Resilience-Driven Scheme in Multiple Microgrids with Secure Transactive Energy System Framework

Dillip K. Mishra[1], Jiatong Wang[1], Li Li[1], Jiangfeng Zhang[2], and M. J. Hossain[1]
[1]School of Electrical and Data Engineering, University of Technology Sydney, Australia
[2]Department of Automotive Engineering, Clemson University, USA

Abstract-- **In concern of energy trilemma such as energy security, energy equity, and environmental sustainability, the electric infrastructures are significantly developing the manifold avenues for decentralization, decarbonization, and digitalization. Over the years, the growth of decentralized power systems using distributed energy resources is increasing rapidly, bringing new prospects for local energy trading concerning economic and control operations in a single framework called transactive energy (TE). However, the continuity of power supply after high-disruptive events has remained a potential challenge for the energy market operator. Thus, to triumph over the challenges, this paper proposes a novel TE framework with resiliency consideration. On the other hand, cyber-attacks are an increasing concern, which impacts the digital platform, such as energy digitization. Considering this, homomorphic Blockchain technology is applied to secure the TE platform against cyber-attacks. To show the leveraging capabilities, this paper considers various case studies in the wake of high-disruptive events such as microgrid outage conditions and cyber-attack. The result shows that the proposed TE framework enhances the microgrid benefit and guarantees optimal trading performance. In addition, empowering Blockchain realizes that the security of the system is vital for the TE system when it faces data tampering or any external attacks. The effectiveness and feasibility of the proposed system are evaluated by cost, benefit, and probability of success.**

Index Terms- **Blockchain, Energy Market, False Data Injection Attack, Microgrids, Resilience, Transactive Energy**

NOMENCLATURE

TE	Transactive energy
FDI	False data injection
MG	Microgrid
MMG	Multi-microgrid
SOC	State of charge
Parameters	
a_{ij}	power loss percentage
$\mathcal{A}_{\mathcal{PV},i}$	size of the PV panel in i^{th} MG
$\mathbb{b}_1$	beneficiary account balance
$\mathfrak{B}$	percentage of the non-critical load
$\mathfrak{C}_{ij,t}^{\mathcal{B}}$	transaction price of MG at time *t*
$\mathfrak{C}_{G,t}^{pur}$	buying price from the upstream grid at time t
$\mathfrak{C}_{G,t}^{sell}$	selling price to the upstream grid
$\mathfrak{C}_{gc}$	generation cost coefficient
$\mathfrak{C}_O$	utilization cost coefficient of each transaction
h	number of sensors that need to be hacked
$\mathbb{E}_{\mathcal{B},i}^c$	battery capacity for MG i
$\mathbb{K}_{pu,M_1}$	public keys
$\mathbb{K}_{pr,M_1}$	private keys
K	number of attacked communication channels
$\mathbb{L}$ & $\mathbb{G}$	lowest common multiple and greatest common factor
n	number of blocks
$\mathbb{N}$	number of MGs
$\mathbb{P}_{LD,i}$ & $\mathbb{P}_{LD,i}^{nc}$	actual demand and non-critical load of MG i, respectively
P_{Rec} & P_{TL}	recovered load and total load of outage MGs.
$\mathcal{P}_{e,t}^{inj}$ & $\mathcal{P}_{e,t}^{gen}$	active power injection/production at e^{th} node at time t
$\mathcal{P}_{\mathcal{L},e,t}$	load demand of e^{th} node at time t
$\mathcal{Q}$ & $\mathbb{X}$	Plaintext & ciphertext
$\mathfrak{R}$	resiliency measure
$\mathbb{S}_{e,f,t}^{inj}$	apparent power between nodes e & f at time t
SOC_i^{min} & SOC_i^{max}	Battery's minimum and maximum SOC for MG i, respectively
$\mathcal{T}^{on}, \mathcal{T}^{mid}, \mathcal{T}$	sets of the on-, mid-, and off-peak time.
$\mathcal{U}$	amount of energy trade in Blockchain
$\mathcal{V}_{e,t}/\emptyset_{e,t}$	voltage/phase angle at e^{th} node at time t
$\mathbb{Z}$	modulus
$\eta_{\mathcal{PV}}$	efficiency of the PV panel
Δt	time interval
$\eta_{\mathcal{B},c}$ & $\eta_{\mathcal{B},d}$	charging and discharging efficiency
$\mathfrak{S}_{\mathcal{PV},t}$	solar radiation at time t
$\mathcal{E}$ & $\mathcal{D}$	encryption and decryption functions
$\mathfrak{P}_{1\mathcal{U}}$ & $\mathfrak{P}_{2\mathcal{U}}$	encryption parameters
$\mathfrak{z}$ & $\mathfrak{y}$	two random prime numbers
Variables	
$\mathcal{C}_i$	total energy cost of i^{th} MG
$\mathcal{C}_{ij}^t$	energy trading cost at time *t* for energy from the i^{th} MG to j^{th} MG or the main grid
$\mathcal{C}_i^{WT}$	energy cost of MG *i* without the TE framework
$\mathcal{C}_{\mathbb{B}_{MO},t}$	market operator benefits at time *t*
$\mathbb{K}$	key
M_{ij}	energy trading amount between MG *i* and MG *j*
$SOC_{i,t}$	battery SOC for MG i at time t

I. INTRODUCTION

OVER the past few decades, power distribution systems have been undergoing significant changes due to the increase in renewable energy penetrations and energy storage. This change has played a key role in distribution system modernization and remarkably switched the mindset of customer choices from consumer to prosumer. Prosumers are the end-users who also have their own generations; thus, the surplus power can be fed to the upstream grid. Nowadays, the smart grid evolved as an emerging technology in the power system in which energy trading services can take place, and the prosumer plays a major role in buying and selling the power. This technology is called transactive energy (TE), where prosumers trade energy economically [1, 2].

Several studies on the TE scheme have focused on different pricing mechanism strategies to achieve economical operation and customer benefits. For example, a TE control mechanism with the double-auction market is introduced in [3], which coordinates the internal electrical equipment of commercial buildings. A day-ahead TE model is proposed in [4] to manage the operation and participation of the distribution system operator in the wholesale market. The active participation of distributed energy resources through residential consumers is modeled via a multi-agent-based TE scheme [5, 6]. The cost-benefit studies of the TE scheme through various scenarios are reported in [7, 8]. In addition, a few other studies cover the TE market based on bidding mechanisms according to consumer priorities [9, 10]. Indeed, the developed TE schemes have great potential to provide better opportunities for the future energy market, but the pricing mechanism and incentive schemes still need attention. On the other hand, the function of the TE system could suffer from a higher degree of complexity in fostering the stakeholder objectives of the market [11]. Notwithstanding, the TE system needs to take care of stakeholder's malicious and inattentive trading action, which would obstruct the trustworthiness of market operations and, subsequently, cause instability in the active distribution system[12]. In addition, privacy leakage is another challenge in the TE system that stakeholders should avoid. A Blockchain-based TE system has recently shed new light on overcoming the abovementioned issues [13].

Furthermore, in the TE scheme, a large amount of information [14], including bids, offers, and energy availability, are exchanged, and it could face huge challenges in the face of a cyber-attack. Thus, the Blockchain-enabled TE scheme is vital to secure the transaction and critical information. Considering the above challenges and issues, power system researchers have initiated Blockchain applications in the TE system in the last few years, which are discussed in [13, 15, 16]. Moreover, these studies are only early-stage designs and frameworks, which still need to be explored more.

In today's world, Blockchain is one of the emerging technologies and has great potential to drive comprehensibility and profitability through a high level of security concern. It has far-reaching appeals in financial services, public sectors, and media industries, but now it is also the emergence of technology in the energy sector to transform the ongoing energy market operation. Notably, Blockchain technology has already been operated in many places across the globe, for example, WePower in Estonia, Power Ledger in Australia, Brooklyn Microgrid in the United States, Sun Exchange in South Africa, etc. In fact, Blockchain is a growing list of files, classed as blocks that are connected to each other through cryptographic signature, and each block includes a hash function, timestamp, and transaction data [17]. Recently, the application of Blockchain through Ethereum has reached a milestone in terms of transactions due to its faster operation [18]. It enables a definitive and trusty computation using smart contracts. In reference to this operation, the application of Blockchain sheds light on energy system security, as evidenced by executing multiple data verification and secure market-based transaction for the peer-to-peer energy markets [19]. It creates a decentralized database where data are stored chronologically with a crypto signatory as an individual secret key that cannot be tampered with. A recent study in [20] elucidates the significance of a secret key, otherwise called a data authentication key, through homomorphic encryption-based Blockchain technology. As far as the data authentication key is concerned, it is explicitly used for securing transaction data through ciphertext. The ciphertext is a text which has two forms, encryption cipher and decryption cipher. The plaintext is encrypted initially, and data can be transferred from one node to another, and then it transforms the ciphertext to plaintext through decryption using secret keys.

Blockchain technology has revolutionized the energy sector recently, particularly in the TE market. A few studies have explored the potential of Blockchain in TE, which can be seen in [13, 21-23]. The authors in [13] developed the Blockchain-based TE framework, aiming to incentivize prosumers in terms of cost reduction. Besides, the trustable TE platform is developed to preserve users' privacy. In [21], an energy trading platform is developed through Blockchain techniques to manage the monetary fund and focus on end-user marginal price at a reduced rate with existing trading pricing methods. In addition, sensitivity analysis is conducted to study the market loss and violation of smart contracts. In [22], the implementation of Blockchain in the TE framework is presented by considering virtual power plants. As noted, the Blockchain in [22] can enhance the reliability and transparency of the TE market to reduce energy costs and increase consumer participation. In [23], a distributed Blockchain is implemented in the modern power system, and a secure hash algorithm is applied for transaction security. However, this study does not cover the TE market.

