SCIENTIFIC Publishing Limited

New Energy Exploitation and Application

http://ojs.ukscip.com/index.php/neea

RESEARCH ARTICLE

Token-Based Smart Power Contract for Interoperable Block-chains of Networked Microgrid System

Desh Deepak Sharma

Electrical Engineering Department, MJP Rohilkhand University, Bareilly, India, deshdeepak101@gmail.com; desh.sharma@mjpru.ac.in

Received: 10 December 2022

Abstract: Designing the secure and privacy-protected smart power contract between electricity suppliers and consumers, considered agents, of different microgrids, is a challenging task in the networked- microgrid system. A framework is suggested in which each microgrid implements a heterogeneous or isomorphic blockchain based platform. The blockchain interoperability, inherently, is present in different blockchains implemented by various microgrids. This paper reviews the interoperability issues and smart contract designs in blockchain based systems. The paper proposes new mechanisms to cater blockchain interoperability challenges to facilitate the design of secure and seamless smart contracts among different blockchains of microgrids. A network hub of heterogeneous or isomorphic blockchains of network microgrids has been created. A methodology has been developed to transfer tokens between interoperable blockchains. Distributed identity-based microgrid (DIBM) scheme is incorporated to make the networked microgrid system secure and trustworthy. This paper suggests an effective consensus protocol for cross-chain architecture that improves the tokenization system and smart power contract designs. For simulation purposes, MATLAB and python programming have been used with real-time data of microgrids.

Keywords: Blockchain, Interoperability, Networked microgrid system, Smart power contracts, Token

1. Introduction

The different prospects, advantages, approaches, and technical challenges pertaining to the application of blockchain technology in smart grids are discussed in[1]. Smart contracts are designed and applied in the digital economy, financial services, health care, and the internet of things. Security and privacy issues are major

*Corresponding Author:
Desh Deepak Sharma
Electrical Engineering Department, MJP Rohilkhand University, Bareilly, India
Email: deshdeepak101@gmail.com

DOI: https://doi.org/10.54963/neea.v2i1.118

challenges in the design of smart contracts[2]. A consensus protocol appropriate to crowdsourcing with the general online service industry has been suggested[3]. A trust-based shard distribution detects malicious nodes in the network with a trust management system and genetic algorithm[4]. A blockchain based security-constrained economic dispatch is proposed in the presence of inefficient and malicious participants at the distributed platform[5]. A decentralized data-driven cognitive computing is applied to solve the problem of data island with privacy protection and efficient processing[6]. A simple and accurate analytical model is proposed to analyze the distributed network split probability[7]. To find the families of cluster-based classification, a new characterization of the consensus algorithm is proposed[8]. For improving the economy and safety of multi-microgrids scheduling, a blockchain-based dynamic electricity price scheme is suggested[9]. A secure, lightweight, and cross-domain blockchain -based internet of thing (IoT) access control system is built by integrating permissioned blockchain, attribute-based access control, and identity-based signature[10,11].

The power transactions represent data stored in the information process and the transactions are grouped in the block. A block is linked to the previous and next one using cryptographic techniques. The smart contracts in the power market facilitate the prosumers to sell a part of their energy per day. A structure of a smart contract comprises (a) interested buyers who decide the amount of electricity to be purchased and the maximum price they can pay, (b) an interested seller who estimates the maximum amount of electricity requirement and capacity to pay the minimum price. Some of the smart contracts utilize the Ethereum network and the energy tokens[14]. The blockchain-based smart contract has advantages as there is no possibility to change the information of transactions by a third party. The Ethereum-based smart contract is written in specific programming languages such as Python, solidity, Golang. These immutable programs tackle the decentralized design of real-world problems[15]

The local trading has been done based on a market that clears the bids and offers, setting the market price. The error-proof intelligent system and different forecasting algorithms are being used to evaluate auctioned quantities. At different time intervals, the imbalance created is resolved with the settlement mechanism[16]. With blockchain technology, market participants can manage transactions effectively. The smart contract comprises the information between the Electric Vehicle and the distribution network. The real-time data sharing and automatic data control process. A charging station gets the hash key of the last transactions and creates a new hash key for the next transaction[17]. Ethereum-based blockchain platform facilitates immutable digital agreements. Automatically, a data command triggers a smart contract on a decentralized blockchain network[19]. The Ethereum virtual machine supports to development of online detection of attacks on smart contracts. A mechanism has to be developed to detect the vulnerabilities in the smart contract and invading transactions[40]. The smart contract is described as a transaction protocol, using digital technology, that executes a request[21]. A heterogonous blockchain system provides interoperability between permissioned and permissionless blockchains of similar protocols and develops the same access control for secured data transfer[22,23].

The electric vehicle trading smart contract consists of three parts (a) inclusion of EV charging and discharging in the auction (b) in the auction, discharging process is considered confidential (c) well-planned execution of the contract[18]. In a contract game approach, electricity consumers develop a trading strategy considering all types of available electricity suppliers. The trading strategies are designed to woo different sorts of electricity suppliers to sell electricity while maximizing revenue.

A. Challenges and Problems

The challenges associated with interoperability among blockchains and the theoretical background of interoperability has been discussed in[22,23]. A mechanism has to be developed to avoid the violation of transactions between two different sorts of blockchains. The standardization of blockchain architecture towards interoperability is a big challenge.

Every blockchain infrastructure possesses the main three objectives such as decentralization, security, and scalability. The process for simultaneous implementation to achieve these three objectives is a challenging task. Several blockchains struggle to implement intercommunication and cross-chain composability and may be isolated within their respective ecosystems. The big challenge in the blockchain ecosystem is that each system and application work in a silo while having no communication of data or compatibility between different protocols. Developing a platform to obtain cross-chain communication and connectivity between multiple blockchains is a challenging task. The Byzantine fault tolerant is implemented in the stable system while considering the fixed consensus threshold.

