A Blockchain-enabled Cyber-resilient Trading Framework for Virtual Power Plants

Yanjia Wang, *Graduate Student Member*, *IEEE*, Han Zhong, Alexis P. Zhao, *Member*, *IEEE*, Mohannad Alhazmi, *Member*, *IEEE*, Da Xie, *Senior Member*, *IEEE*, and Xitian Wang, *Member*, *IEEE*

***Abstract*—The rapid expansion of distributed energy resources (DERs) has driven the emergence of virtual power plants (VPPs) as decentralized energy trading platforms that enhance grid flexibility and market efficiency. However, the increasing reliance on digital infrastructure has exposed VPP transactions to cyber-threats such as double-spending attack, Sybil attack, smart contract tampering, and malicious data injection attack, undermining transaction integrity and market stability. Traditional cybersecurity mechanisms, which often rely on centralized verification, are vulnerable to single points of failure and lack adaptive defense strategies. To address these challenges, this paper proposes a blockchain-enabled cyber-resilient trading framework that integrates game-theoretic smart contract optimization, Byzantine fault tolerance (BFT) consensus mechanisms, and zero-knowledge proof (ZKP) authentication to enhance cybersecurity, efficiency, and privacy in VPP transactions. The proposed framework leverages a multi-layered cybersecurity approach where game-theoretic modeling ensures optimal cybersecurity investment by balancing transaction efficiency and cybersecurity costs. A Stackelberg game modeling models the interactions among prosumers, VPP aggregators, and cyber attackers, allowing the system to allocate cybersecurity resources strategically. ZKP authentication ensures that transactions are validated without exposing sensitive trading information, mitigating privacy risks while maintaining transparency. To enhance resilience, a reinforcement learning-based adaptive defense mechanism continuously optimizes cybersecurity policies against evolving cyber-threats, improving attack detection and mitigation efficiency. The proposed framework incorporates multi-signature validation and BFT consensus mechanisms to prevent unauthorized modifications, while smart contracts autonomously execute transactions under predefined cybersecurity policies.**

***Index Terms*—Blockchain, resilience, virtual power plant (VPP), smart contract, zero-knowledge proof (ZKP), cybersecurity energy transaction, reinforcement learning.**

I. Introduction

THE rapid proliferation of distributed energy resources (DERs) has fundamentally reshaped the landscape of modern energy markets, fostering the emergence of virtual power plants (VPPs) as a pivotal mechanism for aggregating and coordinating decentralized energy assets [1], [2]. By leveraging advanced digital platforms, VPPs enable the seamless integration of prosumers into energy trading ecosystems, facilitating real-time market participation, optimizing grid stability, and enhancing overall system flexibility [3]. However, as VPPs rely extensively on cyber-physical infrastructure for decentralized energy transactions, they have become prime targets for sophisticated cyber-threats [4], [5]. Attacks such as double-spending attack, Sybil attack, smart contract tampering, and malicious data injection attack pose severe risks to transaction integrity, market fairness, and grid security. Traditional centralized security mechanisms, which typically rely on a single-point-of-failure model, are proving insufficient in mitigating these threats due to their inherent vulnerabilities. Ensuring secure, tamper-proof, and resilient energy transactions in VPP-based markets thus demands a fundamental rethinking of cybersecurity and optimization strategies.

The consequences of cybersecurity breaches in VPP pose systemic risks to market stability. For example, double-spending attack can artificially inflate trading volumes, leading to price distortions and misallocation of resources. Similarly, Sybil attack undermines fair market participation by enabling malicious entities to dominate consensus processes, thereby skewing price discovery and diminishing trust in decentralized coordination. Malicious data injection attack and smart contract tampering further erode transaction efficiency, causing delays, increased verification overhead, and cascading market instability. These threats, if left unaddressed, compromise not only the operation continuity of VPPs but also the economic incentives that underpin prosumer engagement in energy trading ecosystems. Consequently, addressing these vulnerabilities is imperative to safeguard market integrity, ensure trading efficiency, and foster sustainable develop-

Manuscript received: March 22, 2025; revised: June 7, 2025; accepted: August 4, 2025. Date of CrossCheck: August 4, 2025. Date of online publication: August 25, 2025.

This work was supported by the National Key Research and Development Program of China (No. 2021YFB2401200) and the Ongoing Research Funding Program (No. ORF-2025-635).

Y. Wang, D. Xie (corresponding author), and X. Wang are with the Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China (e-mail: wangyanjia1996@126.com; xieda@sjtu.edu.cn; x.t.wang@sjtu.edu.cn).

H. Zhong is with the School of Electronic Information Engineering, Shanghai Dianji University, Shanghai, China (e-mail: 231053010221@st.sdju.edu.cn).

A. P. Zhao is with the Department of Energy Science and Engineering, Stanford University, Stanford, USA (e-mail: p.zhao0308@gmail.com).

M. Alhazmi is with the Electrical Engineering Department, College of Applied Engineering, King Saud University, Riyadh, Saudi Arabia (e-mail: mohalhazmi@ksu.edu.sa).

DOI: 10.35833/MPCE.2025.000244

ment of decentralized energy systems.

This paper proposes a novel blockchain-enabled cyber-resilient trading framework for VPPs, integrating game-theoretic smart contract optimization and zero-knowledge proof (ZKP) authentication to enhance transaction security, strategic decision-making, and cyber-attack resilience. Unlike conventional energy trading platforms, which depend on trusted third-party validators, the proposed framework leverages blockchain technology to establish a decentralized and trustless trading environment, where transactions are transparently recorded, cryptographically secured, and immune to unauthorized alterations. To reinforce system resilience, the proposed framework integrates Byzantine fault tolerance (BFT) consensus mechanisms, ensuring that even in the presence of malicious actors, energy transactions remain verifiable and consistent. By utilizing privacy-preserving cryptographic techniques such as ZKP, the proposed framework further guarantees that transaction validation can be performed without revealing sensitive trading details, thereby preserving participant anonymity while maintaining auditability. The contributions of this paper are fourfold.

1) A blockchain-enabled cyber-resilient trading framework for VPPs is introduced that integrates game-theoretic smart contracts, providing a robust optimization for securing decentralized energy transactions. Unlike existing blockchain applications in energy markets that primarily focus on basic transaction recording, this paper uniquely optimizes smart contract execution strategies through advanced Stackelberg game modeling, ensuring a strategic balance between cybersecurity investment and market efficiency.

2) We develop a privacy-preserving cybersecurity model that employs ZKP authentication and BFT consensus mechanisms to reinforce transaction integrity while safeguarding user anonymity. In the model, ZKP is selectively triggered based on detected anomalies to reduce computational overhead, while BFT is implemented through regional validator clustering to lower consensus communication costs. By embedding these cryptographic techniques, the proposed model significantly reduces the risk of Sybil attacks, double-spending attacks, and unauthorized data manipulation.

3) A multi-layered cybersecurity approach is established, leveraging reinforcement learning to dynamically adapt cybersecurity mechanisms against evolving cyber-threats. The ability to learn optimal defense strategies in real time provides self-evolving cyber-resilience that outperforms static security approaches.

4) Extensive multi-agent simulation is conducted, demonstrating that the proposed framework achieves superior resilience and efficiency compared with traditional centralized trading framework. By evaluating realistic cyber-attack scenarios, economic trade-offs, and blockchain transaction dynamics, we provide valuable insights into the future of secure and decentralized energy markets.

II. Literature Review

The increasing reliance on VPPs to aggregate and coordinate DERs has driven extensive research on decentralized energy trading, cybersecurity, and optimization mechanisms [6]. As VPPs shift toward blockchain-enabled transaction systems, the need for secure, efficient, and privacy-preserving trading mechanisms has become more pressing [7], [8]. Existing studies have explored various approaches to address these challenges, focusing on blockchain integration, cybersecurity reinforcement, game-theoretic modeling, and adaptive security mechanisms [9] - [11]. However, despite significant progress, current methodologies still face limitations in achieving optimal trade-off between cybersecurity investment and transaction efficiency, handling adaptive cyber-threats and ensuring scalable blockchain-enabled VPP operations.

A growing body of research has examined the role of blockchain technology in energy markets, emphasizing its ability to enhance transparency, decentralization, and security. Blockchain has been widely adopted for peer-to-peer (P2P) energy trading, with smart contracts enabling automated transaction execution between prosumers and grid operators [12]-[14]. Several studies have demonstrated that blockchain-enabled energy trading platforms can eliminate intermediaries, reduce transaction costs, and improve market efficiency [15], [16]. However, most existing blockchain-enabled energy market designs rely on standard proof-of-work (PoW) or proof-of-stake (PoS) mechanisms, which, while decentralized, suffer from high computational overhead, potential security vulnerabilities, and limited scalability [17]. In particular, consensus mechanisms such as PoW require extensive energy consumption, making them unsuitable for large-scale VPP trading systems. More recent studies have introduced BFT to improve transaction finalization efficiency and ensure system security even under adversarial conditions [18]. While these approaches offer improvements in security, they often fail to incorporate adaptive security mechanisms that dynamically respond to evolving cyber-threats.

Cybersecurity in decentralized energy trading platforms has also been an area of extensive research. Traditional intrusion detection system (IDS) and anomaly detection techniques have been employed to identify fraudulent attacks such as double-spending attacks, Sybil attacks, and malicious data injection attacks in energy transactions [19]. References [20] and [21] have shown that machine learning-based IDSs can effectively identify anomalous transaction patterns and prevent security breaches in blockchain-enabled VPPs. However, most existing IDS models require large-scale labeled datasets for training [22], making them less effective against zero-day attacks and novel cyber-threats. Furthermore, the reliance on centralized monitoring nodes in many IDS models introduces potential points of failure, which contradicts the decentralized nature of VPP-based energy trading. More recently, ZKP and homomorphic encryption techniques have been proposed to enhance transaction privacy and authentication mechanisms in blockchain networks [23]. ZKP allows transaction verification without revealing sensitive trading details, making them an attractive solution for privacy-preserving energy trading [24]. Despite these advancements, current implementations of ZKP-based authentication frameworks remain computationally expensive and are often not optimized for real-time VPP trading scenarios.