Although the emerging study on TE markets and the operational mechanisms have been successfully applied to reduce costs and ensure privacy in the TE market, there is still a need to investigate the improvement of its performance when encountering unpredictable events, such as cyber-attacks and system outages. Cyber-attacks can exploit system vulnerabilities, aiming to attack critical infrastructures and virtual information assets, disrupting the system service and resulting in significant financial losses [14]. On the other hand, while TE markets demonstrate their advantages in the economic sector, this new concept also has the potential to introduce complexities to the existing power system. Therefore, there is an urgent need to evaluate self-healing performance of the system in the event of a system outage [24].

The above-studied papers are limited to cost reduction and privacy assurance in the TE market. However, they do not address the growing concerns of cyber-attacks and other unforeseen events that pose a threat to the TE system. To address these challenges, it is essential to develop a resilient TE system capable of withstanding extreme events. Subsequently, a secure trading platform with a cost-benefit strategy needs to be developed. In this regard, this paper proposes a novel pricing mechanism that considers power loss, homomorphic secret key generation technique, outage implication for energy optimality, security enhancement, and resiliency. From this perspective, a three-layer-based TE architecture is studied in this paper (see Fig. 1), where each layer has its significance and has been evaluated in terms of security and resiliency. This framework aims to not only provide benefits to market participants but also ensure high-security performance during events.

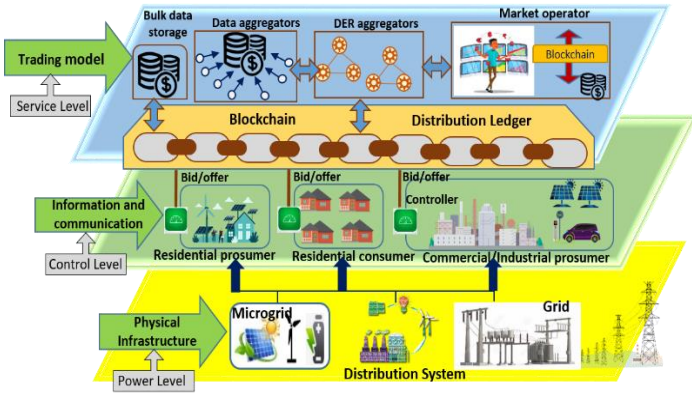


Fig. 1 Three-Level Blockchain-enabled TE architecture

Notably, the cyber-physical power system has already marked a breakthrough in the energy sector, and further implementation of Blockchain can be a remarkable change [25]. Thus, three layers of energy market structure have begun, such as power level, control level, and service level, which are considered in this study, as shown in Fig. 1. The physical infrastructure, such as grid supply and multi-microgrids, is considered in the power level. Each microgrid (MG) comprises energy storage units and renewable generation (including PV and wind). Greater divergence of the load profiles of MGs is assumed, and the energy exchange is made through MG to MG and MG to grid. All the information and communication devices are put into practice at the control level to regulate the bids, offers, and supply-demand profiles. This level enables the TE mechanism to ensure the operator benefits. To enable the TE scheme, the decision of pricing mechanism is not only the key but also needs a secured data exchange platform. Thus, a trading model through Blockchain is implemented at the service level to secure the platform.

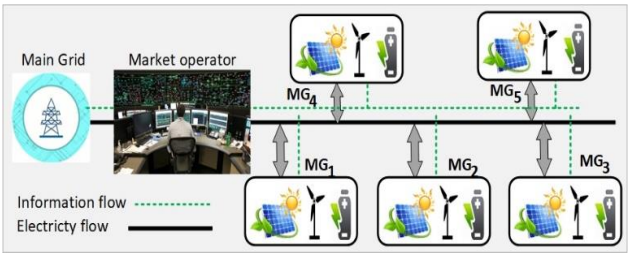
The proposed TE framework considers three factors: economical operation with a better pricing mechanism scheme, resiliency, and security concerns. In the TE framework, multiple MGs are considered with high penetration of renewables, such as PV and wind, and to support the load during an emergency, battery storage is used in each MG. Further, the extreme event is considered to show the resiliency of the system and restore the critical load through MG sharing and grid supply, where MG outage condition is assumed. Moving further, homomorphic Blockchain technology is applied to secure the transaction against cyber-attacks. To sum up, the main contributions of this paper are as follows:

- A novel TE framework is presented in this study to address two critical issues of the energy market, *i.e.*, energy optimality and privacy assurance. Considering energy optimality, a new pricing mechanism scheme is developed and applied in the TE framework.
- Further, secure energy trading is done by Blockchain-empowered technology to ensure privacy assurance. Indeed, concerning extreme or high-disruptive events, such as MG outage conditions and FDI attacks, a defensive mechanism is proposed to operate the TE system resiliently.
- Finally, an extensive evaluation of the attack-defensive capability of Blockchain technology is illustrated in terms of the probability of success.

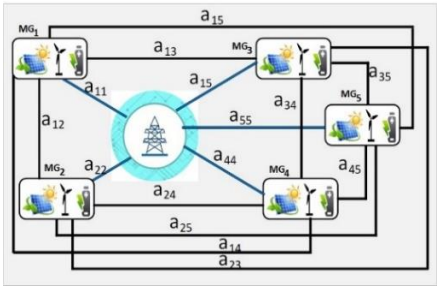
The remainder of this paper is organized as follows. Section II presents the system model and its description. The proposed TE framework and its pricing mechanism are discussed in Section III. Section IV elaborates on implementing blockchain technology in the TE framework. Section V evaluates the performance of the proposed framework with various scenario studies. Finally, Section VI offers the concluding remarks and future scope of the research.

II. System ~~Model~~Model

This section presents the proposed system model for a TE system, which can be applied to any multi-MG system. Each MG comprises a combination of PV, wind, and battery storage systems as a clean energy generation. In the proposed TE system, energy trading occurs between MGs and the power grid, as shown in Fig. 2 (a). The generation from PV and wind can be used in the TE scheme and storage requirement or sent back to the upstream grid. Indeed, there are two ways to trade the energy within the TE system: MG to MG and MG to grid. This condition will arise when the generation is insufficient to meet its load demand, and the required energy can be received from other MGs or the upstream grid, as shown in Fig. 2 (b). Notably, the main aim of the TE scheme is to reduce the dependence on the upstream grid, and optimal trading can be made among neighbor MGs. On the other hand, it is a great platform for dynamic energy balancing; subsequently, through market interaction, the overall energy cost of MG can be minimized.



(a) Operational Framework



(b) Multi-Microgrid TE topology

Fig. 2 TE structure

Moreover, the main focus of the TE scheme exhibits two major factors: economic and environmental. From the economic point of view, the TE system has a low energy cost provider platform, whereas the environmental aspect denotes energy generation through renewable-based sources [26]. Thus, the TE framework is becoming more popular as it realizes the economic and environmental goals through the TE scheme.

A. Objective Function

The objective of the proposed TE system is to minimize the total energy cost of each MG, which is expressed in (1), while satisfying the operational constraints (2-15, 17-18, 20-21).

$$Min\ (\mathcal{C}_1, \mathcal{C}_2, \dots \dots \mathcal{C}_i) \quad (1)$$

$$\mathcal{C}_i = \sum_{t \in \mathcal{T}} \sum_{j \in N} (\mathcal{C}_{ij}^t) \qquad i \in N$$

where $\mathcal{C}_{ij}^t$ ($) is the energy trading cost at time *t* for energy from the i^{th} MG to j^{th} MG *(i ≠ j)*, or to the main grid *(i = j)*, with $\mathcal{C}_{ij}^t > 0$ indicating the obtained energy cost and $\mathcal{C}_{ij}^t < 0$ the delivered energy cost. $\mathcal{C}_{ij}^t$ is calculated using (21), and described at the later stage in Section III. The detailed constraints are discussed as follows.

B. Constraints

1) Generation-Load balance

At every time t, the amount of generation should be equal to the consumption expressed in (2) to maintain the electricity balance.

$$\mathbb{P}_{\mathcal{W},i,t} + \mathbb{P}_{\mathcal{PV},i,t} + \mathbb{P}_{E,i,t} = \mathbb{P}_{LD,i,t} + \mathbb{P}_{\mathcal{B},i,t} \qquad \forall i, \forall t \quad (2)$$

where $\mathbb{P}_{\mathcal{W},i,t}$ is the wind power generation in i^{th} MG at time t; $\mathbb{P}_{\mathcal{PV},i,t}$ is the PV power generation in i^{th} MG at time t; $\mathbb{P}_{E,i,t}$ is the net power injection in i^{th} MG from other MGs/grid through TE market at time t; $\mathbb{P}_{\mathcal{B},i,t}$ is the charging /discharging rates for battery storage in i^{th} MG at time t; (positive is charging, negative is discharging); $\mathbb{P}_{LD,i,t}$ is the load demand in i^{th} MG at time t.

2) PV constraints

$$\mathbb{P}_{\mathcal{PV},i,t} \leq \mathcal{A}_{\mathcal{PV},i} \cdot \eta_{\mathcal{PV}} \cdot \mathfrak{S}_{\mathcal{PV},t} \quad (3)$$

where $\mathcal{A}_{\mathcal{PV},i}$ is the size of the PV panel in i^{th} MG; $\eta_{\mathcal{PV}}$ is the efficiency of the PV panel; $\mathfrak{S}_{\mathcal{PV},t}$ is solar radiation at time t.

3) Wind turbine constraints

$$\mathbb{P}_{\mathcal{W},i,t} = \begin{cases} 0, & \mathcal{W}_{s,t} < \mathcal{W}_{\mathbb{CI}_i} \text{ or } \mathcal{W}_{s,t} > \mathcal{W}_{\mathbb{CO},i} \\ \mathbb{P}_{\mathcal{WR},t,max} \cdot \left(\dfrac{\mathcal{W}_{s,t} - \mathcal{W}_{\mathbb{CI}_i}}{\mathcal{W}_{\mathbb{R},i} - \mathcal{W}_{\mathbb{CI}_i}}\right)^3, & \mathcal{W}_{\mathbb{CI}_i} \leq \mathcal{W}_{s,t} \leq \mathcal{W}_{\mathbb{R},i} \\ \mathbb{P}_{\mathcal{WR},t,max} & \mathcal{W}_{\mathbb{R},i} \leq \mathcal{W}_{s,t} \leq \mathcal{W}_{\mathbb{CO},i} \end{cases} \quad (4)$$

where $\mathbb{P}_{\mathcal{W},i,t}$ is the wind turbine output in i^{th} MG at time t; $\mathbb{P}_{\mathcal{WR},i,max}$ is the rated wind power in i^{th} MG at time t; $\mathcal{W}_{s,t}$,$\mathcal{W}_{\mathbb{R},i}$ $\mathcal{W}_{\mathbb{CI}_i}$, and $\mathcal{W}_{\mathbb{CO},i}$ is the predicated, rated, cut-in, and cut-out wind speeds in i^{th} MG at time t, respectively.