The nodes may leak the information if the nodes are in a limited number. The nodes may replicate the blockchain data. Also, the nodes may be vulnerable to distributed denial of service attacks (DDoS). The various systems comprising only one gateway device are unable to obtain Byzantine systems. The new challenges associated with cryptographic tokens are distributed network security and denial of service which may affect the characteristics of tokens. Designing cross-chain tokens with different access costs and obtaining diversity in chain tokens are challenging tasks. Designing a framework to obtain more participation from an honest node is highly desirable. The available literature lacks the design of smart power contracts and token-based designs among various scattered microgrids which have implemented heterogeneous and/or isomorphic blockchains. So, there is a research gap in the design of robust, resilient, secure, and reliable smart power contracts among different networked microgrids.

B. Contributions

- Peer-to-peer encrypted token based smart contracts are designed for power exchange among various networked- microgrids. The proposed smart contracts incorporate the operational and financial aspects.

- This paper proposes the network hub of microgrids of various capacities, which implement heterogeneous or isomorphic blockchains. This platform aims to remove inefficiency, lack of flexibility, and the risk of centralization.

- Distributed identity-based microgrid (DIBM) scheme is suggested to make the system secure and trustworthy in the networked microgrid system. The encryption of the smart contract has been done with the Hash key within DIBM.

- A consensus trust-based Practical Byzantine (TpBFT) algorithm is suggested for smart power contracts designed for networked microgrids in network hub of blockchains,

- The trust value evaluation approach of a microgrid is developed for smart power contracts using real-time data.

- The different microgrids implement heterogeneous blockchains such as Ethereum, EOS, or isomorphic blockchains. This paper suggests for creation of Parachain based network hub to networked microgrid systems.

- A model has been designed to employ a multi-chain approach. This model integrates the interoperable powerful blockchain. The trust value evaluation approach of a microgrid is developed for smart power contracts using real-time data.

In this paper, section 1 is the introduction part and section 2 includes the tokenization and heterogeneous blockchains. Section 3 focuses on Distributed Identity Based Microgrid Scheme. Section 4. proposes token based smart power contract design. Section 5 creates the network hubs of blockchains. Trust value evaluation approach has been included in Section 6. Simulation and results are covered in section 7. Section 8 is the concluding part.

2. PROBLEM ASSESSMENT: TOKENIZATION AND HETEROGENEOUS BLOCKCHAINS

The major feature of blockchain is that the created node in blockchain cannot be changed or deleted. In smart contracts of blockchain technology, for selling an object, a representation has to be created. These representations are named tokens. The tokens can represent anything like art, music, painting, other physical objects etc. A token has to be created to sell an object. The token comprises the set of rules developed in the smart contract. Some blockchain applications implement blockchain tokens and others may not. The various kind of blockchain tokens has been designed for circulation in different domains considering the network characteristics (security, vulnerability, delay)[44]. Some of the tokens have the properties of currencies and securities, and others may acquire new concepts and properties[25]. Based on the functionality of the tokenization system, the tokens are classified into three main groups Payment, Utility, and Security tokens[26]. An innovation centered and governance-centered are two schemes suggested for the economics of blockchain [27]. Under the framework for token confidence, the entire economic system with tokens works like a vote of confidence[28]. A smart contract design is the key element of Blockchain. The unification of blockchain, smart contracts, and tokens have been done to obtain a trusted and safe operational environment. The architecture of token-based control has been designed considering equivalence, split, merge, and verification algorithms[29]. For neighboring energy transactions, a consortium-blockchain with a privacy-preserving scheme has been proposed[30]. A framework for organic token trading dynamics between generators and consumers has been suggested. However, this token trading dynamics is ad-hoc, expedient, and unregulated[31]. Immutability is an undisputable property of blockchain, that shows the data cannot be edited and deleted, and the transaction data is temper-proof[32]. The self-made token has been considered for a new economic movement (NEM). A scheme that identifies who issued the token has been developed. A consensus algorithm has been developed to avoid the occurrence of repeated transactions of the block. developed on the local network. In the discrete token generation algorithm, a token is generated with the IP address. If a token comprises multiple IP addresses, then it represents a malicious node[33]. The multi-token Proof-of-Stake (PoS) consensus protocol has been suggested for an interoperable system while the validator and nominators act together to improve the security of the system[31].

The scalability, data size, and privacy problems are the challenges in the development of the blockchain-based energy trading platform with renewable energy. The Polkadot[34] comprises various heterogeneous blockchain based systems which may have individual structures and specialized zone. The Polkadot Relay Chain makes the blockchain based system secure and transfers tokens and data. The Parachain[35] network tries to optimize it's all functionality and provides faster transactions at lower costs. The Parachains are customized blockchain that are connected with main blockchain. The parameters of each Parachain are block time, transactions fees, governance mechanism and mining rewards. The Parachains possess a connection to the relay chain which facilitates the coordinated network with shared security, consensus, and cross-chain interoperability.

The transmission reliability in the networked microgrid system corresponds to network trust connection and network node inactive detection. The trustworthiness of the system has to be quantified to minimize the threats in the networked system. The objective is to identify malicious nodes and inauthentic files and reduce communication costs. The objective is to identify the high credible nodes and improves the communication efficiency of the blockchain system. The network trust value is affected by different network layers. A more effective trust value calculation method has to be designed for reducing malicious data dissemination. All the nodes aim to estimate the trust value of the other nodes on peer-to-peer basis considering most of the nodes behave honestly and detect malicious behavior in the network. As per the opinion and estimation of different nodes, high or low trust value is obtained. The trust model finds the reliability of the node in the networked system. The trust model must identify the malicious nodes and be able to find the similarity if any with other nodes. The malicious nodes must not be included in the consensus mechanism and represent the faulty blocks in the blockchain. A successfully malicious attack must be identified in the network system. The motivation in the networked system is to identify malicious nodes so the system must possess a high level of security mechanism and reliability in all operations. The range and bound of the trust value are to be obtained.

A. Sidechains

The sidechains provide a different kind of protocols to the main blockchain and possess separate block parameters. To obtain high throughput, sidechains may compromise some level of decentralization or security. Sidechains facilitate to use of tokens and digital assets of one blockchain in another blockchain. The sidechains permit the interchangeability of tokens and digital assets at a pre-decided rate between various blockchains using a two-way peg. Also, the sidechains can share the computational load of the main blockchain while increasing flexibility and scalability[35,36].