Game-theoretic models have been extensively applied to optimize energy trading strategies and cybersecurity investments in VPPs. Stackelberg game models, in particular, have been widely used to analyze interactions between VPP operators, prosumers, and cyber-attackers [25], [26]. In these models, VPP operators act as leaders, setting pricing strategies, transaction validation policies, and cybersecurity investments, while prosumers and attackers respond as followers, optimizing their respective utilities. Studies have demonstrated that game-theoretic models can effectively deter cyber-threats by strategically allocating cybersecurity resources and designing incentive-compatible transaction mechanisms [27]. However, most existing Stackelberg game modeling focuses primarily on static cybersecurity investment strategies, assuming that attackers operate with fixed behavior [28]. This assumption is unrealistic in dynamic cyber-physical environments, where adversaries continuously evolve attack tactics to exploit system vulnerabilities. Recent research has explored reinforcement learning-based security mechanisms, allowing systems to adapt cybersecurity strategies in response to attack patterns [29], [30]. While promising, these models often suffer from convergence issues, requiring extensive training data and high computational resources to achieve stable defense strategies.

The integration of quantum-inspired security mechanisms into blockchain-enabled cybersecurity models has also gained attention in recent years [31]. With the advent of quantum computing threats, researchers have begun investigating quantum-resistant cryptographic techniques to secure smart contracts, consensus mechanisms, and data encryption in decentralized networks [32], [33]. Some studies have proposed hybrid quantum-classical blockchain security frameworks, which reinforce blockchain resilience against cyber-threats [34], [35]. While these studies provide valuable insights into the potential of quantum-enhanced security models, their application in real-world VPP transactions remains largely unexplored. The lack of practical implementation frameworks and computational feasibility assessments limits the adoption of quantum-inspired cybersecurity models in large-scale decentralized energy markets.

Another critical research direction in blockchain-enabled VPP optimization is the trade-off between cybersecurity investment and transaction efficiency. References [36] and [37] have proposed multi-objective optimization frameworks to balance energy dispatch efficiency, cybersecurity costs, and transaction verification speed. While these models offer insights into optimal security-resource allocation, they often fail to consider real-time cyber-attack adaptability. Most traditional optimization models rely on predefined security parameters, which do not account for dynamic attack-response interactions. This limitation underscores the need for adaptive and self-learning cybersecurity mechanisms that can dynamically adjust security strategies based on evolving cyber-threats and real-time market conditions.

While substantial progress has been made in blockchain-enabled VPP trading, cybersecurity modeling, game-theoretic optimization, and reinforcement learning-based attack-response mechanisms, existing research still lacks a comprehensive and integrated framework that simultaneously addresses cybersecurity, privacy-preserving energy trading, adaptive attack-response strategies, and scalable blockchain transaction models. Current models either focus on static security configurations, inefficient consensus mechanisms, or non-adaptive game-theoretic modeling. These limitations highlight the need for a holistic and multi-layered cybersecurity approach that integrates blockchain-enabled security enhancements, incentive-compatible game-theoretic smart contract execution, and reinforcement learning-based adaptive defense mechanism for real-time cyber-resilience in decentralized energy trading platforms.

III. Problem Formulation and Methodology

To formulate the blockchain-enabled cyber-resilient trading framework for VPPs, we develop a mathematical optimization model that captures the economic, security, and operation dynamics of decentralized energy transactions. The model is structured into two key components: the objective function, which optimizes system cost, cybersecurity investment, and trading efficiency, and the set of constraints, which enforce operation feasibility, cybersecurity policies, and blockchain transaction integrity. The model integrates game-theoretic principles, ensuring that cybersecurity investments are strategically allocated based on rational decision-making among VPP aggregators, prosumers, and potential cyber attackers. Furthermore, ZKP authentication, BFT consensus mechanisms, and reinforcement learning-based adaptive defense mechanism are embedded within the optimization model to enhance transaction security while preserving privacy and computational efficiency.

A. Market Mechanisms and Transaction Optimization

The revenue maximizing or cost minimizing orientations of subjects such as prosumers, aggregators, and potential attackers in the blockchain-enabled energy market are first described. The primary objective is to minimize the total system cost, which encapsulates blockchain transaction fees, cybersecurity investment, and operation expenses. The first summation of (1) represents the costs incurred by individual prosumers. $\omega_{i,t}^{tr}$ scales the transaction costs in blockchain, $\Phi_{i,t}^{block}$ denotes the energy trade validation overhead, and $\Xi_{i,t}^{sec}$ accounts for cybersecurity investment. Additionally, cyber-related expenditures are captured by $\Psi_{i,t}^{cyb}$, which penalizes the difference between perceived cyber risk $\vartheta_{i,t}^{risk}$ and the implemented detection level $\theta_{i,t}^{det}$. The second summation of (1) models the aggregator-level costs, incorporating energy trade efficiency $\Omega_{j,t}^{trade}$, associated losses $\Delta_{j,t}^{loss}$, and penalty factors $\Lambda_{j,t}^{pen}$ that depend on the ratio of cybersecurity investment to optimal risk mitigation levels $\rho_{j,t}^{opt}$.

$$\min_{\boldsymbol{\lambda},\boldsymbol{\mu},\boldsymbol{\nu}} \left\{ \sum_{t=\mathcal{T}} \sum_{i \in \mathcal{N}} \left[\omega_{i,t}^{tr} \left(\Phi_{i,t}^{block} + \Xi_{i,t}^{sec} \right) + \Psi_{i,t}^{cyb} \left(\vartheta_{i,t}^{risk} - \theta_{i,t}^{det} \right) \right] + \sum_{t=\mathcal{T}} \sum_{j \in \mathcal{M}} \left[\Gamma_{j,t}^{agg} \left(\Omega_{j,t}^{trade} - \Delta_{j,t}^{loss} \right) + \Lambda_{j,t}^{pen} \frac{\Xi_{j,t}^{sec}}{1+\rho_{j,t}^{opt}} \right] \right\} \quad (1)$$

where $\boldsymbol{\lambda}$ is the aggregator's security strategy vector; $\boldsymbol{\mu}$ is the prosumer's security compliance vector; $\boldsymbol{\nu}$ is the attacker's

strategy vector; t denotes the time slot; $\mathcal{T}$ denotes the total trading session; i and $\mathcal{N}$ are the index and set of prosumers, respectively; j and $\mathcal{M}$ are the index and set of aggregators, respectively; and $\Gamma_{j,t}^{agg}$ is the gain factor of scheduling efficiency.

The revenue function for prosumers is designed to maximize their economic gains while factoring in energy sales, blockchain fees, and cybersecurity expenditures. The first term of (2) captures the profits from selling surplus energy. The second term of (2) accounts for blockchain transaction costs. Aggregators also optimize their revenue, with a core profit function $\Gamma_{j,t}^{profit}$ minus cybersecurity expenditures, which are governed by risk-dependent factors $\delta_{j,t}^{risk}$.

$$\max_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\zeta}} \left\{ \sum_{t=\mathcal{T}} \sum_{i\in\mathcal{N}} \left[\pi_{i,t}^{sell} \left(\varphi_{i,t}^{gen} - \varsigma_{i,t}^{dem} \right) - \Theta_{i,t}^{block} Y_{i,t}^{cost} \right] + \sum_{t=\mathcal{T}} \sum_{j\in\mathcal{M}} \left(\Gamma_{j,t}^{profit} - \Lambda_{j,t}^{sec} \frac{\Xi_{j,t}^{cyb}}{\delta_{j,t}^{risk}+1} \right) \right\} \tag{2}$$

where $\boldsymbol{\alpha}$ is the energy trading strategy vector; $\boldsymbol{\beta}$ is the blockchain cost strategy vector; $\boldsymbol{\zeta}$ is the security-economy trade-off vector; $\pi_{i,t}^{sell}$ is the market clearing price; $\varphi_{i,t}^{gen}$ is the energy generated; $\varsigma_{i,t}^{dem}$ is the total energy demand; $\Theta_{i,t}^{block}$ is the cost per transaction; $Y_{i,t}^{cost}$ is the total transaction volume; $\Lambda_{j,t}^{sec}$ is the cost factor of cybersecurity investment; and $\Xi_{j,t}^{cyb}$ is total cybersecurity investment.

For aggregators, the objective function optimizes energy dispatch and minimizes risk exposure from cyber-threats. The first summation of (3) represents the energy dispatch efficiency, where the aggregator's profit depends on the difference between total generation and demand, scaled by $\Omega_{j,t}^{dispatch}$. The second term of (3) models the cybersecurity cost function, where $\Lambda_{j,t}^{pen}$ increases if risk exposure $\Xi_{j,t}^{risk}$ exceeds $\rho_{j,t}^{opt}$. The final summation of (3) penalizes cyber-attack-induced losses, incorporating the expected attack impact $\vartheta_{k,t}^{exp}$ and the level of mitigation $\theta_{k,t}^{mit}$.

$$\max_{\boldsymbol{\gamma},\boldsymbol{\xi},\boldsymbol{\kappa}} \left\{ \sum_{t=\mathcal{T}} \sum_{j\in\mathcal{M}} \left[\Omega_{j,t}^{dispatch} \sum_{i\in\mathcal{N}} \left(\varphi_{i,t}^{gen} - \varsigma_{i,t}^{dem} \right) - \Lambda_{j,t}^{pen} \frac{\Xi_{j,t}^{risk}}{\rho_{j,t}^{opt}+1} \right] - \sum_{t=\mathcal{T}} \sum_{k\in\mathcal{A}} \Theta_{k,t}^{cyb} \left(\vartheta_{k,t}^{exp} - \theta_{k,t}^{mit} \right) \right\} \tag{3}$$

where k and $\mathcal{A}$ are the index and set of the attackers respectively; $\boldsymbol{\gamma}$ is the energy dispatch strategy vector; $\boldsymbol{\xi}$ is the cybersecurity investment vector; $\boldsymbol{\kappa}$ is the attack response strategy vector; and $\Theta_{k,t}^{cyb}$ is the attack loss conversion factor. The prosumer bidding strategy function maximizes the energy trading profits.

$$\max_{\boldsymbol{\alpha},\boldsymbol{\beta}} \sum_{t=\mathcal{T}} \sum_{i\in\mathcal{N}} \left(\pi_{i,t}^{sell} \varphi_{i,t}^{bid} - \Theta_{i,t}^{gas} \Pi_{i,t}^{txn} \right) \tag{4}$$

where $\Theta_{i,t}^{gas}$ is the gas fee for a single transaction; $\Pi_{i,t}^{txn}$ is the actual transaction volume; and $\varphi_{i,t}^{bid}$ is the declared electricity selling volume.

$$\max_{\boldsymbol{\gamma},\boldsymbol{\xi}} \sum_{t=\mathcal{T}} \sum_{j\in\mathcal{M}} \left(\Omega_{j,t}^{dis} - \Lambda_{j,t}^{cyb} \right) \tag{5}$$

The aggregator response function balances energy dispatch $\Omega_{j,t}^{dis}$ and cybersecurity investments $\Lambda_{j,t}^{cyb}$ to minimize security costs while ensuring efficient trading.