4) Battery storage constraints

$$SOC_{i,t+1} = SOC_{i,t} + \frac{\mathbb{E}_{\mathcal{B},i,t}}{\mathbb{E}_{\mathcal{B},i}^c} \qquad \forall t \in \mathcal{T}, i \in N \quad (5)$$

$$SOC_i^{min} \leq SOC_{i,t+1} \leq SOC_i^{max} \quad \forall t \in \mathcal{T}, i \in N \quad (6)$$

$$\mathbb{E}_{\mathcal{B},i,t} = \begin{cases} \eta_{\mathcal{B},c} \mathbb{P}_{\mathcal{B},i,t} \Delta t & if\ \mathbb{P}_{\mathcal{B},i,t} > 0 \\ \mathbb{P}_{\mathcal{B},i,t}\ \Delta t / \eta_{\mathcal{B},d} & if\ \mathbb{P}_{\mathcal{B},i,t} \leq 0 \end{cases} \quad (7)$$

$$\mathbb{P}_{\mathcal{B},i,t} \in [-\overline{\mathbb{P}}_{\mathcal{B}}, \overline{\mathbb{P}}_{\mathcal{B}}] \qquad \forall t \in \mathcal{T}, i \in N \quad (8)$$

where $SOC_{i,t}$ is the battery state-of-charge for MG i at time t; SOC_i^{min} and SOC_i^{max} are respectively battery minimum and maximum SOC for MG *i*; $\mathbb{E}_{\mathcal{B},i}^c$ is the battery capacity for MG *i*; Δt is the time interval; and $\eta_{\mathcal{B},c}$/$\eta_{\mathcal{B},d}$ are charging/discharging efficiency. $\mathcal{T}$ = [1, 2, …,24] and N =[1, 2, ..., $\mathbb{N}$].

5) Power grid constraints

Eq. (2) defines active power generation, and Eqs. (9-12) represent the apparent power, voltage, and angle limit.

$$\mathcal{P}_{e,t}^{inj}(\mathcal{V}_{e,t}, \emptyset_{e,t}) + \mathcal{P}_{\mathcal{L},e,t} = \mathcal{P}_{e,t}^{gen} \qquad \forall e, \forall t \quad (9)$$

$$\mathbb{S}_{e,f,t}^{inj}(\mathcal{V}_{e,t}, \mathcal{V}_{f,t}, \emptyset_{e,t}, \emptyset_{f,t}) \leq \mathbb{S}_{e,f}^{max} \qquad \forall e, \forall f, \forall t \quad (10)$$

$$\mathcal{V}_e^{min} \leq \mathcal{V}_{e,t} \leq \mathcal{V}_e^{max} \qquad \forall e, \forall t \quad (11)$$

$$-\pi \leq \emptyset_{e,t} \leq \pi \qquad \forall e, \forall t \quad (12)$$

where $\mathcal{P}_{e,t}^{inj}(\mathcal{V}_{e,t}, \emptyset_{e,t})$/$\mathcal{P}_{e,t}^{gen}$ is the active power injection/ production at e^{th} node at time t; $\mathbb{S}_{e,f,t}^{inj}(\mathcal{V}_{e,t}, \mathcal{V}_{f,t}, \emptyset_{e,t}, \emptyset_{f,t})$ is the apparent power between nodes e & f at time t; $\mathbb{S}_{e,f}^{max}$ is the maximum apparent power; $\mathcal{V}_{e,t}/\emptyset_{e,t}$ is the voltage/phase angle at e^{th} node at time t; $\mathcal{V}_e^{min}/\mathcal{V}_e^{max}$ is the minimum/maximum voltage magnitude.

6) Load demand profile

In this proposed system, each MG has a different load profile, and 30% of its load is considered as critical load. Accordingly, the minimum level of resilience should be 0.3. Hence, considering the resiliency, the load constraint should be $\mathbb{P}_{LD,i,t} \geq (1 - \mathfrak{B})\mathbb{P}_{LD,i}^{rated}$, where $\mathbb{P}_{LD,i}^{rated}$ is the rated load demand profile of MG is; $\mathfrak{B}$ is the percentage of the non-critical load. This means the minimum load can be served if an extreme event happens. In this study, $\mathfrak{B}$ is taken as 70% or 0.7. Assume that the demand profile in i^{th} MG is expressed as (13), and the actual demand is expressed as (14).

$$\mathbb{P}_{LD} = [\mathbb{P}_{LD,1}\ \mathbb{P}_{LD,2} \dots \mathbb{P}_{LD,\mathbb{N}}] \quad (13)$$

$$\mathbb{P}_{LD,i}^{nc} = \mathfrak{B}\mathbb{P}_{LD,i} \quad (14)$$

where $\mathbb{P}_{LD}$ is the demand profile of MGs; $\mathbb{P}_{LD,i}$ and $\mathbb{P}_{LD,i}^{nc}$ are the actual demand and non-critical load of MG *i*, respectively, and $\mathfrak{B}$ is the percentage of the non-critical load.

7) Resilience measure

As per the load demand profile expressed in (13), the critical load must be met irrespective of extreme event conditions. So, the resiliency ($\mathfrak{R}$) of the system can be measured as (15).

$$\mathfrak{R} = \frac{P_{Rec}}{P_{TL}} \quad (15)$$

$\mathfrak{R}$ can also be defined as the load recovery index ($Range$: $0.3 < \mathfrak{R} < 1$); P_{Rec} & P_{TL} are the recovered load and total load of outage MGs. Eqs. (13) and (14) are the load demand profile of each MG and the amount of non-critical load, respectively. Each MG should have a minimum amount of critical load, which is 30% and should be recovered after the extreme events, defined as recovery load, *i.e.*, P_{Rec}. Besides, the resilience $\mathfrak{R}$ must be greater than or equal to a percentage of critical load, defined as $\mathfrak{R} \geq (1 - \mathfrak{B})$. Further, according to the availability of generation, the system's resilience can be improved by restoring more loads, including the non-critical load.

III. Transactive Energy Framework

This section presents the TE modeling and pricing mechanism. The proposed TE model considers five MGs and the main grid for energy trading. Moreover, the market operator is operating all the trading actions optimally as per the load demand and time (on-peak, mid-peak, and off-peak). The energy trading of the MMG system can be defined as (16).

$$M_t = \begin{vmatrix} M_{11,t} & M_{12,t} & M_{13,t} & M_{14,t} & M_{15,t} \\ M_{21,t} & M_{22,t} & M_{23,t} & M_{24,t} & M_{25,t} \\ M_{31,t} & M_{32,t} & M_{33,t} & M_{34,t} & M_{35,t} \\ M_{41,t} & M_{42,t} & M_{43,t} & M_{44,t} & M_{45,t} \\ M_{51,t} & M_{52,t} & M_{53,t} & M_{54,t} & M_{55,t} \end{vmatrix} \quad (16)$$

where M_{ij} is the energy trading amount between MG *i* and MG *j* (*i ≠ j*) or between MG *i* and upstream grid (*i = j*), with a positive sign indicating MG *i* buying energy and a negative sign indicating MG *i* selling energy.

The net power injection in i^{th} MG from other MGs/grid through the TE market at time t is defined in (17),

$$\mathbb{P}_{E,i,t} = \sum_{j=1}^{\mathbb{N}} \widehat{M}_{ij,t}/\Delta t \tag{17}$$

where $\widehat{M}_{ij,t} = \begin{cases} M_{ij,t}, & M_{ij,t} \geq 0 \\ \frac{M_{ij,t}}{1-a_{ij}}, & M_{ij,t} < 0 \end{cases}$ and a_{ij} is the power loss percentage.

Assume $\mathcal{B}$ is a physical transfer contract specifying that the customer receives energy from the TE market at a price $\mathfrak{C}_t^{\mathcal{B}}$. This price is calculated as the average value of a reference price related to the contract, denoted by $\mathfrak{C}_{ij}^{\mathfrak{S}}$, and the pool price $\mathfrak{C}_t^P$. Indeed, the pool prices depend on the time interval t, and the final price of the trading energy through the bilateral contact is defined by $\mathfrak{C}_{ij,t}^{\mathcal{B}}$, expressed in (18). Further, the cost can be calculated using the bilateral price in (18).

$$\mathfrak{C}_{ij,t}^{\mathcal{B}} = \begin{cases} \dfrac{\mathfrak{C}_{ij}^{\mathfrak{S}} + \mathfrak{C}_{ij,t}^{P}}{2} & i \neq j, \\ \mathfrak{C}_{G,t}^{pur} & i = j,\ M_{ij} \geq 0 \\ \mathfrak{C}_{G,t}^{sell} & i = j,\ M_{ij} < 0 \end{cases} \tag{18}$$

where $\mathfrak{C}_{ij,t}^{\mathcal{B}}$ (\$/kWh) is the transaction price of MG at time *t*; $\mathfrak{C}_{G,t}^{pur}$ (\$/kWh) is the buying price from the upstream grid at time *t*; $\mathfrak{C}_{G,t}^{sell}$ (\$/kWh) is the selling price to the upstream grid;

The cost is stated in (19), which depends on the trading hours, such as on-peak, mid-peak, and off-peak time, and the relation is expressed in (20).

$$\mathfrak{C}_t^{\mathcal{B}} = \left[\mathfrak{C}_{ij,t}^{\mathcal{B}}\right]_{\mathbb{N}\times\mathbb{N}}, t \in \mathcal{T} = \mathcal{T}^{on} \cup \mathcal{T}^{mid} \cup \mathcal{T}^{off} \tag{19}$$

$$\mathfrak{C}_{t^{on}}^{\mathcal{B},} > \mathfrak{C}_{t^{mid}}^{\mathcal{B},} > \mathfrak{C}_{t^{off}}^{\mathcal{B},}, \quad t^{on} \in \mathcal{T}^{on}, t^{mid} \in \mathcal{T}^{mid}, t^{off} \in \mathcal{T}^{off} \tag{20}$$

where $\mathcal{T}^{on}, \mathcal{T}^{mid}, \mathcal{T}^{off}$ are the sets of the on-, mid-, and off-peak time.