B. Parachain Network

The limitations of legacy networks can be overcome with the implementation of Parachain s which are the next-generation layer-1 blockchains. The Parachain s facilitate specialized and interconnected diverse ecosystem comprising independent platforms, communities and economies. The Parachain hubs possess various functionalities which can be used to the broader community. The Polkadot integrates communities, rules, economies, and governance with external chains and decentralized digital tokens. An interoperable blockchain known as Polkadot provides a platform to connect multiple heterogeneous blockchain. The Parachain network is capable to process transactions, in parallel. The flexibility, scalability, interoperability, and governance are the main features of the Parachain Network. Interoperability remains a big challenge even after the development of second-generation blockchains such as Ethereum[35].

C. Interoperability in blockchains

Interoperability has been considered a means of survivability and manageability of blockchain system. While there is a transaction between permissionless blockchain and private blockchain then interoperability becomes a complex issue. The blockchain gateways application among interoperable blockchain has to be explored. The definition of interoperability has been shown below[22]: “Interoperable blockchain architecture is a composition of distinguishable blockchain systems, each representing a unique distributed data ledger, where atomic transaction execution may span multiple heterogeneous blockchain systems, and where data recorded in one blockchains are reachable, verifiable, and reference able by another possibly foreign transaction in a semantically compatible manner”. The lack of secured information, inadequate standards, and unavailability of proper communication facilities are major factors in the interoperable blockchains[31]. This paper emphasizes the development of token networks in the cross-chain ecosystem of the network hub of blockchains.

D. Blockchain Enabled Power Transaction

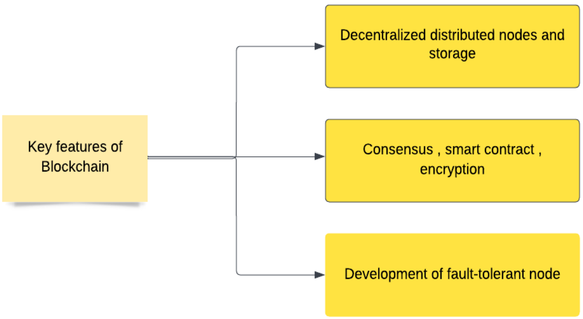

Key features of Blockchain
Decentralized distributed nodes and storage
Consensus , smart contract , encryption
Development of fault-tolerant node

Figure 1. Key features of a Blockchain

Each block of the blockchain comprises (a) the identification ids of buyers and sellers (b) the amount of power to be traded (c) transaction price per kW (d) the time stamp when the execution of the transaction takes place (e) a hash value linking to the previous hash. Furthermore, the transaction has to be validated with some adequate algorithm. The validation time is defined as the difference between transaction submission time and confirmation time. The average validation time (sec) increases as the number of microgrids increases as more blocks representing executed contracts are added to the chain[7]. The key features of blockchain technology are shown in the figure fig.1.

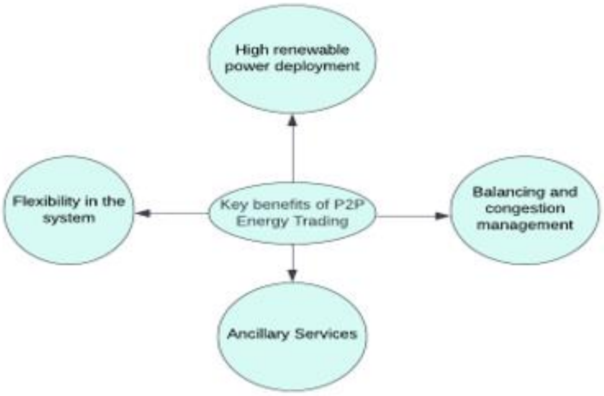

High renewable power deployment
Flexibility in the system
Key benefits of P2P Energy Trading
Balancing and congestion management
Ancillary Services

Figure 2. The key benefits of peer-to-peer energy trading

The prosumers can (a) buy energy from the conventional power system (b) buy renewable energy from other users (c) store their harvested energy (d) sell their energy to other users[17]. The key benefits of peer-to-peer energy trading have been shown in fig.2.

3. PROPOSED DISTRIBUTED IDENTITY BASED MICROGRID SCHEME

Distributed identity-based microgrid (DIBM) scheme allows a microgrid to use its identity as its public key. In a networked microgrid system, DIBM filters access requests to prevent DDoS attacks. In this networked, system, huge data is obtained from IoT devices, edge devices etc. and the distributed information system comprises communication, record-keeping, decision-making, and data analysis. The mechanism of the filter should identify the access request generated by different IoT devices and end devices. The IoT device's ID number and its associated microgrid ID number are specified as *devID*={*deviceID@Microgrid ID*}. The ID of various stakeholders in a networked microgrid is specified as *stackID*={*stackID@Microgrid ID*}. The Barreto-Libert-McCullaghQuisquater (BLMQ) is considered for the implementation of the DIBM scheme. The algorithm of DIBM is shown below : Let the security be k and a group of microgrids in a networked microgrid system be <$\boldsymbol{\mathcal{M}}_1$,………. $\boldsymbol{\mathcal{M}}_N$> that has the same prime order $q > 2^k$. A mapping of $\boldsymbol{\phi}_{21} : \boldsymbol{\mathcal{M}}_2 \longrightarrow \boldsymbol{\mathcal{M}}_1$ represents the tokenized smart power contract between microgrids $\boldsymbol{\mathcal{M}}_1$ and $\boldsymbol{\mathcal{M}}_2$. Select the has function $\boldsymbol{\mathcal{H}}_1:\{0,1\}^* \times \boldsymbol{\mathcal{M}}_1$, ………, $\boldsymbol{\mathcal{H}}_2 :\{0,1\}^* \times \boldsymbol{\mathcal{M}}_2$. The parameters of the networked system of microgrids for DIBM scheme is *param* =< $\boldsymbol{\mathcal{M}}_1$. …….. $\boldsymbol{\mathcal{M}}_N$, $\boldsymbol{\mathcal{H}}_1$……., $\boldsymbol{\mathcal{H}}_N$, $\boldsymbol{\phi}_{ij}$. The cyclic groups <$\boldsymbol{\mathcal{M}}_1$,………. $\boldsymbol{\mathcal{M}}_N$> are generated in subsequent steps of time horizon . The pairing of groups is standardized using IEEE 1363.3-2013 standard. Let $\boldsymbol{\mathcal{R}}_1 \in \boldsymbol{\mathcal{M}}_1$ and $\boldsymbol{\mathcal{R}}_2 \in \boldsymbol{\mathcal{M}}_2$ be the random generator to obtain an efficient isomorphism. $\boldsymbol{\mathcal{H}}_1$……., $_N$ be the set of cryptographic hash function observed as a random oracle used for hashing the *ID* of a receiver with a specific SHA function. The set $\boldsymbol{\mathcal{H}}_1$……., $_N$ is being used in the authenticity, integrity, and confidentiality services of the networked microgrid system.