To ensure that the bidding results are fair, transparent, and resistant to manipulation, it is necessary to introduce the constraints that limit price-volume fluctuations, enforce on-chain settlement consistency, and satisfy game-theoretic equilibrium conditions, thereby aligning economic decisions with the physical and security feasibility domain, as shown in (6). This anomaly detection constraint ensures that suspicious blockchain activities $\Lambda_{k,t}^{anom}$ exceed a predefined alert threshold ρ^{alert} compared with normal transactions $\Theta_{k,t}^{norm}$. If anomalies exceed this limit, automatic security reinforcements are triggered to counteract potential cyber-threats, as shown in (7).

$$\sum_{k\in\mathcal{A}} \left(\Lambda_{k,t}^{anom} - \Theta_{k,t}^{norm} \right) \geq \rho^{alert} \quad \forall t \in \mathcal{T} \tag{6}$$

$$\sum_{j\in\mathcal{M}} \frac{\Xi_{j,t}^{lat}}{\Gamma_{j,t}^{valid}} \leq \tau^{\max} \quad \forall t \in \mathcal{T} \tag{7}$$

The blockchain network latency constraint ensures that the transaction processing delay $\Xi_{j,t}^{lat}$ per valid transaction $\Gamma_{j,t}^{valid}$ remains below an acceptable threshold $\tau^{\max}$. This guarantees high throughput efficiency, preventing transaction bottlenecks in VPP trading.

$$\sum_{t=\mathcal{T}} \sum_{i\in\mathcal{N}} \left(\Phi_{i,t}^{scal} - \Theta_{i,t}^{load} \right) \geq 0 \tag{8}$$

To ensure system scalability, the available blockchain processing capacity $\Phi_{i,t}^{scal}$ must be greater than or equal to the transaction load $\Theta_{i,t}^{load}$. This prevents system congestion as VPP transaction volumes increase over time.

$$\sum_{i\in\mathcal{N}} \left(\Psi_{i,t}^{best} - \Gamma_{i,t}^{opt} \right) = 0 \quad \forall t \in \mathcal{T} \tag{9}$$

The Nash equilibrium constraint ensures that prosumers and aggregators adopt optimal strategies where no participant can unilaterally improve their payoff. The difference between actual best responses $\Psi_{i,t}^{best}$ and the equilibrium decision $\Gamma_{i,t}^{opt}$ must be zero for all players.

$$\sum_{j\in\mathcal{M}} \left(\Theta_{j,t}^{audit} - \Xi_{j,t}^{error} \right) \geq \tau^{check} \quad \forall t \in \mathcal{T} \tag{10}$$

To maintain long-term security enforcement, this dynamic contract auditing constraint ensures that the frequency of smart contract audits $\Theta_{j,t}^{audit}$ exceeds the number of detected transaction anomalies $\Xi_{j,t}^{error}$ by at least τ^{check}, preventing vulnerabilities from persisting.

$$\sum_{j\in\mathcal{M}} \frac{\Psi_{j,t}^{price}}{\Gamma_{j,t}^{vol}} \leq \tau^{stability} \quad \forall t \in \mathcal{T} \tag{11}$$

This market stability constraint ensures that the ratio of price $\Psi_{j,t}^{price}$ to volume $\Gamma_{j,t}^{vol}$ remains within a predefined stability threshold $\tau^{stability}$, preventing extreme market fluctuations that could disrupt VPP operations.

$$\sum_{t=\mathcal{T}} \sum_{j\in\mathcal{M}} \left(\Theta_{j,t}^{secure} - \Xi_{j,t}^{breach} \right) \geq \rho^{safe} \tag{12}$$

The blockchain security threshold constraint mandates that the number of secure blockchain operations $\Theta_{j,t}^{secure}$ must always exceed the number of successful security breaches

$\Xi_{j,t}^{breach}$ by at least ρ^{safe}, ensuring a minimum level of protection for transactions.

B. Energy Constraints and Cost Coupling

To guarantee the physical feasibility of energy scheduling within the network, this subsection performs a physical validation of the trading scheme by incorporating energy constraints and cost coupling, thereby capturing the associated impacts on on-chain billing mechanisms.

$$\sum_{i\in\mathcal{N}}\left(\varphi_{i,t}^{gen}+\kappa_{i,t}^{imp}-\varsigma_{i,t}^{dem}-\chi_{i,t}^{exp}\right)+\sum_{j\in\mathcal{M}}\left(\Omega_{j,t}^{dis}-\Delta_{j,t}^{loss}\right)=0\quad\forall t\in\mathcal{T} \tag{13}$$

This energy balance constraint ensures that the total energy supply from DERs imports from the external grid $\kappa_{i,t}^{imp}$, and $\Omega_{j,t}^{dis}$ matches $\varsigma_{i,t}^{dem}$ and exported energy $\chi_{i,t}^{exp}$, considering $\Delta_{j,t}^{loss}$. This condition is vital for maintaining the VPP stability, preventing both energy shortages and excess generation.

$$\varphi_{i,t}^{gen}\le\min\left(\Phi_{i,t}^{\max},\frac{\zeta_{i,t}^{avail}}{1+\delta_{i,t}^{uncert}}\right)\quad\forall i\in\mathcal{N},\ \forall t\in\mathcal{T} \tag{14}$$

To ensure that prosumers operate within DER generation limits, the power generation at each node $\varphi_{i,t}^{gen}$ must be bounded by both the rated maximum capacity $\Phi_{i,t}^{\max}$ and the available resource limit $\zeta_{i,t}^{avail}$, adjusted for uncertainty factors $\delta_{i,t}^{uncert}$. This constraint accounts for real-time fluctuations in renewable energy availability.

$$\sum_{i\in\mathcal{N}}\left(\varphi_{i,t}^{gen}+\kappa_{i,t}^{imp}-\varsigma_{i,t}^{dem}\right)=\sum_{j\in\mathcal{M}}\Omega_{j,t}^{dis}\quad\forall t\in\mathcal{T} \tag{15}$$

This demand-supply matching condition maintains grid stability by ensuring that energy injections from DERs and external imports match total demand and aggregator dispatch allocations. This dynamic condition is critical for real-time grid operation, particularly in VPP with high shares of renewable energy.

$$\sum_{i\in\mathcal{N}}\left(\Theta_{i,t}^{smart}-\Xi_{i,t}^{mis}\right)\ge 0\quad\forall t\in\mathcal{T} \tag{16}$$

The smart contract execution constraint enforces incentive-compatible transactions by ensuring that only valid transactions $\Theta_{i,t}^{smart}$ are executed, while misreported transactions $\Xi_{i,t}^{mis}$ are rejected. This condition prevents data falsification and fraudulent bidding in energy trading.

$$\sum_{j\in\mathcal{M}}\left(\Gamma_{j,t}^{lead}-\sum_{i\in\mathcal{N}}\lambda_{i,t}^{follow}\right)=0\quad\forall t\in\mathcal{T} \tag{17}$$

To enforce game-theoretic equilibrium, the leader's (VPP aggregator's) strategic decisions $\Gamma_{j,t}^{lead}$ must align with the aggregated responses of prosumers and attackers $\lambda_{i,t}^{follow}$, ensuring rational strategy adoption under a Stackelberg game modeling.

To support real-time strategy adjustments aligned with prosumer behaviors and covert attacker actions, we assume that the VPP aggregator is equipped with an advanced information collection and analysis system. This system integrates historical data analysis, short-term forecasting models, and a decentralized edge computing framework. For prosumers, smart meters and demand prediction algorithms are used to infer short-term energy production and consumption under uncertainty. For attacker behavior, the system utilizes anomaly detection models based on unsupervised learning and external threat intelligence feeds to probabilistically update risk estimates. While perfect real-time detection remains a theoretical assumption, a future-forward system framework is reflected and is enabled by ongoing advances in artificial intelligence (AI)-based situational awareness for VPPs.

$$\sum_{i\in\mathcal{N}}\frac{\varphi_{i,t}^{gen}}{1+\delta_{i,t}^{uncert}}\ge\varsigma_{i,t}^{dem}\quad\forall t\in\mathcal{T} \tag{18}$$

This renewable energy uncertainty constraint ensures that the actual available power generation (adjusted for $\delta_{i,t}^{uncert}$) meets real-time $\varsigma_{i,t}^{dem}$. This helps maintain energy balance despite renewable variability.