Further, the energy cost is calculated in a different form, either obtained or delivered, and from MG to MG and MG to main grid, as expressed in (21).

$$\mathcal{C}_{ij}^{t} = \begin{cases} M_{ii} \times \mathfrak{C}_{G,t}^{pur} & i = j,\ M_{ij} \geq 0 \\ M_{ii} \times \mathfrak{C}_{G,t}^{sell} & i = j,\ M_{ij} < 0 \\ M_{ij} \times \left(\mathfrak{C}_{ij,t}^{B} + \dfrac{\mathfrak{C}_O}{2}\right), & M_{ij} \geq 0, i \neq j\ (obtained) \\ -\dfrac{M_{ij}}{1-a_{ij}}\mathfrak{C}_{gc} + M_{ij}\mathfrak{C}_{ij,t}^{B} - M_{ij}\dfrac{\mathfrak{C}_O}{2}, & M_{ij} < 0, i \neq j\ (delivered) \end{cases} \tag{21}$$

where $\mathfrak{C}_{gc}$ (\$/kWh) is the generation cost coefficient; $\mathfrak{C}_O$ (\$/kWh) is the utilization cost coefficient of each transaction, which is the benefit of the market operator paid by the seller and buyer evenly; a_{ij} is the power loss percentage.

In this calculation, the following assumptions are taken. The trading can be done through MG to MG or MG to Grid; The trading price (\$/kWh) is dynamic according to time (on-peak, mid-peak, and off-peak); The purchasing price from the grid is greater than the TE trading price ($\mathfrak{C}_{G,t}^{pur} > \mathfrak{C}_{ij,t}^{\mathcal{B}}$); The selling price to the grid is less than the TE trading price ($\mathfrak{C}_{G,t}^{sell} < \mathfrak{C}_{ij,t}^{\mathcal{B}}$); The seller will pay the extra cost due to power loss; The market operator benefit will be calculated as per the amount of energy transactions. The price will be paid by the receiver and delivery side (half-half), as they are using the network, such as network utilization fees.

Further, the benefit of the market operator is calculated as (22). It uses the power network to trade the energy, in which the utilization fee is considered for each transaction.

$$\mathcal{C}_{\mathbb{B}_{MO},t} = \sum_{i=1}^{\mathbb{N}} \sum_{j=1, i\neq j}^{\mathbb{N}} |M_{ij,t}| \times \frac{\mathfrak{C}_O}{2} \tag{22}$$

where $\mathcal{C}_{\mathbb{B}_{MO},t}$ is the market operator benefit at time *t*.

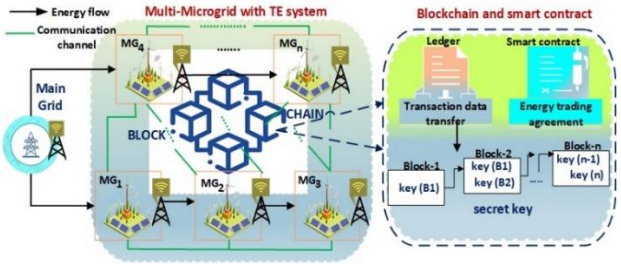


Fig. 3 Energy trading approach on Blockchain-enabled TE platform

IV. Blockchain Implementation

Blockchain defines that the data or transactions are structured in blocks, and then it links with each other like chains stored in cryptologic hash keys from one block to another, followed by the consensus protocol among the Blockchain network [27]. It brings up a top-notch technological solution for data security in terms of transparency, verifiability, and immutability. Notably, in the Blockchain, consensus protocol and smart contracts are the great players driving the technology into a resilient system [28].

The energy trading approach using Blockchain is shown in Fig. 3, where the left half of the figure implies the physical system, and the right half indicates the digital system. In the physical system, each MG is defined as a block connected to each other. In addition, the main grid is connected to each MG to support the load demand during an emergency or to meet the demand. Similarly, Blockchain is implemented in digital systems through the shared ledger, consensus protocol, and smart contracts. A homomorphic encryption scheme is implemented for the secret key generation, where public and private keys assist in trading between MGs.

A. Consensus Protocol

The consensus protocol plays a critical role in establishing the trusted path through transaction verification. Moreover, the consensus protocol deals with verification and validation followed by the linking from an old to a new block in the distributed ledger, shown in Fig. 3. This mechanism expels the role of central authorities in dealing with data authentication. Eventually, it manages peer-to-peer without any intermediatory. The implementation of the consensus protocol is to verify and validate the transaction in each stage; however, it is critically important in the final stage as private key authentication is required to start the trading process. The procedure is discussed in Algorithm 1.

B. Smart Contract

A smart contract defines a handshake between seller and buyer established by a digitally signed computer [29]. According to

the energy requirements, the operator is responsible for automatically performing the trading action in each period. The seller and buyer could respond to the bids and offers generated by the market operator regarding energy quantity and price. Then, the parties will validate the contract, which is the price and quantity of energy exchanged by all the peers in the TE market. Once it achieves the optimal pricing, the energy exchange can be done. In a smart contract, three components will be written in the agreement: energy quantity, trading price, and trading time. The trading price is not constant as it depends on the time of transfer. There will be two ways of action: for example, MG_i receives M_{ij} quantity of energy from MG_j, thereafter, the MG_i will transfer the $\mathcal{C}_{ij}$ dollars to MG_j as per the quantity of energy received. Indeed, the payment will be automatically executed and updated through ciphertext. On the other hand, computational efficiency is a vital task for large-scale systems or high-complex systems. Indeed, the computational burden for the proposed model is not high as a minimal number (5) of MG systems has been considered, and the number of transactions (trading activities) is low. However, the computational burden could be high for a large-scale complex energy system, as the smart contract needs to verify all the nodes to replicate the computation in a transaction. So, the current form of smart contract may fail to maintain computational efficiency. To deal with these challenges, a new hybrid solver pattern named TRANSAX is developed in [30], where an off-chain-based smart contract does the verification and eventually enhances computational efficiency.

C. Homomorphic Encryption Scheme

In this scheme, the plaintext and ciphertext are denoted as $\mathcal{Q}$ and $\mathbb{X}$, encryption and decryption functions are stated as $\mathcal{E}$ and $\mathcal{D}$, and public and private keys are specified as $\mathbb{K}_{pu,M_1}$ and $\mathbb{K}_{pr,M_1}$, respectively.

Plaintext = $\mathcal{Q} = \{\mathcal{U}_1, \mathcal{U}_2, \mathcal{U}_3 \ldots\ldots \mathcal{U}_n\}$

Ciphertext = $\mathbb{X} = \{\mathfrak{x}_1, \mathfrak{x}_2, \mathfrak{x}_3 \ldots\ldots \mathfrak{x}_n\}$

Key = $\mathbb{K} = \{\mathcal{k}_1, \mathcal{k}_2, \mathcal{k}_3 \ldots\ldots \mathcal{k}_n\}$

The function f is called homomorphic when it follows (23).

$$\mathcal{E}\big(f(\mathcal{u}_1, \mathcal{u}_2, \ldots\ldots \mathcal{u}_n)\big) = f\big(\mathcal{E}(\mathcal{u}_1), \mathcal{E}(\mathcal{u}_2), \ldots \mathcal{E}(\mathcal{u}_n)\big) \quad (23)$$

where n is the number of blocks.

The implementation of the homomorphic encryption method is to verify and validate the transaction in each stage. This method is categorized into four steps: key generation, data authentication (encryption and decryption function), and transaction confirmation.

Firstly, it starts with the key generation, formed according to the number of nodes (sender as a source node and receiver as destination), which are different from each other. Secondly, node identification means identifying the parties who wish to trade with each other. Then the nodes of the parties must go through the authentication (homomorphic encryption/ decryption) stage. Further, the TE nodes use the secret keys to get the authentic response. If the authentication fails, trading can't be done, and it will be assumed that there is a privacy leakage or any form of attack. Once the authentication is passed, trading (both energy and payment) can be executed automatically based on the smart contract. After the confirmation of the transaction, a new block will be created in the Blockchain, and the same process will go on.

Let us assume each MG has its own beneficiary account with a balance of $\{\mathbb{b}_1, \mathbb{b}_2, \mathbb{b}_3 \ldots\ldots \mathbb{b}_n\}$. With this account balance, the ciphertext can be defined as $\big(\mathbb{X}(\mathbb{b}_1), \mathbb{X}(\mathbb{b}_2), \ldots \mathbb{X}(\mathbb{b}_n)\big)$ and then the miner can easily estimate $\mathcal{E}\big(f(\mathcal{u}_1, \mathcal{u}_2, \ldots\ldots \mathcal{u}_n)\big)$ by $f\big(\mathcal{E}(\mathcal{u}_1), \mathcal{E}(\mathcal{u}_2), \ldots \mathcal{E}(\mathcal{u}_n)\big)$.

When the energy supplier M_1 intends to transfer energy as per the need by M_2, M_1 commences the transaction to the Blockchain. Assume that the energy available in M_1 is $\mathbb{R}_1$ and the energy trading that M_1 wants to transfer to M_2 is $\mathcal{U}_1$. Then the secured energy trading actions can be performed through the homomorphic encryption scheme in three steps are discussed as follows [20].