$$PToK_{i,ex}(t) = f_{DNO}(|X_b^i| + |Y_s^i|) + f_{MO}(|X_b^i| + |Y_s^i|) \quad (1)$$

where $|X_b^i|$ be the number of buying smart contracts and $|Y_S^i|$ be the number of selling smart contracts, and f_{DNO} and f_{MO} are service fee payable to the distribution network operator (DNO) for power exchange between the microgrid and main grid, microgrid operator (MO) for power exchange between two microgrids, respectively. $PToK_{i,ex}$ be the token of the microgrid *i* for the power exchange.

4. PROPOSED TOKEN-BASED SMART POWER CONTRACT

Let S_m be the set of contracts for the market m $\in\{M_f, M_r\}$ where M_f, M_r are forward and real-time markets, respectively. A contract is defined in pair as C=(P_T, PToK)∈ S_m where P_T is the power trade and PToK is the bidding Power Token. Let ρ(S_m^o:={P_T∈Ωm|(P_T, PToK) ∈ S_m^o be the set of underlying power exchanges where $S_m^o \subseteq S_m$ be feasible power exchange and Ωm be feasible trades. Each trade P_T has a buyer $M_b(P_{Tb}) \in N_{MG}$ and seller $M_s(P_{Ts}) \in N_{MG}$ where N_{MG} is the set of microgrids, M_b ∈ $\mathcal{M}_1$……..$\mathcal{M}_N$ and M_s ∈ $\mathcal{M}$1 . …….. $\mathcal{M}$N

are buyer and seller microgrids, P_{Tb} and P_{Ts} are buying and selling power of the microgrid, respectively. The buying and selling power tokens PToKb and PToKs , may be same or different. For a contract, C buying and selling trades are denoted as $P_{Tb}(C)$ and seller $P_{Ts}(C)$. The microgrid involved in a set of contracts. S_m^o are given as $S_m^o := \{U_{c \in S_m^0} P_{Tb}(C), P_{TS}(C)\}$, where $\boldsymbol{U_{c\in S_m^o}}$ is the utility function. A microgrid k has buying smart contracts $X_b^k = \{x \in S_m \,|\, (P_{Tb}(c), PToK_b)\}$ and microgrid k has selling smart contracts $Y_S^k = \{y \in S_m \,|\, (P_{Ts}(c), PToK_s)\}$.

Let u_{MG}^k be the valuation function of microgrid k in the electricity market which are possessing a different set of trades. Each microgrid decides its valuation at different time intervals. For a smart contract, the utility function of microgrid k is defined as

$$U_{MG}^k = \sum_{t=1}^{T} \left[\begin{array}{l} PToK_{k,ex}(t) + u_{MG}^k(t) + \\ \sum_{Y_m^k} PToK_{s,k}(t) - \sum_{X_m^k} PToK_{b,k}(t) \end{array} \right] \quad (2)$$

where [$(P_{Ts}, PToK_s)$, $\mathcal{H}$S:{0,1}*×$\mathcal{M}$S] and [$(P_{Tb}, PToK_b)$,$\mathcal{H}$b:{0,1}*×$\mathcal{M}$b] are sets of selling and buying smart power contracts, respectively. Using utility function microgrid *k* prefers a set of contracts.The token-based smart power transaction scheme in networked microgrid provides the following solution (i) flexible and efficient power transactions (ii) distributed and trusted process (ii) development of fault-tolerant platform (ii) security, concurrency and efficient circulation of PToK (ii) automatic creation of the smart contract .

In the networked microgrid system, the distribution network operator and microgrid charge the amount, in terms of tokens, on each smart power transaction. This is known as the tokenized power exchange cost to be paid by the microgrid.

5. PROPOSED NETWORK HUB OF BLOCKCHAINS

In the proposed network hub of different blockchains, the cross-chain transaction must be validated. The validators are rewarded on the validation of blocks. The cross-chain platform makes it possible to move tokens from one blockchain to another blockchain in the network hub of microgrid, fig. 3. The followings are the functionalities of the network hub.