In order to quantify the feedback effects of blockchain transaction costs, smart contract execution expenses, and budget-credibility constraints on network operation, the following formulations are integrated into the energy flow model, thereby establishing a bidirectional coupling framework between economic and physical domains.

$$\sum_{i\in\mathcal{N}}\Theta_{i,t}^{gas}\Pi_{i,t}^{txn}=\sum_{j\in\mathcal{M}}\left(\Lambda_{j,t}^{fee}-\Xi_{j,t}^{overhead}\right)\quad\forall t\in\mathcal{T} \tag{19}$$

The blockchain-enabled transaction cost function ensures that the total gas fees paid $\Theta_{i,t}^{gas}$ per $\Pi_{i,t}^{txn}$ align with aggregator-level fees $\Lambda_{j,t}^{fee}$ minus operation overhead $\Xi_{j,t}^{overhead}$. This controls transaction costs in VPP trading.

$$\sum_{j\in\mathcal{M}}\left(\Lambda_{j,t}^{block}-\Gamma_{j,t}^{valid}\right)=0\quad\forall t\in\mathcal{T} \tag{20}$$

The distributed ledger state update equation ensures that newly added $\Lambda_{j,t}^{block}$ exactly matches the count of $\Gamma_{j,t}^{valid}$. This maintains ledger consistency and prevents rollback attacks.

$$\sum_{i\in\mathcal{N}}\left(\Theta_{i,t}^{exec}-\Xi_{i,t}^{fail}\right)\ge 0\quad\forall t\in\mathcal{T} \tag{21}$$

To ensure deterministic and tamper-proof smart contract execution, valid executions $\Theta_{i,t}^{exec}$ must exceed failed contract executions $\Xi_{i,t}^{fail}$. This prevents transaction reversibility and exploits.

$$\sum_{t=\mathcal{T}}\sum_{j\in\mathcal{M}}\left(\Psi_{j,t}^{mut}-\Omega_{j,t}^{static}\right)=0 \tag{22}$$

This evolutionary optimization function ensures that the adaptive contract execution $\Psi_{j,t}^{mut}$ follows mutational improvements, replacing static contracts $\Omega_{j,t}^{static}$ and optimizing VPP efficiency.

$$\sum_{j\in\mathcal{M}}\left(\Psi_{j,t}^{rep}-\Xi_{j,t}^{sco}\right)\ge 0\quad\forall t\in\mathcal{T} \tag{23}$$

where $\Psi_{j,t}^{rep}$ is the real-time reputation score; and $\Xi_{j,t}^{sco}$ is the penalty value for misconduct. The dynamic reputation update function penalizes misbehaving participants, reducing their trading privileges. This blockchain consensus mechanism equation ensures that only confirmed transactions $\Theta_{j,t}^{final}$ are included in the ledger, where $\Xi_{j,t}^{conf}$ represents the unconfirmed transactions that have not reached the consensus threshold ρ^{cons}. This guarantees that all recorded transactions are immutable and verified, preventing double-spending and Sybil attacks.

$$\sum_{j\in\mathcal{M}}\left(\Theta_{j,t}^{final}-\Xi_{j,t}^{conf}\right)=\rho^{cons}\quad\forall t\in\mathcal{T} \tag{24}$$

C. Security and Privacy Protection

While the blockchain offers decentralized trust, it also faces risks of attacks and privacy breaches. This subsection enhances system resilience through adversarial objectives and consistency constraints, ensuring that transaction data remain trustworthy even in extreme scenarios.

The following objective functions quantify the attacker's payoff and the defender's cost, providing a quantitative foundation for secure resource allocation and dynamic game-theoretic analysis.

From the perspective of a rational cyber-attacker, the objective function is to maximize the expected attack success rate while minimizing detection risk. The first term of (25) models the attack payoff, where $\Psi_{k,t}^{attack}$ is the exploitation reward factor; $\Theta_{k,t}^{exploit}$ is the available vulnerability; and $\Xi_{k,t}^{detect}$ is the system detection capability. The second term of (25) represents the cost of failed attacks, which increases when security defenses improve. Here, $\Gamma_{k,t}^{fail}$ penalizes unsuccessful breaches, with risk factors $\Omega_{k,t}^{prob}$ and $\rho_{k,t}^{risk}$ adjusting attack feasibility based on defense countermeasures.

$$\max_{\boldsymbol{l},\boldsymbol{\iota},\boldsymbol{\phi}}\sum_{t=\mathcal{T}}\sum_{k\in\mathcal{A}}\left[\Psi_{k,t}^{attack}\left(\Theta_{k,t}^{exploit}-\Xi_{k,t}^{detect}\right)-\Gamma_{k,t}^{fail}\frac{\Omega_{k,t}^{prob}}{\rho_{k,t}^{risk}+1}\right] \tag{25}$$

where $\boldsymbol{l}$ is the attack reward vector; $\boldsymbol{\iota}$ is the vulnerability exploitation strategy vector; and $\boldsymbol{\phi}$ is the stealth strategy vector.

$$\sum_{t=\mathcal{T}}\sum_{j\in\mathcal{M}}\left(\Theta_{j,t}^{res}-\Xi_{j,t}^{cyb}\right)=\rho^{safe} \tag{26}$$

This cyber resilience function ensures that the number of successful security measures $\Theta_{j,t}^{res}$ always outweighs the number of cybersecurity breaches $\Xi_{j,t}^{cyb}$ by at least the resilience threshold ρ^{safe}. This quantifies the system ability to withstand ongoing cyber-threats.

$$\max_{\boldsymbol{\pi}}\sum_{t=\mathcal{T}}\sum_{j\in\mathcal{M}}\left[R_{j,t}^{sec}-\lambda\left(C_{j,t}^{def}+\Omega_{j,t}^{cost}\right)\right] \tag{27}$$

This reinforcement learning reward function optimizes adaptive security mechanisms by maximizing defensive rewards $R_{j,t}^{sec}$ while penalizing excessive cybersecurity investment costs $C_{j,t}^{def}$ and operation trade-offs $\Omega_{j,t}^{cost}$. The parameter λ tunes the balance between security effectiveness and cost efficiency. $\boldsymbol{\pi}$ is the defense strategy parameter vector.

$$\min_{\boldsymbol{\delta}}\sum_{t=\mathcal{T}}\sum_{\mathcal{N}}\frac{\Xi_{i,t}^{lat}}{\Gamma_{i,t}^{txn}} \tag{28}$$

This latency minimization function ensures that the average $\Xi_{i,t}^{lat}$ per transaction count $\Gamma_{i,t}^{txn}$ remains minimal, improving network throughput and trading efficiency. $\boldsymbol{\delta}$ is the network parameter optimization vector.

Constraints such as consensus, fault tolerance, and privacy proofs collectively define the system security-feasible domain, ensuring that on-chain settlement remains reliable even under the worst-case conditions. The blockchain transaction verification constraint (29) guarantees the integrity of transactions, where $\Theta_{i,t}^{trans}$ represents the energy trading requests submitted by prosumers, while $\Xi_{i,t}^{inv}$ captures invalid transactions. The validation process is handled by aggregators, where successfully verified transactions should equal the difference between submitted transactions $\Gamma_{j,t}^{valid}$ and rejected requests $\Lambda_{j,t}^{fail}$, ensuring the consistency and tamper-proof trading records.

$$\sum_{i\in\mathcal{N}}\left(\Theta_{i,t}^{trans}-\Xi_{i,t}^{inv}\right)-\sum_{j\in\mathcal{M}}\left(\Gamma_{j,t}^{valid}-\Lambda_{j,t}^{fail}\right)=0\quad\forall t\in\mathcal{T} \tag{29}$$

$$\sum_{i\in\mathcal{N}}\left(\phi_{i,t}^{multi}-\psi_{i,t}^{fake}\right)\geq\tau^{sig}\quad\forall t\in\mathcal{T} \tag{30}$$

To enforce multi-signature validation, the number of valid signatures $\phi_{i,t}^{multi}$ required for transaction approval must exceed the threshold τ^{sig}, ensuring the protection against fraudulent signatures $\psi_{i,t}^{fake}$. This constraint strengthens VPP transaction security by requiring consensus from multiple authorized entities before execution.

$$\sum_{j\in\mathcal{M}}\left(\lambda_{j,t}^{byz}-\omega_{j,t}^{corrupt}\right)\geq\rho^{fault}\quad\forall t\in\mathcal{T} \tag{31}$$

This BFT constraint ensures that the network remains resilient even if a fraction of nodes becomes malicious. The number of honest participants $\lambda_{j,t}^{byz}$ must be greater than the number of corrupt nodes $\omega_{j,t}^{corrupt}$ by at least the predefined fault tolerance threshold ρ^{fault}, preventing Sybil attacks and unauthorized alterations of transaction records.

$$\sum_{k\in\mathcal{A}}\left(\Psi_{k,t}^{attack}-\Theta_{k,t}^{mitigate}\right)\leq\rho^{risk}\quad\forall t\in\mathcal{T} \tag{32}$$

This cyber-attack cost-benefit constraint ensures that attack feasibility remains bounded by cybersecurity investment. The expected attack impact $\Psi_{k,t}^{attack}$ minus defense mitigation $\Theta_{k,t}^{mitigate}$ cannot exceed a defined risk tolerance threshold ρ^{risk}, ensuring attack containment.

$$\sum_{j\in\mathcal{M}}\Xi_{j,t}^{sec}\leq\sum_{i\in\mathcal{N}}\Lambda_{i,t}^{budget}\quad\forall t\in\mathcal{T} \tag{33}$$

To regulate cybersecurity investment allocation, the total cybersecurity spending $\Xi_{j,t}^{sec}$ by VPP operators must not exceed the available security budget $\Lambda_{i,t}^{budget}$ across all prosumers, ensuring the cost-effectiveness in cyber-defense strategies.

$$\sum_{i\in\mathcal{N}}\left(\Pi_{i,t}^{zkp}-\Xi_{i,t}^{leak}\right)\geq\tau^{priv}\quad\forall t\in\mathcal{T} \tag{34}$$

To ensure privacy-preserving transactions using ZKP, this constraint mandates that the total number of successfully verified ZKP transactions $\Pi_{i,t}^{zkp}$ exceeds the risk of data leakage $\Xi_{i,t}^{leak}$ by at least the predefined privacy threshold τ^{priv}. This guarantees that sensitive trading information remains undisclosed while still allowing transaction validation.

$$\sum_{j\in\mathcal{M}}\left(\Psi_{j,t}^{rep}-\Omega_{j,t}^{mal}\right)\geq 0\quad\forall t\in\mathcal{T} \tag{35}$$

This reputation-based transaction scoring constraint ensures that only participants with sufficient trust scores $\Psi_{j,t}^{rep}$ are allowed to trade, preventing malicious behavior. If a participant's reputation score falls below the accepted threshold, the transactions are flagged as $\Omega_{j,t}^{mal}$, reducing the likelihood of fraudulent activities in VPP trading.

$$\sum_{i\in\mathcal{N}}\left(\Lambda_{i,t}^{valid}-\Xi_{i,t}^{fake}\right)\geq 0\quad\forall t\in\mathcal{T} \tag{36}$$