Algorithm 1: Blockchain-Enabled TE trading algorithm

Initialization
for MG i=1, $\mathbb{N}$ **do**
  With a homomorphic encryption algorithm, MG i generates a public key $\mathbb{K}_{pu}$ as the digital signature receipts and private key $\mathbb{K}_{pr}$ as the digital signature to confirm the transaction. Then, they are stored in the Blockchain ledger.
end for
for MG i=1, $\mathbb{N}$ **do**
  MG i solves an optimization problem to minimize the total cost ($min\ C_{MG,i}$).
  MG i obtains the optimal energy trading quantity $M_{ij}(t)$ with MG j ($j \neq i$) and the Grid ($j = i$).
end for
for time step $t = 1, T$ **do**
  for MG i=1, $\mathbb{N}$ **do**
    MG i generates the proposed optimal trading quantity $M_{ij}(t)$ with MG j using public-key $\mathbb{K}_{pu}$.
    The information is sent to the Blockchain.
  end for
  The Blockchain miner is responsible to verify the transactions that are delivered by each MG.
  $\begin{cases} if\ M_{ij} = -M_{ji}, \text{verification passes, process the transactio} \\ else, \text{ verification fails, ignore the transaction} \end{cases}$
  The verified transaction will generate a new block and enter the Blockchain. The balance transfer will be automatically triggered for verified transactions.
end for

Step-1: Key generation: Assume that there are two random prime numbers chosen by M_1 and M_2, such as $\mathfrak{z}_{\mathbb{i}}$ and $\mathfrak{y}_{\mathbb{i}}$, $\mathbb{i} = 1,2 \ldots$ and compute $\mathbb{Z}_{\mathbb{i}}$ and $\mathbb{K}_{\mathbb{i}}$, as in (24), and (25), respectively.

$$\mathbb{Z}_{\mathbb{i}} = \mathfrak{z}_{\mathbb{i}} \cdot \mathfrak{y}_{\mathbb{i}} \quad (24)$$

$$\mathbb{K}_{\mathbb{i}} = \mathbb{L}(\mathfrak{z}_{\mathbb{i}} - 1, \mathfrak{y}_{\mathbb{i}} - 1), \mathbb{i} = 1,2 \ldots \quad (25)$$

Again, M_1 and M_2 choose another integer randomly as $\mathfrak{g}_{\mathbb{i}} = \mathcal{R}^*_{\mathbb{Z}^2}$, $\mathbb{i} = 1,2 \ldots$, which must satisfy (26).

$$\mathbb{G}\left(\frac{\mathfrak{g}_{\mathbb{i}}^{\mathfrak{T}_{\mathbb{i}}} \bmod \mathbb{Z}_{\mathbb{i}}^2 - 1}{\mathbb{Z}_{\mathbb{i}}}, \mathbb{Z}_{\mathbb{i}}\right) = 1 \quad (26)$$

where $\mathbb{Z}$ is the modulus, $\mathbb{K}$ is the key, $\mathbb{L}$ and $\mathbb{G}$ are the lowest common multiple and greatest common factor, respectively, $\mathcal{R}_{\mathbb{Z}^2}$ is the set of integers that is lower than $\mathbb{Z}^2$ and $\mathcal{R}^*_{\mathbb{Z}^2}$ is the set of integers co-prime with $\mathbb{Z}^2$.

Let the public and private keys of M_1 and M_2 be stated as (27) and (28).

$$\mathbb{K}_{pu,M_1} = (\mathbb{Z}_1, \mathfrak{g}_1), \text{ and } \mathbb{K}_{pr,M_1} = \mathbb{K}_1 \quad (27)$$

$\mathbb{K}_{pu,M_2} = (\mathbb{Z}_2, \mathfrak{g}_2)$, and $\mathbb{K}_{pr,M_2} = \mathbb{K}_2$ (28)

Step-2: Encryption phase:

In this stage, data encryption is done through ciphertext. The sender (M_1) randomly chooses the encryption parameter, such as $\mathfrak{P}_{1\mathcal{U}} \in \mathcal{R}_{\mathbb{Z}}^*$. Then it encrypts $\mathcal{U}_1$ by $\mathbb{K}_{pu,M_1} = (\mathbb{Z}_1, \mathfrak{g}_1)$ to derive the ciphertext, expressed in (29). Further M_1 selects another encryption parameter randomly as $\mathfrak{P}_{2\mathcal{U}} \in \mathcal{R}_{\mathbb{Z}}^*$ and then it encrypts $\mathcal{U}_2$ by $\mathbb{K}_{pu,M_2} = (\mathbb{Z}_2, \mathfrak{g}_2)$ to derive the ciphertext, expressed in (30).

$$\mathbb{X}_{1\mathcal{U}} = \mathcal{E}_1(\mathcal{U}_1) = \mathfrak{g}_1^{\mathcal{U}_1} \cdot \mathfrak{g}_{1\mathcal{U}}^{\mathbb{Z}_1} \mod \mathbb{Z}_1^2 \quad (29)$$

$$\mathbb{X}_{2\mathcal{U}} = \mathcal{E}_2(\mathcal{U}_2) = \mathfrak{g}_2^{\mathcal{U}_2} \cdot \mathfrak{g}_{2\mathcal{U}}^{\mathbb{Z}_2} \mod \mathbb{Z}_2^2 \quad (30)$$

The above two ciphertexts are derived from the randomness of $\mathfrak{P}$ with the same energy transaction $\mathcal{U}$, and then it can be decrypted with the same $\mathcal{U}$. Thus, M_1 needs to prove to the miner that the plaintext data of the ciphertext $\mathbb{X}_{1\mathcal{U}}$, $\mathbb{X}_{2\mathcal{U}}$ are equal.

Step-3: Decryption phase

The ciphertext is the encrypted text that needs to be decrypted using a private key to validate the transaction and energy transfer. Suppose that $\mathbb{Z}_1 = \mathbb{Z}_2$ and private keys for M_1 and M_2 are $\mathbb{K}_1$ and $\mathbb{K}_2$, and the decryption can be done using (31).

$$\mathcal{U}_{\mathbb{i}} = \mathcal{D}(\mathbb{X}_{\mathbb{i}\mathcal{U}}) = \frac{F(\mathbb{X}_{\mathbb{i}\mathcal{U}}^{\mathbb{K}_{\mathbb{i}}}) \bmod \mathbb{Z}^2}{F(\mathfrak{g}_{\mathbb{i}}^{\mathbb{K}_{\mathbb{i}}}) \bmod \mathbb{Z}^2} \bmod \mathbb{Z} \quad (31)$$

where $F(\mathbb{a}) = \frac{\mathbb{a}-1}{\mathbb{Z}}$, $\mathcal{U}_1 = \mathcal{U}_2 = \mathcal{U}$. In this case, the below properties are to be followed [31].

Property-1: $\forall \mathcal{U}_1, \mathcal{U}_2 \in \mathcal{R}_{\mathbb{Z}}$

$$\mathcal{D}(\mathcal{E}(\mathcal{U}_1) \cdot \mathcal{E}(\mathcal{U}_2) \mod \mathbb{Z}^2) = (\mathcal{U}_1 + \mathcal{U}_2) \mod \mathbb{Z} \quad (32)$$

Property-2: $\forall \mathcal{U} \in \mathcal{R}_{\mathbb{Z}}$

$$\mathcal{D}\left(\mathcal{E}(\mathcal{U})^{\hbar} \mod \mathbb{Z}^2\right) = \hbar\mathcal{U} \mod \mathbb{Z} \quad (33)$$

Step-4: Transaction confirmation

As per the aforementioned process, the homomorphism of the cryptographic system is used to certify the miner that the ciphertexts $\mathbb{X}_{1\mathcal{U}}$ and $\mathbb{X}_{2\mathcal{U}}$ comprise the identical plaintext records, which then validate the transaction's authority, ensuring trading security. The detailed discussion of the authentication process is summarized as follows.

Authentication process

1. ***Initialization:***
   - 1.1 Take $\mathcal{J}$ as the safety parameter
   - 1.2 M_1 generates random number $\rho_{\mathbb{i}}$
   - 1.3 Estimate $\mathcal{U}_1 + \rho_{\mathbb{i}}$, where $1 \le \mathbb{i} \le \mathcal{J}$
   - 1.4 Assume $\mathcal{Q}_{1\mathbb{i}} = \mathcal{E}_1(\rho_{\mathbb{i}})$, $\mathcal{Q}_{2\mathbb{i}} = \mathcal{E}_2(\rho_{\mathbb{i}})$ where $1 \le \mathbb{i} \le \mathcal{J}$
   - 1.5 Addition of homomorphic by the public key (M_1). $\mathcal{U}_{1\mathbb{i}} = \mathbb{X}_{1\mathcal{U}} + \mathcal{Q}_{1\mathbb{i}}$, $1 \le \mathbb{i} \le \mathcal{J}$
   - 1.6 Addition of homomorphic by the public key (M_2). $\mathcal{U}_{2\mathbb{i}} = \mathbb{X}_{2\mathcal{U}} + \mathcal{Q}_{2\mathbb{i}}$, $1 \le \mathbb{i} \le \mathcal{J}$
2. ***Process:***
   - 2.1 M_1 sends the required parameters to Blockchain, such as $\mathbb{X}_{1\mathcal{U}}, \mathbb{X}_{2\mathcal{U}}, \mathcal{Q}_{1\mathcal{U}}, \mathcal{Q}_{2\mathcal{U}}, \mathcal{U}_{1\mathbb{i}}$, and $\mathcal{U}_{2\mathbb{i}}$.
   - 2.2 Miner sends a string Ξ to M_1, $\Xi_{\mathbb{i}} \in \{0,1\}$
   - 2.3 When M_1 receives Ξ,
     if $\Xi_{\mathbb{i}} = 0$,
     M_1 sends $\rho_{\mathbb{i}}$ of $\mathcal{Q}_{1\mathbb{i}}$,$\mathcal{Q}_{2\mathbb{i}}$, and $\mathfrak{P}_{1\mathbb{i}}$, $\mathfrak{P}_{2\mathbb{i}}$ to miners.
     if $\Xi_{\mathbb{i}} = 1$,
     M_1 sends $\mathcal{U}_1 + \rho_{\mathbb{i}}$ of $\mathcal{U}_{1\mathbb{i}}$, $\mathcal{U}_{2\mathbb{i}}$ and $\mathfrak{P}_{1\mathcal{U}} + \mathfrak{P}_{1\mathbb{i}}$,$\mathfrak{P}_{2\mathcal{U}} + \mathfrak{P}_{2\mathbb{i}}$ to miners.
3. When verification is passed, miners accept the transaction; otherwise, decline the transaction.