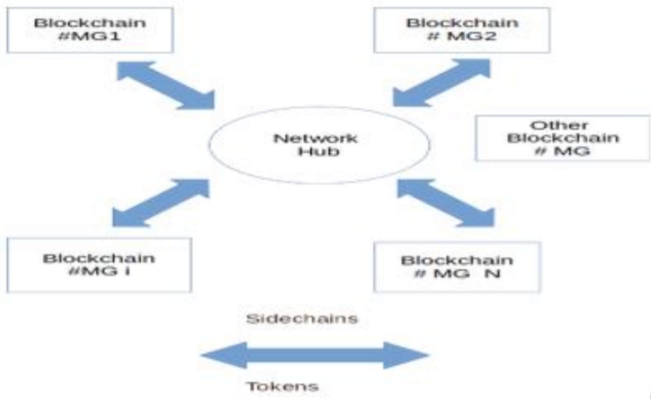


Fig. 3. Network hub of heterogeneous or isomorphic blockchains

1: Broadcast: the main blockchain sends or broadcasts smart power transactions and tokens to output address of the network hub: Broadcast: {*PToK*, X_b, Y_s} >> *NHuB*

2: Lock Network hub assesses and locks this broadcasted smart power transactions and tokens: Lock: {*PToK*, X_b, Y_s}

3: Confirmation: A confirmation signal of smart power transaction design has been broadcasted across the chain

4: Wait: A waiting period occurs for security purposes

5: Equivalence: The two blockchains A and B are equivalent if $PToK_A \rightarrow PToK_B$. The sidechain obtains an equivalent number of locked tokens. 6: Transfer: On request, the smart power transactions token:{*PToK*, X_b, Y_s} may be transferred from the sidechain to main chain.

A. Definition of Token

$PToK_i$ is the token of microgrid *i*. Let G be a subspace of vector space V. An independent set of vectors $\overline{PToK} = \{PToK_1, PToK_2, PToK_N\}$ in space V is a basis for G if

(i) $\overline{PToK}$ is linearly independent and

(ii) The subspace spanned by $\overline{PToK}$ is congruent with G , which means

$$G = Span\{PToK_1, ..., PToK_N\} \quad (3)$$

Theorem 1: Basically, the isomorphism represents a one-to-one linear transformation from a vector space V on to *W*. Let $\overline{PToK} = \{PToK_1, PToK_2, PToK_N\}$ be the basis for a vector space V, Then the coordinate mapping $x \rightarrow [x]_{PToK}$ is one to one linear transformation from V onto W .

Proof :

Two different vectors are considered as

$$u = c_1 PToK_1 + ... + c_N PToK_2$$
$$w = d_1 PToK_1 + ... + d_N PToK_N \quad (4)$$

With vector operations

$$u + w = (c_1 + d_1) PToK_1 + ...$$
$$+ (c_N + d_N) PToK_N \quad (5)$$

Then, it follows

$$[u+w]_{PToK} = \begin{bmatrix} c_1 + d_1 \\ ...... \\ c_N + d_N \end{bmatrix} = \begin{bmatrix} c_1 \\ ...... \\ c_N \end{bmatrix} + \begin{bmatrix} d_1 \\ ...... \\ d_N \end{bmatrix} \quad (6)$$
$$= [u]_{PToK} + [w]_{PToK}$$

6. TRUST VALUE EVALUATION

The different topologies and transmission protocols available in the various network can accelerate the transmission rate and hence Blockchain network performance can be improved. If the network diameter of the Blockchain Network is shortened, then fully distributed unstructured topology can be optimized. But the computation burden is increased due to repeated calculation of network distance by a node from all other nodes[14].

The trust value of an MG is evaluated by the quantization of reliability and credibility evaluated in a cluster of networked microgrid systems. For microgrid i which is a power surplus, using the Euclidean norm, the trust value is formulated as given below.

$$Tv_i(t) = (\sigma_P \| P_{Ts,i}(t) \| + \sigma_C \| PToK_{s,i}(t) \|)^{1/2} \quad (7)$$

where σ_P and σ_C are scaling factors. Similarly, for microgrid i which is a power deficit, the trust value is formulated as given below.

$$Tv_i(t) = (\sigma_P \,\|\, P_{Tb,i}(t) \,\|\, + \sigma_C \,\|\, PToK_{b,i}(t) \,\|)^{1/2} \quad (8)$$

The MG that are rich with surplus power is possessing high trust value and MG with deficit power may have lesser trust value. Microgrids which are having high trust values are assumed the validator MG or the leader MG in the networked microgrid system. The MG with inconsistent and unreliable generation are to be identified with the proposed methodology.

If the total number of microgrids is NMG then the possible smart power contracts energy transaction would be among NMG – f microgrids and where f microgrids are not responding. These f microgrids are misbehaving and faulty, and possess 'no trust'. Furthermore, non-faulty microgrids must be more than faulty microgrids for the design of smart power contracts. For smart power contracts f < fth where fth =round(ln(NMG)). The fth +1 is the minimum number of microgrids that allows a networked-microgrid heterogeneous system works safely and reliably while f < fth microgrids are faulty.

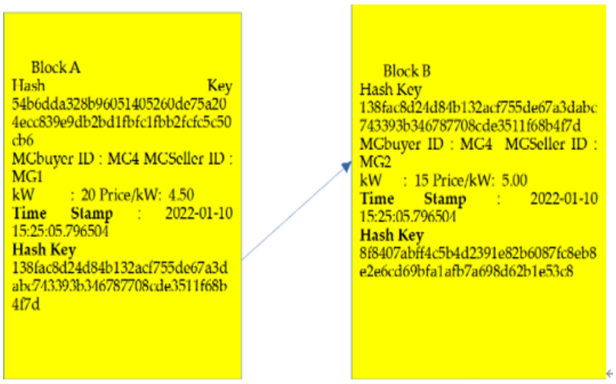
Proposed Algorithm

```
1. procedure pBFT and DBIM
2. Input $N_{MG}$ , $f_{th}$,, $PToK_{s,i}$, $PToK_{b,j}$, <$\mathcal{M}_1$ . ........ $\mathcal{M}_N$ >
3. Define isomorphism mapping as $\phi_{21}$ : $\mathcal{M}_2 \rightarrow \mathcal{M}_1$ with $\mathcal{R}_1 \in \mathcal{M}_1$ and $\mathcal{R}_2 \in \mathcal{M}_2$
4. For encryption generate cryptographic hash key $\mathcal{H}_1$:{0,1}* × $\mathcal{M}_1$ and $\mathcal{H}_2$:{0,1}* × $\mathcal{M}_2$
5. All microgrids implement heterogeneous or isomorphic blockchain
6. Creation of network hubs of heterogeneous or isomorphic blockchain, Parachain
7. For $i$= 1,2,3, ……, $N_{MG}$ do
8. Identification of surplus or deficit power in MG $i$
9. Identification of validator microgrids
10. Creation of smart power contracts by microgrids $X_b^i$ and $Y_s^i$
11. Validation of smart power contracts
12. Request: MG $i$ sends a request of a power transaction to Network Hub
13. The network hub evaluates the $PToK_{s,i}$ , and $X_b^i$ and $Y_s^i$ of MG $i$
14. Received Request: All other microgrids received the request for power transaction
15. Broadcast << PRE-PREPARE
16. $N_{MG}^i$ changes its status to PRE-PREPARED
17. $N_{MG}^i$ broadcasts this message to each other
18. Change their phases to PREPARED
19. Evaluation of trust value of each microgrid $Tv_i$
20. Finalization of the set of smart power contracts $X_b^i$ and $Y_s^i$ .
21.Finalization of the set of smart contracts
22.Network hub sends COMMITED messages to each other
23. If $f < f_{th}$ , then PROCEED else STOP
24.Continue till $t$= 24
```