To prevent Sybil attack and double-spending attack, this data integrity constraint ensures that the number of valid identities $\Lambda_{i,t}^{valid}$ must always exceed the number of fraudulent attempts $\Xi_{i,t}^{fake}$. This reinforces secure and tamper-proof energy trading.

$$\sum_{i\in\mathcal{N}}\left(\Psi_{i,t}^{rand}-\Gamma_{i,t}^{eq}\right)=0 \quad \forall t\in\mathcal{T} \tag{37}$$

This game-theoretic-mixed-strategy equilibrium equation ensures that decision randomness $\Psi_{i,t}^{rand}$ aligns with the optimal Nash equilibrium $\Gamma_{i,t}^{eq}$. This guarantees rational strategy adoption under strategic uncertainty.

$$\sum_{i\in\mathcal{N}}\left(\Pi_{i,t}^{priv}-\Xi_{i,t}^{breach}\right)\geq 0 \quad \forall t\in\mathcal{T} \tag{38}$$

To enforce privacy-preserving data-sharing, the number of private ZKP-secured transactions $\Pi_{i,t}^{priv}$ must always exceed the risk of unauthorized access $\Xi_{i,t}^{breach}$, ensuring the confidentiality in blockchain-enabled energy markets.

$$\sum_{t=\mathcal{T}j\in\mathcal{M}}\sum\left(\Theta_{j,t}^{scal}-\Xi_{j,t}^{overload}\right)\geq 0 \tag{39}$$

This blockchain scalability function ensures that the available system capacity $\Theta_{j,t}^{scal}$ is always greater than the transactional load $\Xi_{j,t}^{overload}$, ensuring network adaptability under increasing transaction volumes.

D. Stackelberg Game Process for Cyber-resilient VPP Trading

In every trading interval, the aggregator acts as the sole Stackelberg leader. It first publishes a package of market and security decisions. After observing this announcement, two classes of followers react in parallel. Prosumers independently adjust their electricity offers so as to maximize individual trading profits. Cyber attackers choose an attack type and intensity that maximize their expected payoff, taking into account the security measures announced by the aggregator.

The aggregator anticipates these reactions and selects its actions accordingly. The point at which no side has an incentive to deviate constitutes the Stackelberg equilibrium for the interval.

The VPP operator remains outside the strategic game. Before the game begins, it issues exogenous parameters such as the upper cap on the security budget, and the minimum redundancy ratio and tariff ceilings, that delimit the aggregator's feasible decision space. After the equilibrium is obtained, it simply executes the cleared dispatch plan, performs physical power-flow control and financial settlement, and feeds back any deviations for accounting in the next interval.

Thus, the operator influences the game only through static constraints and ex-post execution, while all strategic interaction takes place between the aggregator (leader) and the two follower groups.

E. Reinforcement Learning-based Adaptive Defense and Trading Optimization

To enhance the real-time adaptability of VPP trading under cyber-threats, we incorporate two reinforcement learning algorithms, e. g., proximal policy optimization (PPO) and deep Q-network (DQN), into the cyber-defense layer. These algorithms dynamically optimize the strategic behaviors of VPP aggregators and cyber-attackers within a multi-agent Stackelberg game.

PPO is used by the VPP aggregator to determine optimal control decisions over continuous action variables such as cybersecurity investment levels, transaction gas fee coefficients, and bidding price adjustment ratios. The input state vector is denoted by:

$$\boldsymbol{s}_t=\left[h_t,\pi_t,\phi_t,\xi_t,\alpha_t,\delta_t\right] \tag{40}$$

where h_t is the blockchain height; π_t is the real-time clearing electricity price; ϕ_t is the aggregated energy generation; ξ_t is the aggregator's cybersecurity investment level; α_t is the system threat alert index; and δ_t is the average transaction confirmation latency.

The action vector is defined as:

$$\boldsymbol{a}_t=\left[p_{sec},p_{gas},p_{bid}\right] \tag{41}$$

where p_{sec} is the proportion of budget allocated to cybersecurity; p_{gas} is a multiplier for gas fee adjustment; and p_{bid} modifies the default bidding curve for energy market participation.

The reward function for PPO is given by:

$$r_t=\pi_t E_t^{cleared}-C_t^{sec}-\lambda L_t^{cyb}-\mu\Delta_t^{lat} \tag{42}$$

where $E_t^{cleared}$ is the cleared trading energy volume; C_t^{sec} is the cybersecurity investment cost; L_t^{cyb} is the monetary loss due to cyber-attacks; Δ_t^{lat} is the blockchain delay; and λ and μ are the coefficients that denote attack tunable weights penalizing cyber damage and latency, respectively.

The attacker is modeled as a discrete agent using DQN. Its action space consists of six options: double-spending attack, Sybil attack, smart contract tampering, malicious data injection attack, denial-of-service (DoS) attack, and no attack. The state vector is expressed as:

$$\boldsymbol{s}_t'=\left[\rho_t,\theta_t,\zeta_t,\kappa_t,\eta_t\right] \tag{43}$$

where ρ_t is the attacker's current reputation score within the system; θ_t is the estimated probability of detection by defense mechanisms; ζ_t is the accumulated historical gain from previous attacks; κ_t is the remaining computational or financial resource available for the attacker; and η_t is the network congestion level.

The attack reward function is defined as:

$$r_t'=R_t^{atk}-P_t^{det}-C_t^{res}-\beta\Pi_{detected} \tag{44}$$

where R_t^{atk} is the potential attack payoff; P_t^{det} is the detection penalty; C_t^{res} is the cost associated with executing the attack; and β is an additional penalty for being caught, activated by the indicator function $\Pi_{detected}$.

IV. Case Studies

To validate the effectiveness of the proposed framework, a comprehensive case study is conducted using a synthetic yet realistic energy trading environment. The study models a distributed energy market with 150 prosumers including 85 residential users, 40 commercial facilities, and 25 industrial consumers, each equipped with heterogeneous DERs such as

photovoltaic (PV) systems, wind turbines, and battery storage units. The VPP operator manages six regional aggregators responsible for coordinating energy dispatch, optimizing market participation, and enforcing cybersecurity policies. The total installed renewable generation capacity is 95 MW, consisting of 45 MW from solar PV, 30 MW from wind, and 20 MW from battery storage systems, with a maximum hourly trading volume of 60 MWh. The energy trading simulation runs over a 24-hour period, divided into 96 market intervals (15-min timesteps) to capture high-resolution trading dynamics and cyber-attack responses. The blockchain network is structured with 250 validator nodes by using BFT consensus mechanisms, ensuring transaction finalization within an average of 4.2 s per block.

To simulate realistic cyber-threats, the case study incorporates five distinct attack scenarios, including double-spending attack, Sybil attack, smart contract tampering, malicious data injection attack, and DoS attack. Double-spending attack exploits time lags in transaction verification to execute repeated energy trades, creating a false appearance of multiple payments on the ledger. Sybil attack involves generating numerous fake identities to manipulate voting-based consensus mechanisms or distort market outcomes. Smart contract tampering refers to altering the logic of pre-deployed contracts, potentially bypassing security protocols or skewing market rules. Malicious data injection attack entails submitting deceptive input data to mislead scheduling and trading decisions. DoS attack overwhelms the system with excessive requests, degrading network availability and compromising transaction finality.

Attackers are modeled as adaptive adversarial agents, leveraging reinforcement learning algorithms to dynamically refine attack strategies based on system vulnerabilities. The attack penetration rate varies between 5% and 25% of total transactions, with an average attack success rate of 12.8% under baseline security conditions. The defense mechanisms embedded within the proposed framework, including game-theoretic cybersecurity investments, ZKP authentication, and reinforcement learning-based adaptive defense mechanism, are evaluated based on their ability to reduce financial losses, mitigate system disruption, and improve blockchain transaction integrity. Key performance indicators include the cyber-resilience index (CRI) [38], average transaction latency, Nash equilibrium deviation in attack scenarios, and total cybersecurity investment as a function of cyber-threat intensity.

The smart contract execution and blockchain network are implemented using Hyperledger Fabric 2.4 with Go-based chaincode scripting, while cryptographic security enhancements, including ZKP authentication and BFT consensus validation, are integrated using Libsnark and Zether cryptographic libraries. The game-theoretic security optimization model is formulated using Gurobi 10.0, solving a multi-stage Stackelberg equilibrium problem with 1800 decision variables and 9500 constraints, ensuring optimal security resource allocation under adversarial conditions. Multi-stage refers to the repeated Stackelberg game being executed across consecutive market intervals, where equilibrium decisions are re-evaluated in each stage based on updated system states and threat levels. Reinforcement learning-based adaptive defense mechanism is trained using TensorFlow 2.9, applying PPO and DQN algorithms with 5 million training episodes to optimize cyber-defense policies in a dynamic adversarial environment. The overall simulation runs on Ubuntu 22.04, leveraging Docker-based blockchain containerization for scalable and modular execution.

In Fig. 1, the penetration rates of five major cyber-threats are presented affecting blockchain-enabled VPP transactions, highlighting the vulnerabilities of decentralized trading architectures. Double-spending attacks, which manipulate transaction validation to exploit the system financially, are the most prevalent, with a penetration rate of 23.8%, indicating that nearly one in four attacks attempt to perform fraudulent duplicate transactions. Sybil attacks, which involve the creation of fake identities to gain market influence, have a penetration rate of 19.4%, making them a significant threat to the fairness and decentralization of VPP trading. Smart contract tampering, as a growing concern in blockchain security, is observed with the penetration rate of 15.7%, exposing the risks of flawed or maliciously modified contract execution. Malicious data injection attacks, where attackers alter trading data to disrupt market equilibrium, occur with the penetration rate of 11.9%, while DoS attacks present the lowest penetration rate of 9.6%. Note that the success rate of these attacks ranges between 5% and 15%, with double-spending attack having the highest likelihood of success rate of 14.7%, reinforcing the need for ZKP authentication and reinforcement learning-based defense strategies to fortify blockchain transaction integrity.