V. Results and Discussion

In this section, the verification of the proposed TE framework is presented with four different scenarios: such as, Case-1 is the base case where no TE framework is considered; in Case-2, the proposed TE framework is implemented; in Case-3, the TE framework with MG outage condition is investigated; and finally, in Case-4, the Blockchain technology is applied to show the effectiveness of the system through the premise of success probability using various FDI attack.

In the proposed model, the market operator maintains the energy balance of the whole system through optimal energy trading between MGs and grid supply. The main objective of this framework is to minimize the overall energy cost and helps to benefit each MG in terms of selling surplus energy to other MGs or Grid, which are illustrated in Figs. 6-9. In this simulation, the cost has been estimated in 24 hours of duration in three time-of-use periods such as on-peak (6-9 hrs, and 18-21hrs), mid-peak (10-17hrs), and off-peak time (22-5 hrs), and the prices are also varied accordingly.

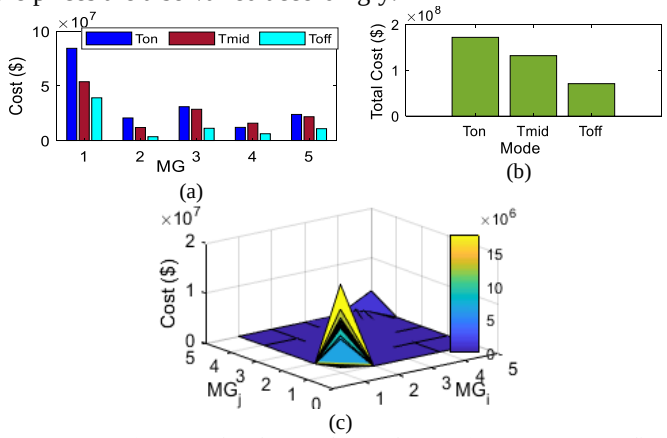


Fig. 4. Case-1: (a) Cost of each MG, (b) Total cost, (c) MGs' energy trading cost

$$\mathcal{C}_{ij}^t = \begin{bmatrix} 1569.1 & 0 & 0 & 0 & 0 \\ 0 & 338.6 & 0 & 0 & 0 \\ 0 & 0 & 629.3 & 0 & 0 \\ 0 & 0 & 0 & 326.4 & 0 \\ 0 & 0 & 0 & 0 & 509.9 \end{bmatrix}_{5\times5} \times 10^5 \quad (C.1)$$

A. Case-1: Base case (Without TE trading mechanism)

In this case, the load demand has been met through the MG's own generation and grid supply. Thus, the following objective function is considered, expressed in (34), where the interconnection of MGs is not assumed.

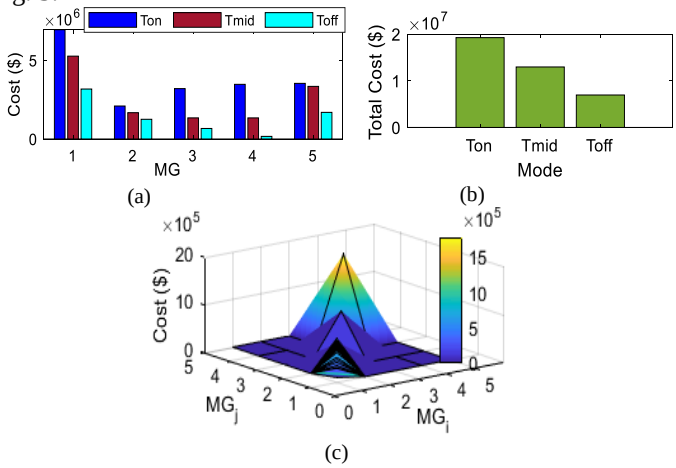
$$Min\ \mathcal{C}_i^{WT} = \sum_{t \in \mathcal{T}} \mathcal{C}_{i,t}^{WT} \quad i \in N, t \in \mathcal{T} \quad (34)$$

where $\mathcal{C}_i^{WT}$ is the energy cost of MG i without the TE framework and $\mathcal{C}_{i,t}^{WT} = \begin{cases} M_{ii,t} \times \mathfrak{C}_{G,t}^{pur} & M_{ii,t} \ge 0 \\ M_{ii,t} \times \mathfrak{C}_{G,t}^{sell} & M_{ii,t} < 0 \end{cases}$

As can be seen from Fig. 4, the cost of most MGs (MG_1, MG_2, MG_3, MG_5) is high (Fig. 4 (a)) at the on-peak compared to mid-peak and off-peak time, and subsequently, the overall cost is also high at the on-peak time (see Fig. 4 (b)). In this case, the MGs only trade the energy with the grid, and the cost of trading energy can be seen in Fig. 4 (c). In addition, to better understand the energy trading cost of MG_i and MG_j, a matrix $[\mathcal{C}_{ij}^t]_{5\times5}$ is presented above in (C.1). It is evident that only MG has traded with the main grid, and no trading activity is done between the MGs, as this case study does not consider the TE framework. The trading cost between each MG and the main grid can be seen in $[\mathcal{C}_{ij}^t]_{5\times5}$. From the matrix, it is clear that the MGs only trade with the main grid, and the costs between MGs to the main grid are $\mathcal{C}_{11}^t$, $\mathcal{C}_{22}^t$, $\mathcal{C}_{33}^t$, $\mathcal{C}_{44}^t$, and $\mathcal{C}_{55}^t$, and other elements in the matrix are zero.

B. Case-2: With TE framework

In this case, the proposed TE framework has been implemented, and the overall energy cost and each MG benefit are optimized. As can be seen from Fig. 5, the cost of each MG is high (Fig. 5 (a)) at the on-peak compared to mid and off-peak time, and subsequently, the overall cost is also high at the on-peak time (see Fig. 5 (b)). The trading energy cost between the MGs can be seen in Fig. 5 (c). It is noted that, compared to Case-1, the energy cost is reduced significantly in Case-2, as illustrated in Fig. 5.



(a) (b) (c)

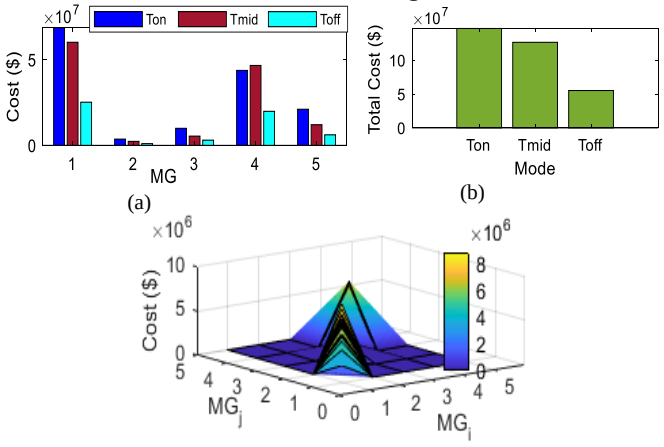
Fig. 5. Case-2: (a) Cost of each MG, (b) Total cost, (c) MGs' energy trading cost

$$\mathcal{C}_{ij}^t = \begin{bmatrix} 1469.4 & -1.3483 & 0.350 & 0.642 & -0.650 \\ 1.9594 & 490.72 & -0.552 & 0.396 & -0.357 \\ -1.3787 & 0.744 & 507.57 & 0.7652 & -1.0792 \\ -0.340 & 0.878 & 0.0136 & 493.68 & -0.505 \\ -2.627 & 0.892 & 1.5856 & 1.779 & 823.42 \end{bmatrix}_{5\times5} \times 10^4 \quad \text{(C.2)}$$

Further, Fig. 5 (c) shows the energy trading cost performed by the TE framework, and the corresponding cost is calculated in (C.2). The cost matrix, $[\mathcal{C}_{ij}^t]_{5\times5}$, represents the selling and purchasing activities in the TE system, denoted as +ve and -ve, respectively. As the TE market is operating all the activities to perform optimal trading, and for that, the operator should get the benefit, which is calculated using (22), and the estimated value is $\$1.26 \times 10^4$.

C. Case-3: With TE framework and resiliency

This study considers the resilience-based approach where two MGs are taken as outage conditions. As per the load demand profile based on (15), a minimum of 30% of the load needs to be served, as it is considered a critical load, and then the minimum level of resilience (0.3) can be maintained. With this objective, energy trading has been done with the healthy MGs and the main grid. It can be observed that the proposed TE framework achieves the minimum resilience level and restores the critical load optimally. As shown in Fig. 6, the overall cost of the TE system cost is considerably higher than Case-2, but it is smaller than Case-1, even considering the extreme events.

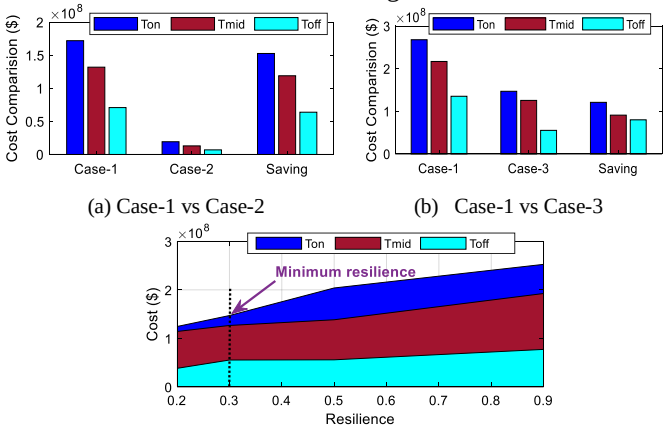


(a) (b) (c)

Fig. 6. Case-3: (a) Cost of each MG, (b) Total cost, (c) MGs' energy trading cost

$$\mathcal{C}_{ij}^t = \begin{bmatrix} 1539.2 & 2.8519 & -0.3833 & -3.9435 & -0.561 \\ 0 & 69.9 & 0 & 0 & 0 \\ 0 & 0 & 183.8 & 0 & 0 \\ -0.742 & -0.218 & 6.015 & 1102.1 & 1.725 \\ 3.1662 & 0.0317 & -0.452 & 0.447 & 392.9 \end{bmatrix}_{5\times5} \times 10^5 \quad \text{(C.3)}$$

As can be seen from Fig. 6 (c), no trading activity is done in MG_2 and MG_3, and they only receive power from the main grid, as these two MGs are in outage condition, assuming as generation is zero. The cost matrix, $[\mathcal{C}_{ij}^t]_{5\times5}$ in (C.3), represents the selling and purchasing activities. In addition, the benefit of the market operator is $\$0.784 \times 10^4$. This value is low compared to Case-2, as two MGs have an outage with fewer transactions.