7. SIMULATION AND RESULTS

1 MW of rooftop solar power plant is installed in the University Campus (MJP Rohilkhand University, Bareilly India) . This 1 MW of solar power plant comprises 30 inverters that can be represented as microgrids of various capacities. Each microgrid comprises around 30-35 solar panels and the real-time 05 min data has been measured and recorded. The data comprises irradiance (w/m2) and power generated by each microgrid. An IoT-based cyber-physical system is implemented and a cluster of these microgrids is considered a networked microgrid. The power generation capabilities of these microgrids are different and the consumers are within the microgrids and outside of the microgrids. A microgrid is facilitated to sell or buy the surplus or deficit energy, respectively, to or from another microgrid or main grid. The amount of energy decided by each seller microgrid to be sold is deter-

mined based on the demand of the buyer microgrid and consumer demand. There is a possibility that the microgrid with deficit power can buy electricity from the main grid and sell it to another microgrid at a higher electricity rate to gain profit in the electricity market of a networked microgrid system. Block A and block B comprise transactions between MG 1 and MG 4, MG 2 and MG 4 respectively, fig.4. The smart energy transactions are held between MG 1 and MG 4, MG 2 and MG 4, and these peer-to-peer energy transactions are encrypted with the hash key generated using the python programming language. These blocks are validated by the distributed network operator. Similarly, new blocks representing energy transactions are created, and after validation, these encrypted blocks are added to previous blocks and, consequently, chain code is formed.



Block A
Hash Key
54b6dda328b96051405260de75a20
4ecc839e9db2bd1fbfc1fbb2fcfc5c50
cb6
MCbuyer ID : MC4 MCSeller ID :
MG1
kW : 20 Price/kW: 4.50
Time Stamp : 2022-01-10
15:25:05.796504
Hash Key
138fac8d24d84b132acf755de67a3d
abc743393b346787708cde3511f68b
4f7d

Block B
Hash Key
138fac8d24d84b132acf755de67a3dabc
743393b346787708cde3511f68b4f7d
MGbuyer ID : MG4 MGSeller ID :
MG2
kW : 15 Price/kW: 5.00
Time Stamp : 2022-01-10
15:25:05.796504
Hash Key
8f8407abff4c5b4d2391e82b6087fc8eb8
e2e6cd69bfa1afb7a698d62b1e53c8

Figure 4. An example of Chaincode formation with blocks for energy transaction

Block A and block B comprise transactions between MG 1 and MG 4, MG 2 and MG 4 respectively, fig.4. The smart energy transactions are held between MG 1 and MG 4, MG 2 and MG 4, and these peer-to-peer energy transactions are encrypted with the hash key generated using the python programming language. These blocks are validated by the distributed network operator. Similarly, new blocks representing energy transactions are created, and after validation, these encrypted blocks are added to previous blocks and, consequently, chain code is formed.

In MATLAB, the smart contracts for peer-to-peer electricity trading are simulated. At a time instant, the set of surplus power (kW) generated by MG1, MG2, MG5, MG6, MG9, MG12, MG13, MG15, MG18, MG19, MG22, MG 23 MG24, MG27, MG28, is [33.8 21.5 18.4 34.4 18.4 37.2 20.3 12.9 12.9 22 12.8 33 33.9 22 36 32.6]. The set of deficit power (in kW) with MG3, MG4, MG7, MG8, MG10, MG11, MG13, MG14, MG16, MG17, MG20, MG 25, MG26, MG29, MG30 is [16.1 14.9322 11.0571 11.5920 11.37 12.05 11.09 05.1654 11.4476 07.1533 09.97 12.28 06.9103 07.4069 06.5512]. The set of selling tokens (in Rs/kW) of microgrids (1,2,5,6,9,12,13,15,18,19,22,23,24,27,28) with surplus power is [5.7202 6.3396 2.6426 5.5240 7.8986 7.1275 7.9529 5.2985 3.2635 5.0176 4.2826 6.4947 4.3872 9.8641 7.9598]. The set of buying smart contract of MG3 is X_b^k (kW,Rs/kW)=[(5.50,5.72), (10.40,2.64) , (6.80,5.52), (10.5,3.26), (5.57,4.28)].

It is assumed that DNO and MO decide to charge 0.25Rs/kW and 0.15Rs/kW per energy transaction hence fDNO =0.75 Rs/kW and fMO =0.75 Rs/kW. In the development of peer-to-peer energy transactions, the trust value of MG3 has been evaluated and is equal to 5.29. The total cost incurred in buying the electricity by MG3 is 6.21 Rs/kW. The trust value was evaluated and equal to 5.29. fth =round(ln(NMG)) as given in section 4 is obtained equal to 4. If 04 or less than 04 microgrids may have problems such as the occurrence of faults, communication failure, denial of service, etc. then successful peer-to-peer smart transactions can be developed among other microgrids. The trust values of different microgrids are obtained using (7) and (8) while and The trust values of MG1 and MG2 are shown in figure 6.