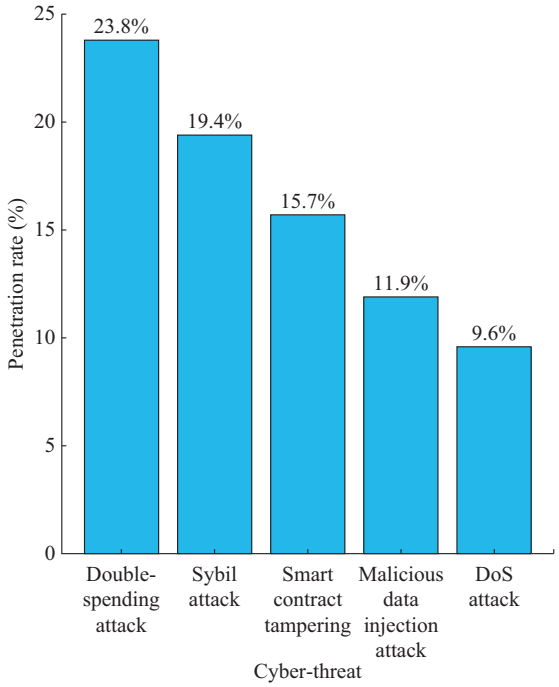

Fig. 1. Penetration rates of five major cyber-threats.

Figure 2 examines the relationship between cybersecurity investment level and their effectiveness in defending blockchain-enabled energy trading systems against cyber-threats. The investment spectrum ranges from $\$2.5\times10^6$ (low) to $\$14.7\times10^6$ (very high), while security effectiveness is quanti-

fied on a 0-100% scale, representing the system resilience against various attacks. At low investment level ($\$2.5\times10^6$), the security effectiveness is only 45%, indicating vulnerability to sophisticated cyber-threats such as Sybil attacks and smart contract tampering. At moderate investment level ($\$5.8\times10^6$), security effectiveness improves to 68%, successfully mitigating double-spending and malicious data injection risks. A high investment level ($\$9.3\times10^6$) raises security effectiveness to 85%, neutralizing most forms of cyber-attacks, while the very high investment level ($\$14.7\times10^6$) achieves the security effectiveness of 97%, ensuring robust ZKP authentication, anomaly detection, and real-time threat mitigation. The results demonstrate a non-linear relationship between investment level and security effectiveness, where strategic game-theoretic cybersecurity investment optimization is crucial to maximizing the protection while maintaining cost efficiency.

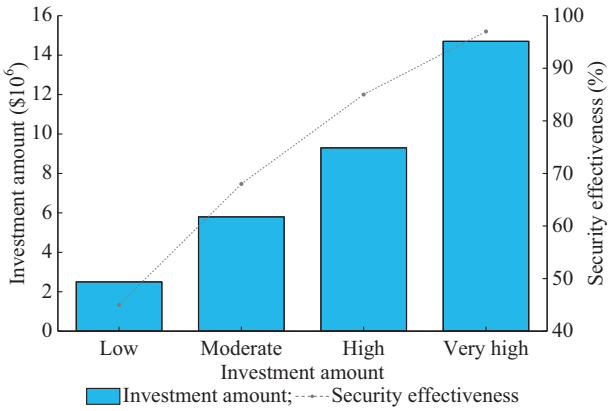

Fig. 2. Relationship between investment level and their security effectiveness in defending blockchain-enabled energy trading systems against cyber-threats.

Figure 3 presents the effectiveness of defense mechanisms against cyber-threats in decentralized energy markets. A heatmap is presented illustrating the interaction between five major cyber-threats and five corresponding defense mechanisms, quantifying their effectiveness in neutralizing security breaches in blockchain-enabled VPP trading. The double-spending attack is best countered by BFT consensus mechanisms, which demonstrates the effectiveness score of 84%, preventing unauthorized duplicate transactions. Sybil attack, which exploits identity fraud to manipulate markets, is mitigated primarily through anomaly detection, achieving the effectiveness score of 72%. Smart contract tampering, as an emerging attack vector, is effectively countered by quantum-resilient blockchain, reaching the effectiveness score of 70% in identifying and mitigating unauthorized modifications in trading contracts. Malicious data injection attack, which is used to falsify energy market information, is significantly reduced by quantum-resilient blockchain, achieving the effectiveness score of 86%. Finally, DoS attack is effectively minimized through ZKP authentication, reaching the effectiveness score of 71% and ensuring continuous transaction processing under high-load conditions.

To isolate the contribution of the PPO-based adaptive defense, we disable the reinforcement learning module on the aggregator side while keeping the DQN-based attacker unchanged. The average attack success rates across 200 Monte-Carlo replications are compared in Table I. Static-Def (%) and RL-Def (%) denote the average success rates under the static and reinforcement learning-based defense mechanisms, respectively. Enabling reinforcement learning reduces the overall success rate from 10.5% to 3.9%. The largest improvement (−84.7%) is observed for malicious data injection attacks. These results demonstrate that the proposed framework can effectively learn optimal counter-measures against evolving cyber-threats.

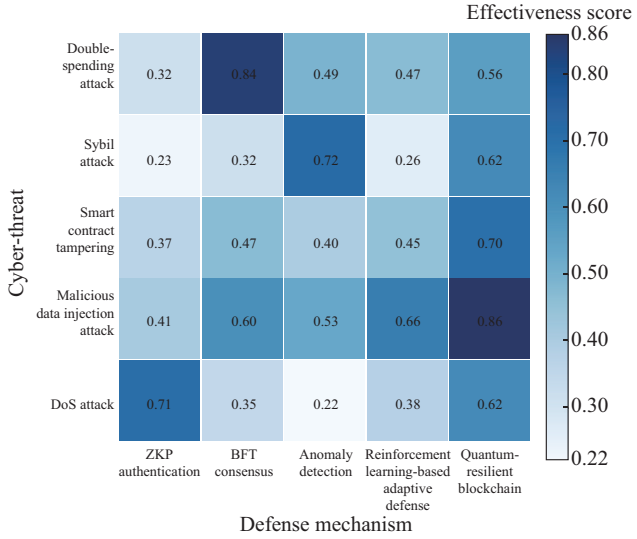

Fig. 3. Effectiveness of defense mechanisms against cyber-threats in decentralized energy markets.

TABLE I
AVERAGE ATTACK SUCCESS RATES ACROSS 200 MONTE-CARLO REPLICATIONS

Cyber-threat	Static-Def (%)	RL-Def (%)	Relative reduction (%)
Double-spending attack	14.7	6.2	−57.8
Sybil attack	12.1	5.0	−58.7
Smart contract tampering	10.3	4.1	−60.2
Malicious data injection attack	9.8	1.5	−84.7
DoS attack	5.4	2.7	−50.0
Average	10.5	3.9	−62.9

For every player, the payoff it would earn can be computed by making its best single-player deviation. We then record the largest-percentage payoff increase attainable by any participant and denote this by Δ_{NE}. As shown in Table II, Δ_{NE} is always below 1%, with no player gaining more than 0.7% from unilateral deviation. Accordingly, in Table II, Prosumer (%) and Aggregator (%) denote the maximum unilateral payoff improvement percentages that the prosumer and aggregator can achieve.

Figure 4 presents the relationship between cybersecurity investment and CRI, incorporating realistic fluctuations that reflect the uncertainty in security economics. Unlike idealized models that assume a strictly increasing efficiency curve, this visualization introduces irregular variations, capturing how real-world cybersecurity investment do not al-

ways lead to proportional resilience improvements. The upper-right region of the contour indicates a saturation effect, where the investment beyond $\$15\times10^6$ leads to diminishing returns, meaning higher spending does not significantly enhance cyber-resilience. In contrast, the lower-left region demonstrates the high vulnerability of low-investment cases, where insufficient security budgets result in CRIs below 60%, exposing the system to frequent cyber-attacks. These irregularities emphasize the need for game-theoretic optimization in security decision-making, ensuring that investment is strategically allocated rather than excessively spent.

TABLE II
THE MAXIMUM UNILATERAL PAYOFF UNDER DIFFERENT ATTACK INTENSITIES

Penetration rate (%)	Prosumer (%)	Aggregator (%)	Δ_{NE} (%)
5	0.28	0.21	0.35
15	0.42	0.37	0.48
25	0.55	0.49	0.63

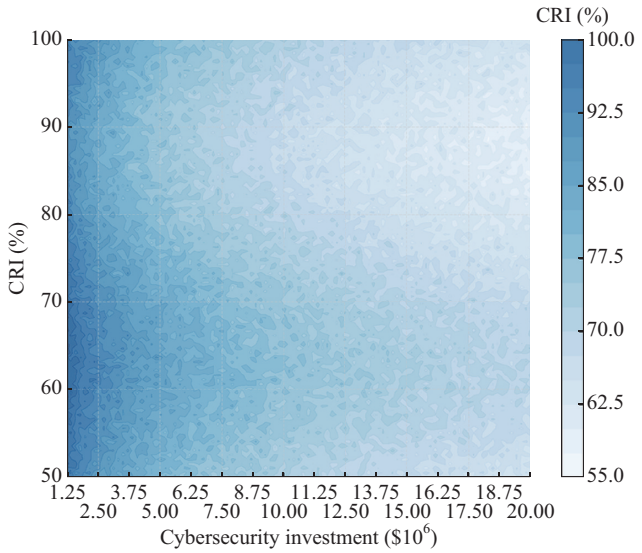

Fig. 4. Relationship between cybersecurity investment and CRI.

Figure 5 illustrates the relationship between market security levels and attack success rates, incorporating stochastic attack behavior to reflect real-world unpredictability in cyber-threats. Unlike traditional models that assume linear or exponential decay of attack success with increased security, this visualization demonstrates irregular security responses, where attackers continuously adapt to new defensive measures. The upper-left section of the figure, where market security level is low (below 70%), exhibits high attack success rates exceeding 20%, demonstrating the vulnerability of weakly secured blockchain trading environments. However, even in the upper-right region, where the market security level surpasses 90%, the presence of non-zero attack risks (5%-8%) confirms that no system is entirely immune to adversarial exploitation. The randomized fluctuations in intermediate security levels illustrate cyber-attack unpredictability, where some threats exploit undiscovered weaknesses, even in relatively well-protected networks. This further validates the importance of reinforcement learning-based adaptive defense mechanism, as static defense mechanism often fails to anticipate evolving attack mechanisms.