(a) Case-1 vs Case-2 (b) Case-1 vs Case-3

(c) Cost vs resilience

Fig. 7. Cost comparison and resilience characteristics

In addition to the above analysis, the cost comparison with Case -1 & 2 and Case-1 & 3 are depicted in Fig. 7 (a) and (b), respectively. It is observed that using TE technology in the existing system can save \$288.17M. While considering the resiliency of the TE system, it saves \$46.6M. Notably, Fig. 7 (b) reveals that if any high-disruptive event happens in Case-1,

the cost can be exceptionally high because the outage MGs should purchase the power from the main grid, which has a high trading price compared to other MG's prices. Henceforth, the overall cost is reduced using the TE framework even after the outage happens.

Fig. 7 (c) demonstrates the cost versus resilience, which needs to be a trade-off. The minimum resilience 30% is considered here as it is assumed as the critical load. The resiliency can be improved, but the cost would be very high due to MG outage conditions. During the event, the available MG has no sufficient capacity to meet all the load demand; eventually, the unmet demand can be bought from the grid, which increases the cost significantly.

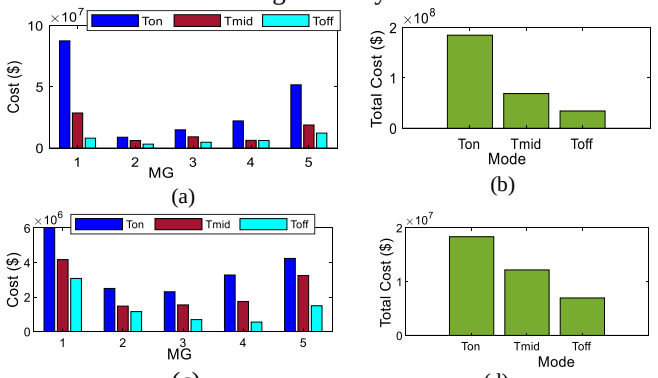


Fig. 8. Cost comparison: (a) Cost of each MG (without Blockchain), (b) Total cost (without Blockchain), (c) Cost of each MG (with Blockchain), (d) Total cost (with Blockchain)

D. Case-4: TE framework and Blockchain

There are many types of attacks possible in the TE system by cyberpunk; however, the FDI attack is well known. The FDI attack can be shot into the system by three ways of data falsification, such as at the sender side (prior to data transfer), the transmission path (data in transmission), and the receiver side (after the data are received) [32]. This can be done using the meters used in the network or falsifying the control center's data. All the FDI attacks are considered in this study with and without the application of Blockchain as scenario-1 and scenario 2, respectively. Indeed, to show the effectiveness of security operations using the homomorphic-based Blockchain technique against FDI, the success probability of an attack is estimated. When the FDI attack is applied to the TE system, it is observed that the cost of each MG and the overall cost are exceptionally high, which can be seen in Fig. 8 (a) & (b). Since the energy cost is remarkably high, which does not meet the objective of the proposed TE framework, it needs to be revamped through advanced technology. With the implementation of Blockchain, the cost has been reduced significantly, as seen in Figs. 8 (c) & (d). Further, the benefit of the market operator is calculated using (22), and the estimated value is $\$1.2754 \times 10^4$.

With this concern, state-of-the-art technology such as Blockchain is applied and studied in scenario 2. While considering the security operation against the attack, the probability of success illustration is vital, showing the attack-defensive mechanism of the proposed system, which is discussed as follows.

Three cases have been considered: data manipulation can be done pre, during, and after the data transfer.

Assumption 1: Data manipulation in pre-transmission: it is assumed that the attacker has hacked h sensors before data transmission and then manipulated the sensor's key information.

Assumption 2: Data manipulation during transmission: it is assumed that the attacker has hacked K pairs of channels during data transmission and manipulated the sensor's key information.

Assumption 3: Data manipulation after transmission: it is assumed that the attacker has hacked h sensors after data transmission and then manipulated the sensor's key information.

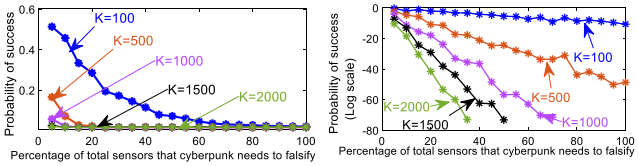


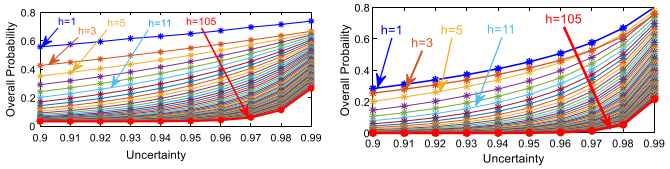
Fig. 9. Probability of successful attacks comparison

Let us assume there are 105 sensors used in the TE system to collect the data, such as voltage, current, frequency, power, etc. With these 105 sensors, there are $105 \times (105-1)/2 = 5460$ communication channels established, as derived in [23]. Cyberpunk can hack sensor data and try to steal critical information to launch a fruitful attack. Therefore, the probability of a successful attack is measured in this study with and without Blockchain technology. The same concept of successful attack probability is used in [23]. In scenario 1, it is assumed that the TE system has no private key for each node, and then the cyberpunk has made the attack on K communication channels. In scenario 2, it is assumed that each transaction has a secret key with encryption and decryption techniques, and then the FDI attack is applied. Further, a Monte Carlo method is used to generate random draws to show the best comparison in terms of short to long variation (in this study, increasing the number of communication channels is considered). The success probability of scenarios 1 and 2 with various K (attacked communication channels) values in [1, 5460] is presented in Fig. 9. Further, Figs. 9 (a) and (b) represent the probability of success for scenarios 1 and 2, respectively. In scenario 1, the probability of success is high in the context of data falsification by cyberpunk, which can dramatically affect the system, leading to an outage. However, in scenario 2, after implementing Blockchain in the proposed model, the probability of success significantly decreases to less than 0.01. To better understand the probability of success, a natural logarithm scale is taken on the y-axis. Although the y-axis shows a negative value, that does not mean the probability is less than zero. Indeed, the natural logarithm scale signifies the probability is very low as compared to scenario 1, which means the successful attack is almost negligible. This indicates that the robustness and defensive capability of Blockchain technology are tremendous and less likely to be affected by hackers or other cyber-related issues on account of data falsification.

In addition, in Fig. 9 (a), it is reported that the probability of success decreases as the number of sensors that need to be hacked increases. Data manipulation has been done through

communication channels with steps such as 5% to 100% of K value, where K has been set to 100, 500, 1000, and 1500 for comparative analysis. On the other hand, Fig. 9 (b) reveals the attack-defensive capability using Blockchain, reducing the probability of success.

Further, the overall probability is measured by considering the scenario where the system is assumed to be very weak with the successful attacking probability for the attacker in the range of [0.9, 0.99], and the probabilities of all three ways of data falsification (sender side, transmission path, receiver side) are assumed to be equal. In addition, uncertainty is considered here, which is the combination of the probability of cyberpunk in three ways of attack. As shown in Fig. 10, the number of sensors that need to be hacked (h) and uncertainty are considered variables, and it is observed that when a cyberpunk has a definite proportion of falsification data with less sensors, the overall probability of success is high, as can be seen in Fig. 10 (a), whereas, with the Blockchain in scenario 2, the overall probability of success is low, as shown in Fig 10 (b). Moreover, with fewer sensors, the probability of successful attacks is higher, as it is easy to duplicate the data in the sensors and channels. It is noticed that a Blockchain-enabled TE system provides a highly secure platform for trading energy as well as payment operations.



(a) Scenario 1 (b) Scenario 2

Fig. 10. Overall probability of successful attacks and its defensive capability

As can be seen from TABLE 1 and TABLE 2, it is evident that the proposed framework offers an optimal and secure framework solution to the TE system. A detailed comparison study is highlighted below.

- Considering an outage in Case 1, the energy cost has been increased significantly, and to reduce that, the TE framework with a resilient approach is implemented in Case 3. It is noticed that the proposed TE model saved energy costs up to 47% (see TABLE 1: comparing two cases: Case 1(with outage: 2.6804×10^8) and Case 3 (1.470×10^8)). However, in the literature, the energy cost can only be saved up to 15-20% in [3] and 24 % in [13] by using the TE mechanism.
- Further, taking attack into consideration, Blockchain with homomorphic encryption is implemented, and it offers a better defense mechanism in the TE framework (see TABLE 2). As can be noted, the application of Blockchain provides a low probability of success on account of the attack, enhancing the system's security. From TABLE 2, the probability of success for scenario 1 in [22] is 0.66 and 0.53 for K=100 & 500, respectively, whereas the proposed method has less probability as 0.54 and 0.18, respectively. Similarly, other probability comparisons are reported in TABLE 2 to show the better performance of the proposed method.