The tokens are generated using the Gaussian function for different microgrids . The value of the tokens is more at higher surplus power, and this value lessens while the surplus power reduces. The tokens of the MG1 and MG4 are isomorphic as discussed in Theorem 1 and shown in figure 7.

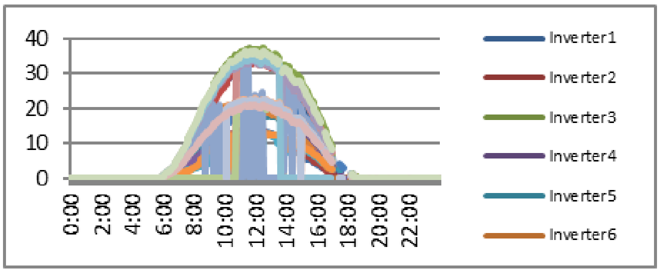


Figure 5. Solar power generation (in kW) by different microgrids(termed as an inverter) at different instants

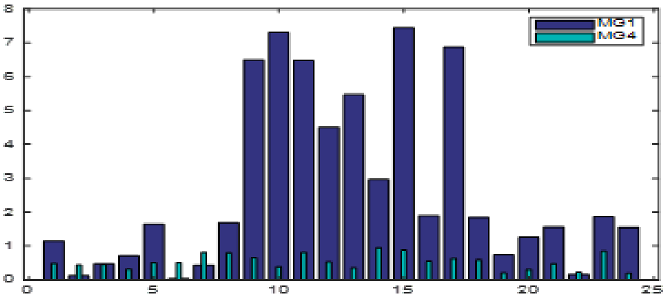


Figure 6. Trust values of isomorphic blockchains implemented by MG1 and MG 4

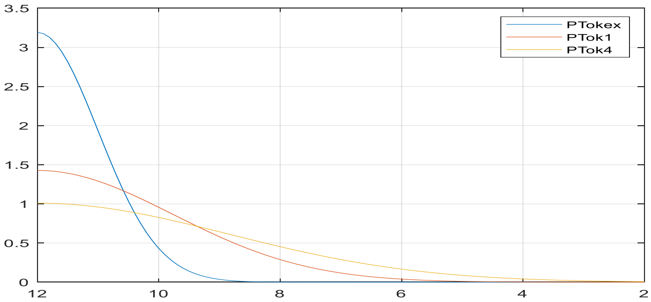


Figure 7. Tokens for smart power contract of MG1 and MG 4 (x- axis: power (kw) , y-axis : tokens(Rs/kW))

8. CONCLUSIONS

In this paper, the architecture of a networked microgrid system has been discussed and peer-to-peer smart power exchange transactions are obtained with information on surplus and deficit power microgrids. The heterogeneous or isomorphic blockchain based platform has been considered for different microgrids. The cross chain-based ecosystem has been developed for the network hub comprising various kinds of blockchains implemented by microgrids. The token-based smart power contracts have been developed for different microgrids. The DIBM scheme is incorporated to create secure, reliable, and authentic the networked microgrid. The proposed methodology makes the networked microgrid maintain integrity and confidentiality. The isomorphism in the tokens of various smart power transactions has been analyzed. Possible selling and buying smart power exchanges are encrypted using blockchain.

References

[1] A. S. Musleh, G. Yao, S. M. Muyeen. Blockchain Applications in Smart Grid–Review and Frameworks. IEEE Access. 7 (2019) 86746- 86755. 10.1109/ACCESS.2019.2920682

[2] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F.-Y. Wang. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. IEEE Transactions on Systems, Man, And Cybernetics: Systems. 49(11) (2019) 2266 – 2277. 10.1109/TSMC.2019.2895123

[3] J. Zhou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, L. Lie. A proof of trust consensus protocol for enhancing accountability in crowdsourcing services. IEEE Transactions on Services Computing. 12(3) (2019) 429-425. 10.1109/TSC.2018.2823705

[4] J. Yun, Y. Goh, and J.-M. Chung, Trust-based shard distribution scheme for fault-tolerant shard blockchain networks IEEE Access , 7 (2019), 135164-175. 10.1109/ACCESS.2019.2942003

[5] S. Chen, L. Zhang, Z. Yan, and Z. Shen, A distributed and robust security-constrained economic dispatch algorithm based on blockchain, IEEE Transactions on Power System, 37(1) 2022, 691-700. 10.1109/TPWRS.2021.3086101

[6] Y. Qu, S. R. Pokhral, Sahil Garg, L. Gao, and Y. Xiang, A blockchain federated learning framework for cognitive computing in industry 4.0 networks, IEEE Transactions on Industrial Informatics, 17(4) , 2021, 2964-2973. 10.1109/TII.2020.3007817

[7] D.Huang, X. Ma, S. Zhang, Performance analysis of the raft consensus algorithm for private blockchains, IEEE Transactions on Systems, Man and Cybernetics: Systems, vol. 50, no. 1, 2020, 172-181. 10.1109/TSMC.2019.2895471

[8] F. Aponte, Luz Gutierrez, M. Pineda, I. Merino, A. Salazar, P. Wightman, Cluster-based classification of blockchain consensus algorithms, IEEE Latin

America Transactions, 19(4) 2021, 688-696. DOI:10.1109/TLA.2021.9448552

[9] M. Tao, Z.Wang, and S. Qu, Research on multi-microgrids scheduling strategy considering dynamic electricity price based on blockchain, IEEE Access, 9, 2021, 52825-52838. DOI:10.1109/ACCESS.2021.3070436

[10] S. Sun, R. Du, S. Chen, and W. Lie, Blockchain-based IoT access control system: towards security, lightweight, and cross domain, IEEE Access, 9(2021), 36868-36878. 10.1109/ACCESS.2021.3059863

[11] P. M. Royo, J. Rodríguez-Molina, J. Garbajosa and P. Castillejo, Towards Blockchain-Based Internet of Things Systems for Energy Smart Contracts With Constrained Hardware Devices and Cloud Infrastructure, in IEEE Access, vol. 9, pp. 77742-77757, 2021, doi: 10.1109/ACCESS.2021.3081932.