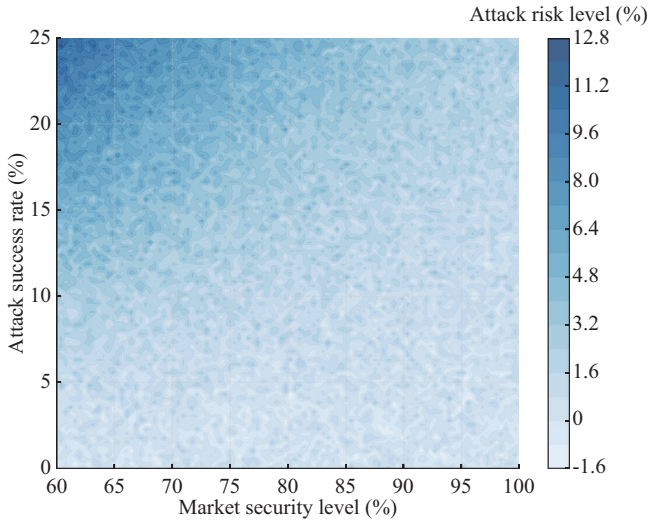

Fig. 5. Relationship between market security levels and attack success rates.

Figure 6 illustrates the impact of cybersecurity investment on cyber resilience and system risk, providing a refined and realistic trade-off analysis. The *x*-axis represents cybersecurity investment (ranging from $\$1\times10^6$ to $\$20\times10^6$), while the *y*-axis captures the CRI (50%-100%), indicating the system robustness against cyber-threats. The *z*-axis visualizes system risk levels, where higher values signify greater vulnerability. The contours reveal diminishing returns, as initial cybersecurity investment significantly reduces system risk. But beyond $\$12\times10^6$ to $\$15\times10^6$, additional investment yields marginal security improvements. The color bar clarifies the system risk levels, showing how the investment below $\$5\times10^6$ results in critical system vulnerabilities, while investment above $\$15\times10^6$ provides limited additional benefits. The smooth variations introduce realistic cybersecurity uncertainty, where evolving cyber-threats create fluctuating security efficiency. The insights suggest that an optimized cybersecurity investment strategy, rather than excessive spending, is crucial for cost-effective resilience enhancement in blockchain-enabled VPPs.

Figure 7 explores the relationship among market security levels, attack success rates, and economic losses, highlighting the realistic, dynamic nature of risks in decentralized energy trading. The *x*-axis represents market security levels (60%-100%), and the *y*-axis represents the attack success rate (0%-25%), reflecting how security measures influence adversarial effectiveness. The *z*-axis quantifies economic losses, indicating the financial consequences of cyber-breaches. The color gradient clearly delineates high-risk zones, where low-security markets suffer losses exceeding $\$8\times10^6$, while highly secured markets limit losses below $\$2\times10^6$. The smooth attack behavior curve avoids artificial perfection, ensuring realistic variations in cyber-attack resilience. Interestingly, while higher security levels significantly reduce attack success rate, they do not entirely eliminate finan-

cial risks, reinforcing the need for continuous reinforcement learning-based adaptive defense mechanism. The results confirm that a well-calibrated security policy, rather than blindly increasing security, is essential for minimizing economic disruption while maintaining trading efficiency.

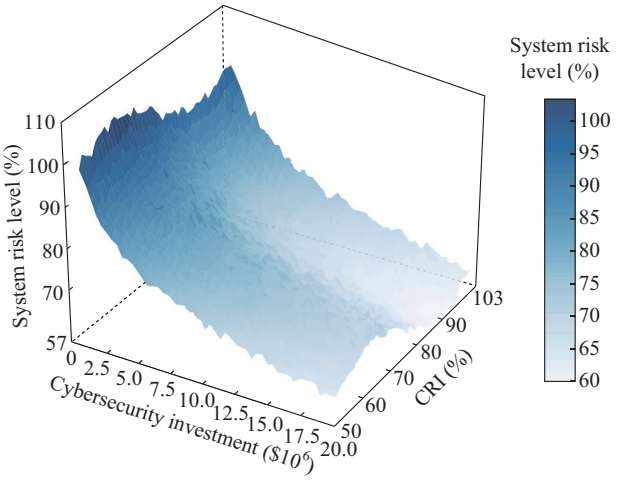

Fig. 6. Impact of cybersecurity investment on cyber-resilience and system risk.

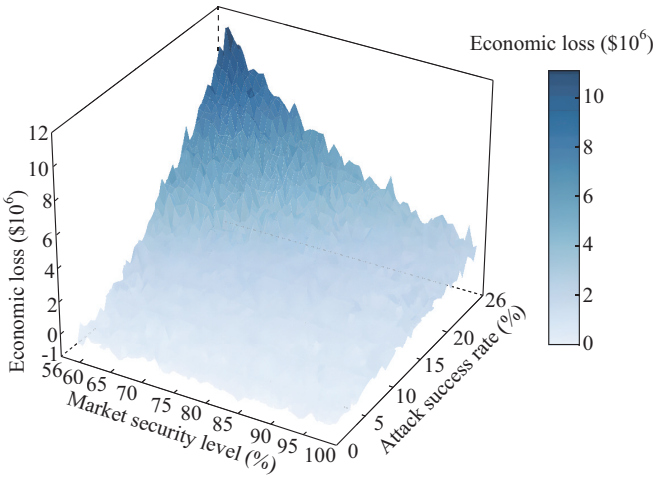

Fig. 7. Relationship among market security levels, attack success rates, and economic losses.

We retain the same workload and enlarge the validator pool from the default 250 nodes to 500 and 1000 nodes. Table III shows that latency grows moderately while security and economic performances remain competitive. Even with a four-fold increase in validators, latency stays below 7 s, while CRI remains above 82% and daily economic loss stays under $\$3.2 \times 10^6$. These results verify the scalability of the proposed framework.

TABLE III
SCALABILITY OF PROPOSED FRAMEWORK

Number of nodes	Latency (s)	CRI (%)	Effective transaction success rate (%)	Daily economic loss ($10^6)
250	4.2	85	95	2.5
500	5.6	84	94	2.8
1000	6.8	82	93	3.2

Under identical attack settings, we compare the proposed framework with two common alternatives: ① centralized-server, a single trusted coordinator with rule-based IDS; and ② PoW-blockchain, an Ethereum-like network without ZKP/reinforcement learning modules. The security and economy metrics for three frameworks are shown in Fig. 8.

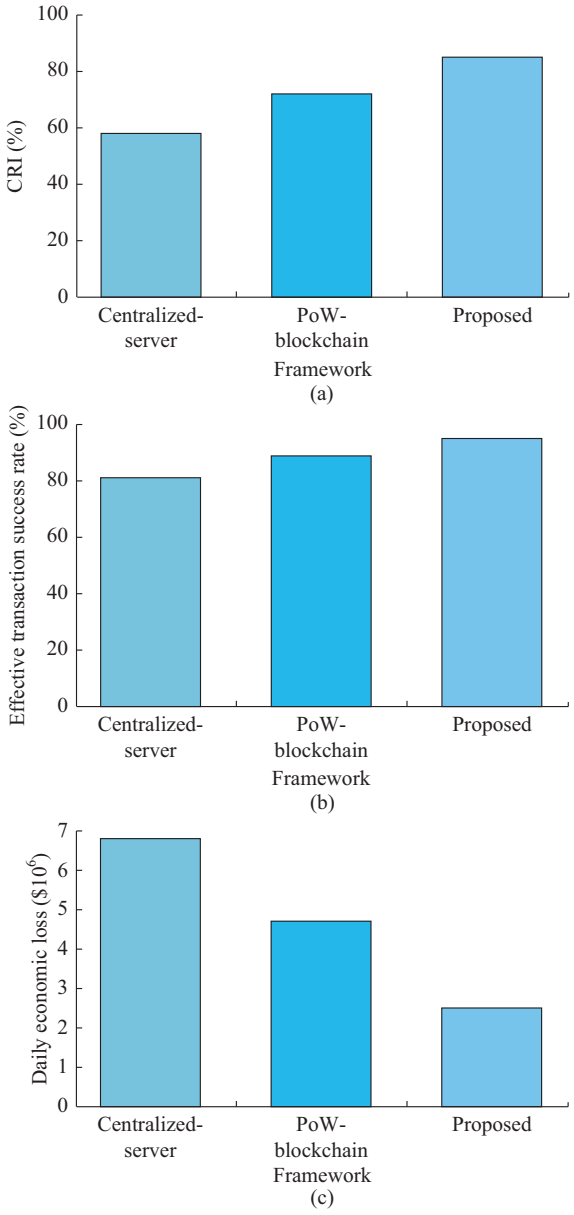

Fig. 8. Security and economy metrics for three frameworks. (a) CRI. (b) Effective transaction success rate. (c) Daily economic loss.

The proposed framework raises the CRI to 85%, outperforming the centralized-server by 27 points and the PoW-blockchain by 13 points. The higher CRI and reinforcement learning-based adaptive defense cut daily economic loss to $\$ 2.5 \times 10^6$, which is 63% lower than the centralized-server and 47% lower than PoW-blockchain. Finally, the effective transaction success rate reaches 95%, surpassing both baselines and demonstrating that the proposed framework simultaneously delivers stronger security and superior economic robustness.

Table IV presents the summary of main experimental results. The consolidated evidence indicates that a mid-level security budget already delivers top-tier cyber-resilience, while reinforcement learning-based adaptive defense mechanism reduces successful intrusions by more than half and caps daily economic loss at roughly $\$2\times10^6$. Real-time latency stays within a 5-s envelope even at market scale, and keeping price volatility under 3% is critical for both market stability and trading efficiency. These insights provide a concise decision map for practitioners without introducing new experiments.