TABLE 1: COST COMPARISON ANALYSIS

Case	Cost ($)	On-peak (×108)	Mid-peak (×108)	Off-peak (×108)
Case 1	Without outage	1.7204	1.320	0.7090
	With outage	2.6804	2.170	1.353
Case 2		0.1925	0.1297	0.0695
Case 3		1.470	1.256	0.5526
Case 4	Attack without BC	1.910	0.793	0.3436
	Attack with BC	0.18329	0.12165	0.0695

(BC: Blockchain)

TABLE 2: BLOCKCHAIN PERFORMANCE COMPARISON

Indices	Scenario-1	Scenario-2	Method
Probability of success	0.66 (K=100)	Range: 0-(-25) at (K=100-20000)	[22]
	0.53 (K=500)		
	0.54 (K=100)	Range: 0-(-80) at (K=100-2000)	Proposed method
	0.18 (K=500)		
Overall probability	0.61 (h=1)	0.28 (h=1)	[22]
	0.578(h=1)	0.253 (h=1)	Proposed method

VI. CONCLUSION

This paper presents a Blockchain-empowered TE framework for improving privacy preservation and energy security against cyber threats. The proposed scheme greatly enhances the overall energy cost-saving, and each MG benefits from using the bilateral trading pricing mechanism. In addition, implementing Blockchain into the TE system shows a remarkable achievement when it faces cyber-attacks. Various operational case studies are demonstrated with the inclusion of extreme events such as MG outage conditions and FDI attacks, and in both cases, the proposed system has shown its defensive capabilities. The effectiveness of the proposed system is verified with resiliency versus cost trade-off in Case-3 and the probability of successful attacks in Case-4.

In a nutshell, the resilience-based TE framework has a renowned interest in this paper, where the various distinguishing characteristics appealing to the current needs of the energy market have been shown. The results outlined that the proposed TE platform provides better economical operation to the operator and energy providers. In addition, with the Blockchain, the whole system can be regarded as a promising solution for economic and secure operations for the TE scheme.

An efficient decentralized-based TE scheme with a large-scale system and renewable energy uncertainties will be studied in future work. In addition, the breakthrough of Blockchain with more favorable features is to be implemented in the TE scheme, such that it could follow the industrial revolution in the energy sector.

VII. ~~APPENDIX~~ APPENDIX (A)

A1: System parameters:

Resources	MG1 (kW)	MG2 (kW)	MG3 (kW)	MG4 (kW)	MG5 (kW)
Solar	200	250	200	400	350
Wind	250	300	350	500	400
Battery	200	250	200	300	300

A2: POWER LOSS PERCENTAGE

$$a_{ij} = \begin{vmatrix} 0.04 & 0.01 & 0.015 & 0.04 & 0.045 \\ 0.01 & 0.04 & 0.015 & 0.03 & 0.015 \\ 0.025 & 0.015 & 0.04 & 0.025 & 0.03 \\ 0.04 & 0.03 & 0.025 & 0.04 & 0.015 \\ 0.045 & 0.015 & 0.03 & 0.015 & 0.04 \end{vmatrix}$$

A3: ENERGY PRICE DURING ON-PEAK, MID-PEAK, AND OFF-PEAK HOURS

$$\mathfrak{C}^{\mathcal{B},}_{t^{on\_peak}} = \begin{vmatrix} 0.31 & 0.216 & 0.226 & 0.223 & 0.214 \\ 0.21 & 0.30 & 0.199 & 0.187 & 0.219 \\ 0.23 & 0.21 & 0.312 & 0.21 & 0.214 \\ 0.22 & 0.198 & 0.21 & 0.315 & 0.234 \\ 0.20 & 0.198 & 0.197 & 0.219 & 0.309 \end{vmatrix}$$

$$\mathfrak{C}^{\mathcal{B},}_{t^{mid\_peak}} = \begin{vmatrix} 0.278 & 0.181 & 0.189 & 0.179 & 0.19 \\ 0.18 & 0.279 & 0.179 & 0.178 & 0.179 \\ 0.189 & 0.187 & 0.281 & 0.186 & 0.18 \\ 0.177 & 0.176 & 0.179 & 0.283 & 0.175 \\ 0.184 & 0.180 & 0.189 & 0.187 & 0.272 \end{vmatrix}$$

$$\mathfrak{C}^{\mathcal{B},}_{t^{off\_peak}} = \begin{vmatrix} 0.25 & 0.15 & 0.157 & 0.159 & 0.154 \\ 0.147 & 0.254 & 0.146 & 0.141 & 0.143 \\ 0.146 & 0.139 & 0.253 & 0.147 & 0.148 \\ 0.14 & 0.139 & 0.138 & 0.257 & 0.149 \\ 0.15 & 0.156 & 0.144 & 0.148 & 0.259 \end{vmatrix}$$

$$\mathfrak{C}^{sell}_{G,t} = \{0.12 \quad flat\ rate\ for\ all\ the\ time$$

$$\mathfrak{C}_O = 0.05\ \$/\text{kWh}$$

VIII. REFERENCES

[1] Y. Cao *et al.*, "Optimal Energy Management for Multi-Microgrid Under a Transactive Energy Framework With Distributionally Robust Optimization," *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 599-612, 2021.

[2] S. D. Rodrigues and V. J. Garcia, "Transactive energy in microgrid communities: A systematic review," *Renewable and Sustainable Energy Reviews*, vol. 171, p. 112999, 2023.

[3] H. Hao, C. D. Corbin, K. Kalsi, and R. G. Pratt, "Transactive control of commercial buildings for demand response," *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 774-783, 2016.

[4] Y. K. Renani, M. Ehsan, and M. Shahidehpour, "Optimal transactive market operations with distribution system operators," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6692-6701, 2017.

[5] M. S. H. Nizami, M. J. Hossain, and E. Fernandez, "Multiagent-based transactive energy management systems for residential buildings with distributed energy resources," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1836-1847, 2019.

[6] Y. Zou, Y. Xu, and C. Zhang, "A risk-averse adaptive stochastic optimization method for transactive energy management of a multi-energy microgrid," *IEEE Transactions on Sustainable Energy*, 2023.

[7] M. N. Akter, M. A. Mahmud, and A. M. Oo, "A hierarchical transactive energy management system for microgrids," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 2016: IEEE, pp. 1-5.

[8] S. M. Sajjadi, P. Mandal, T.-L. B. Tseng, and M. Velez-Reyes, "Transactive energy market in distribution systems: A case study of energy trading between transactive nodes," in *2016 North American Power Symposium (NAPS)*, 2016: IEEE, pp. 1-6.

[9] G. Prinsloo, A. Mammoli, and R. Dobson, "Customer domain supply and load coordination: A case for smart villages and transactive control in rural off-grid microgrids," *Energy*, vol. 135, pp. 430-441, 2017.

[10] C. Zhang, J. Wu, Y. Zhou, M. Cheng, and C. Long, "Peer-to-Peer energy trading in a Microgrid," *Applied Energy*, vol. 220, pp. 1-12, 2018.

[11] H. Hui *et al.*, "A transactive energy framework for inverter-based HVAC loads in a real-time local electricity market considering distributed energy resources," *IEEE Transactions on Industrial Informatics*, 2022.

[12] Y. Lu, J. Lian, M. Zhu, and K. Ma, "Transactive Energy System Deployment over Insecure Communication Links," *IEEE Transactions on Automation Science and Engineering*, 2023.

[13] Q. Yang and H. Wang, "Blockchain-empowered socially optimal transactive energy system: Framework and implementation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3122-3132, 2020.

[14] C. Barreto and X. Koutsoukos, "Attacks on electricity markets," in *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2019: IEEE, pp. 705-711.

[15] U. Cali, C. Lima, X. Li, and Y. Ogushi, "DLT/blockchain in transactive energy use cases segmentation and standardization framework," in *2019 IEEE PES Transactive Energy Systems Conference (TESC)*, 2019: IEEE, pp. 1-5.

[16] S. Saha, N. Ravi, K. Hreinsson, J. Baek, A. Scaglione, and N. G. Johnson, "A secure distributed ledger for transactive energy: The Electron Volt Exchange (EVE) blockchain," *Applied Energy*, vol. 282, p. 116208, 2021.

[17] S. Farshidi, S. Jansen, S. España, and J. Verkleij, "Decision support for blockchain platform selection: Three industry case studies," *IEEE transactions on Engineering management*, vol. 67, no. 4, pp. 1109-1128, 2020.

[18] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1-32, 2014.

[19] E. Münsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *2017 IEEE conference on control technology and applications (CCTA)*, 2017: IEEE, pp. 2164-2171.

[20] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Y. Zomaya, "Circuit copyright blockchain: blockchain-based homomorphic encryption for IP circuit protection," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1410-1420, 2020.

[21] M. R. Hamouda, M. E. Nassar, and M. Salama, "A novel energy trading framework using adapted blockchain technology," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2165-2175, 2020.

[22] M. Gough *et al.*, "Blockchain-based transactive energy framework for connected virtual power plants," *IEEE Transactions on Industry Applications*, vol. 58, no. 1, pp. 986-995, 2021.

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

[24] J. Dong *et al.*, "Integrating transactive energy into reliability evaluation for a self-healing distribution system with microgrid," *IEEE Transactions on Sustainable Energy*, vol. 13, no. 1, pp. 122-134, 2021.

[25] K. Kaur, G. Kaddoum, and S. Zeadally, "Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5178-5189, 2021.

[26] R. Ambrosio, "Transactive energy systems," *IEEE Electrification Magazine*, vol. 4, no. 4, pp. 4-7, 2016.

[27] J. Kempf, P. Heitmann, and U. Cali, "The IEEE Blockchain Transactive Energy Demo Initiative," in *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)*, 2022: IEEE, pp. 1-6.

[28] A. Shukla, P. Mathuria, R. Bhakar, and S. Sharma, "An Implementation of a Socially Adaptive Blockchain-Based Transactive Energy System," in *2023 IEEE PES Conference on Innovative Smart Grid Technologies-Middle East (ISGT Middle East)*, 2023: IEEE, pp. 1-5.

[29] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266-2277, 2019.

[30] S. Eisele *et al.*, "Blockchains for transactive energy systems: opportunities, challenges, and approaches," *Computer*, vol. 53, no. 9, pp. 66-76, 2020.

[31] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM Journal on computing*, vol. 43, no. 2, pp. 831-871, 2014.

[32] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, 2016.