[12] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges, IEEE Access, pp. 1–1, 2020

[13] S. -V. Oprea, A. Bâra and A. I. Andreescu, Two Novel Blockchain-Based Market Settlement Mechanisms Embedded Into Smart Contracts for Securely Trading Renewable Energy," in IEEE Access, vol. 8, pp. 212548-212556, 2020, doi:10.1109/ACCESS.2020.3040764.

[14] B. Duan, K. Xin and Y. Zhong, Optimal Dispatching of Electric Vehicles Based on Smart Contract and Internet of Things, in IEEE Access, vol. 8, pp. 9630-9639, 2020, doi:10.1109/ACCESS.2019.2961394.

[15] H. Liu, Y. Zhang, S. Zheng and Y. Li, "Electric Vehicle Power Trading Mechanism Based on Blockchain and Smart Contract in V2G Network," in IEEE Access, vol. 7, pp. 160546-160558, 2019, doi:10.1109/ACCESS.2019.2951057.

[16] S. Seven, G. Yao, A. Soran, A. Onen and S. M. Muyeen, Peer-to-Peer Energy Trading in Virtual Power Plant Based on Blockchain Smart Contracts, in IEEE Access, vol. 8, pp. 175713-175726, 2020, doi: 10.1109/ACCESS.2020.3026180.

[17] E.S. Negara, A.N. Hidanto, R. Andrayani, and Rezki Syaputra, Survey of Smart Contract Framework and Its Application, Information, MDPI, vol. 12, no, 2, 2021, doi ; https://doi.org/10.3390/info12070257.

[18] W. Tushar, T. K. Saha, C. Yuen, D. Smith, and V. Poor, ‘‘Peer-to-peer Trading in Electricity Networks: An Overview,’’ IEEE Trans. Smart Grid, vol. 1, no. 99, early access pp. 1- 1, Jan. 2020.

[19] T. Hardjono, A. Lipton and A. Pentland, "Toward an Interoperability Architecture for Blockchain Autonomous Systems," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1298-1309, Nov. 2020, doi: 10.1109/TEM.2019.2920154.

[20] Pascal Lafourcade, Marius Lombard-Platet (2020) About blockchain interoperability, Information Processing letters , vol.161, https://doi.org/10.1016/j.ipl.2020.105976.

[21] J. Barreiro-Gomez and H. Tembine, "Blockchain Token Economics: A Mean-Field-Type Game Perspective," in IEEE Access, vol. 7, pp. 64603-64613, 2019, doi: 10.1109/ACCESS.2019.2917517.

[22] J. P. Conley, ‘‘Blockchain and the economics of crypto-tokens and initial coin offerings,’’ Dept. Econ. Work. Papers, Vanderbilt Univ., Nashville, TN, USA, Working Paper 17-00008, 2017.

[23] Kharitonova, A.I. (2021). Capabilities of Blockchain Technology in Tokenization of Economy. Proceedings of the 1st International Scientific Conference "Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development" (LARDER 2020).

[24] S. Davidson, P. De Filippi, and J. Potts, ``Economics of Blockchain," Tech. Rep., Mar. 2016, pp. 1_23. doi: 10.2139/ssrn.2744751.

[25] J. Hargrave, N. Sahdev, and O. Feldmeier, ``How value is created in tokenized assets," in Blockchain Economics: Implications Of Distributed Ledgers-Markets, Communications Networks, And Algorithmic Reality. Singapore: World Scienti_c, 2018. doi: 10.2139/ssrn.3146191.

[26] G. Gan, E. Chen, Z. Zhou and Y. Zhu, "Token-Based Access Control," in IEEE Access, vol. 8, pp. 54189-54199, 2020, doi:10.1109/ACCESS.2020.2979746.

[27] X. Zhang, S. Jiang, Y. Liu, T. Jiang and Y. Zhou, "Privacy-Preserving Scheme With Account-Mapping and Noise-Adding for Energy Trading Based on Consortium Blockchain," in IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 569-581, March 2022, doi:10.1109/TNSM.2021.3110980.

[28] M. T. Devine and P. Cuffe, "Blockchain Electricity Trading Under Demurrage," in IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 2323-2325, March 2019, doi: 10.1109/TSG.2019.2892554.

[29] E. Politou, F. Casino, E. Alepis and C. Patsakis, "Blockchain Mutability: Challenges and Proposed Solutions," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 4, pp. 1972-1986, 1 Oct.-Dec. 2021, doi: 10.1109/TETC.2019.2949510.

[30] X. Cong, L. Zi and D. -Z. Du, "DTNB: A Blockchain Transaction Framework With Discrete Token Negotiation for the Delay Tolerant Network," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1584-1599, 1 April-June 2021, doi: 10.1109/TNSE.2021.3065058.

[31] Y. Pang, "A New Consensus Protocol for Blockchain Interoperability Architecture," in IEEE Access, vol. 8, pp. 153719-153730, 2020, doi:10.1109/ACCESS.2020.3017549

[32] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A.

Dehghantanha, and K.-K.-R. Choo ``Sidechain technologies in blockchain networks: An examination and state-of-the-art review," J. Netw. Comput. Appl., vol. 149, Jan. 2020, Art. no. 102471

[33] J. S. Bellagarda and A. M. Abu-Mahfouz, "An Updated Survey on the Convergence of Distributed Ledger Technology and Artificial Intelligence: Current State, Major Challenges and Future Direction," in IEEE Access, vol. 10, pp. 50774-50793, 2022, doi: 10.1109/ACCESS.2022.3173297.

[34] H. Abbas, M. Caprolu and R. Di Pietro, "Analysis of Polkadot: Architecture, Internals, and Contradictions," 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 61-70, doi: 10.1109/Blockchain55522.2022.00019.

[35] J. S. Bellagarda and A. M. Abu-Mahfouz, "An Updated Survey on the Convergence of Distributed Ledger Technology and Artificial Intelligence: Current State, Major Challenges and Future Direction," in IEEE Access, vol. 10, pp. 50774-50793, 2022, doi:10.1109/ACCESS.2022.3173297.