] J. Sun, Y. Liu, and J. S. Dong, "Model Checking CSP revisited: Introducing a Process Analysis Toolkit," in *Leveraging Applications of Formal Methods, Verification and Validation: Third International Symposium, ISoLA 2008, Porto Sani, Greece, October 13-15, 2008. Proceedings 3*. Springer, 2008, pp. 307–322.

[22] H. Afzaal, M. Imran, M. U. Janjua, and S. P. Gochhayat, "Formal Modeling and Verification of a Blockchain-based Crowdsourcing Consensus Protocol," *IEEE Access*, vol. 10, pp. 8163–8183, 2022.

[23] A. Noureddine, "Powerjoular and joularjx: Multi-platform software power monitoring tools," in *18th International Conference on Intelligent Environments (IE2022)*, Biarritz, France, Jun 2022.

[24] F. Gündüz, S. Birogul, and U. Kose, "Proof of Optimum (PoO): Consensus Model based on Fairness and Efficiency in Blockchain," *Applied Sciences*, vol. 13, no. 18, p. 10149, 2023.

[25] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, "Blockchain Consensus: An Overview of Alternative Protocols," *Symmetry*, vol. 13, no. 8, p. 1363, 2021.

[26] J. HussainiWindiatmaja, D. Hanggoro, M. Salman, and R. F. Sari, "PoIR: A Node Selection Mechanism in Reputation-Based Blockchain Consensus Using Bidirectional LSTM Regression Model," *Computers, Materials & Continua*, vol. 77, no. 2, 2023.