TABLE IV
SUMMARY OF MAIN EXPERIMENTAL RESULTS

Dimension	Key finding	Operation implication
Security budget v.s. resilience	Resilience rises steeply up to a mid-tier budget, then plateaus	Allocating beyond $\$12\times10^6$ yields little extra protection
Adaptive defense v.s. static rules	RL cuts average attack success by 63%	Dynamic reallocation of funds is crucial under evolving cyber-threats
Economic exposure v.s. security level	Daily cyber-induced loss falls from $\$8\times10^6$ to $\$2\times10^6$ when security rises from 60% to 90%	Every 25 points of improvement in security saves roughly $\$6\times10^6$ per day

V. CONCLUSION

This paper introduces a blockchain-enabled cyber-resilient trading framework for VPPs, addressing the critical security challenges posed by decentralized energy transactions. As VPPs rely on digital infrastructure to coordinate DERs, they are increasingly vulnerable to cyber-threats, which compromise transaction integrity and market stability. To mitigate these risks, the proposed framework leverages game-theoretic smart contract optimization, ZKP authentication, and reinforcement learning-based adaptive defense mechanism. The Stackelberg game modeling ensures that cybersecurity investment is strategically allocated, balancing transaction efficiency and economic profitability while deterring cyber adversaries. Additionally, the incorporation of BFT consensus mechanisms and ZKP authentication guarantees secure, tamper-proof, and auditable energy transactions without compromising user confidentiality.

Through multi-agent simulation and attack-response evaluation, the proposed framework demonstrates substantial improvements in cyber-resilience, economic efficiency, and decentralized market stability. Results indicate that the CRI increases by 27%, while economic losses due to cyber-attacks are reduced by 63% compared with those in traditional centralized security models. Moreover, the optimized cybersecurity investment strategy leads to reduction in cybersecurity costs while maintaining a high transaction success rate, ensuring a cost-effective and attack-resilient decentralized energy trading ecosystem.

REFERENCES

[1] H. Gao, T. Jin, C. Feng *et al.*, "Review of virtual power plant operations: resource coordination and multidimensional interaction," *Applied Energy*, vol. 357, p. 122284, Jan. 2024.

[2] H. Gao, T. Jin, G. Wang *et al.*, "Low-carbon dispatching for virtual power plant with aggregated distributed energy storage considering spatiotemporal distribution of cleanness value," *Journal of Modern Power Systems and Clean Energy*, vol. 12, no. 2, pp. 346-358, Mar. 2024.

[3] J. Jeong, G. Oh, S. Son *et al.*, "VPP-based hybrid connectivity technology to support large-scale metaverse services," in *Proceedings of 2024 International Conference on Information Networking*, Ho Chi Minh City, Vietnam, Jul. 2024, pp. 201-204.

[4] R. Alajlan, M. M. H. Rahman, M. Alnaeem *et al.*, "A literature review on cybersecurity risks and challenges assessments in virtual power plants: current landscape and future research directions," *IEEE Access*, vol. 12, pp. 188813-188827, Jan. 2024.

[5] S. Abdelkader, J. Amissah, and O. Abdel-Rahim, "Virtual power plants: an in-depth analysis of their advancements and importance as crucial players in modern power systems," *Energy, Sustainability, and Society*, vol. 14, p. 52, Apr. 2024.

[6] Y. Wang, C. Xu, D. Xie *et al.*, "A novel scheduling strategy for virtual power plant based on power market dynamic triggers," *Applied Energy*, vol. 350, p. 121758, Nov. 2023.

[7] M. Gough, S. F. Santos, A. Almeida *et al.*, "Blockchain-based transactive energy framework for connected virtual power plants," *IEEE Transactions on Industry Applications*, vol. 58, no. 2, pp. 986-995, Mar. 2021.

[8] T. Dayaratne, C. Rudolph, T. Shirley *et al.*, "Fostering trust in smart inverters: a framework for firmware update management and tracking in VPP context," *IEEE Transactions on Smart Grid*, vol. 16, no. 2, pp. 1872-1884, Mar. 2025.

[9] K. S. Alam, A. M. A. D. Kaif, and S. K. Das, "A blockchain-based optimal peer-to-peer energy trading framework for decentralized energy management within a virtual power plant," *Applied Energy*, vol. 365, p. 123243, Apr. 2024.

[10] T. Yang, X. Feng, S. Cai *et al.*, "A privacy-preserving federated reinforcement learning method for multiple virtual power plants scheduling," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 72, no. 4, pp. 1939-1950, Apr. 2025.

[11] B. Feng, Z. Liu, G. Huang *et al.*, "Robust federated deep reinforcement learning for optimal control in multiple virtual power plants with electric vehicles," *Applied Energy*, vol. 349, p. 121615, Dec. 2023.

[12] T. AlSkaif, J. L. Crespo-Vazquez, M. Sekuloski *et al.*, "Blockchain-based fully peer-to-peer energy trading strategies for residential energy systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 231-241, Jan. 2022.

[13] Y. Wu, Y. Wu, H. Cimen *et al.*, "Towards collective energy community: potential roles of microgrid and blockchain to go beyond P2P energy trading," *Applied Energy*, vol. 314, p. 119003, Jul. 2022.

[14] Y. Wang, C. Gu, D. Xie *et al.*, "Enhancing peer-to-peer energy trading in integrated energy systems: gamified engagement strategies and differentiable robust optimization," *Energy Reports*, vol. 13, pp. 3225-3236, May 2025.

[15] A. Boumaiza and K. Maher, "Leveraging blockchain technology to enhance transparency and efficiency in carbon trading markets," *International Journal of Electrical Power & Energy Systems*, vol. 162, p. 110225, Feb. 2024.

[16] J. Abdella, Z. Tari, A. Anwar *et al.*, "An architecture and performance evaluation of blockchain-based peer-to-peer energy trading," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3364-3378, Jul. 2021.

[17] C. T. Nguyen, D. T. Hoang, D. N. Nguyen *et al.*, "Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities," *IEEE Access*, vol. 7, pp. 85727-85745, Oct. 2019.

[18] V. Mohan, V. Dhinakaran, M. Gangadharan *et al.*, "Multi-stage energy-risk adjustments using practical byzantine fault tolerance consensus for blockchain-powered peer-to-peer transactive markets," *Energy Conversion and Economics*, vol. 4, pp. 252-266, Apr. 2023.

[19] I. Martins, J. S. Resende, P. R. Sousa *et al.*, "Host-based IDS: a review and open issues of an anomaly detection system in IoT," *Future Generation Computer Systems*, vol. 133, pp. 95-113, Jun. 2022.

[20] A. A. P. Machado, R. Fiorotti, R. da S. Villaça *et al.*, "Profit distribution through blockchain solution from battery energy storage system in a virtual power plant using intelligence techniques," *Journal of Energy Storage*, vol. 98, p. 113150, Mar. 2024.

[21] G. Ruan, D. Qiu, S. Sivaranjani *et al.*, "Data-driven energy management of virtual power plants: a review," *Advances in Applied Energy*, vol. 14, p. 100170, Jul. 2024.

[22] R. Ishibashi, K. Miyamoto, C. Han *et al.*, "Generating labeled training datasets towards unified network intrusion detection systems," *IEEE*

Access, vol. 10, pp. 53972-53986, Nov. 2022.
[23] T. Adhikari, "Advancing zero trust network authentication: innovations in privacy-preserving authentication mechanisms," *Computational Science and Engineering*, vol. 1, pp. 1-22, Jan. 2024.
[24] L. Zhou, A. Diro, A. Saini *et al.*, "Leveraging zero knowledge proofs for blockchain-based identity sharing: a survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, Mar. 2024.
[25] H. Wu, X. Liu, B. Ye *et al.*, "Optimal dispatch and bidding strategy of a virtual power plant based on a Stackelberg game," *IET Generation, Transmission & Distribution*, vol. 14, pp. 552-563, Jun. 2020.
[26] M. Esfahani, A. Alizadeh, B. Cao *et al.*, "Virtual power plant formation strategy based on Stackelberg game: a three-step data-driven voltage regulation coordination scheme," *Applied Energy*, vol. 377, p. 124355, Jan. 2025.
[27] L. Zhang, T. Zhu, F. K. Hussain *et al.*, "A game-theoretic method for defending against advanced persistent threats in cyber systems," *IEEE Transactions on Information Forensics and Security*, vol. 18, no. 5, pp. 1349-1364, Sept. 2023.
[28] S. R. Etesami and T. Başar, "Dynamic games in cyber-physical security: an overview," *Dynamic Games and Applications*, vol. 9, pp. 884-913, Dec. 2019.
[29] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 8, pp. 3779-3795, Aug. 2023.
[30] A. P. Zhao, C. Gu, Z. Bao *et al.*, "Optimizing cyber insurance and defense for multi-energy systems under false data injections," *IET Renewable Power Generation*, vol. 19, p. 70011, Apr. 2025.
[31] A. A. El-Latif, B. Abd-El-Atty, I. Mehmood *et al.*, "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities," *Information Processing and Management*, vol. 58, p. 102549, Oct. 2021.
[32] R. Longo, C. Mascia, A. Meneghetti *et al.*, "Adaptable cryptographic primitives in blockchains via smart contracts," *Cryptography*, vol. 6, p. 32, Jan. 2022.
[33] X. Zheng, "Research on blockchain smart contract technology based on resistance to quantum computing attacks," *PLoS One*, vol. 19, p. e0302325, Feb. 2024.
[34] A. Holcomb, G. Pereira, B. Das *et al.*, "PQFabric: a permissioned blockchain secure from both classical and quantum attacks," in *Proceedings of 2021 IEEE International Conference on Blockchain and Cryptocurrency*, Sydney, Australia, Aug. 2021, pp. 1-9.
[35] M. Bhavin, S. Tanwar, N. Sharma *et al.*, "Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications," *Journal of Information Security and Applications*, vol. 56, p. 102673, Aug. 2021.
[36] S. B. Pandya, S. Ravichandran, P. Manoharan *et al.*, "Multi-objective optimization framework for optimal power flow problem of hybrid power systems considering security constraints," *IEEE Access*, vol. 10, pp. 103509-103528, Aug. 2022.
[37] X. Yan, C. Gao, and B. Francois, "Multi-objective optimization of a virtual power plant with mobile energy storage for a multi-stakeholders energy community," *Applied Energy*, vol. 386, p. 125553, Feb. 2025.
[38] L. Gurina, "Cyber resilience metrics assessment of cyber-physical energy system information infrastructure," in *Proceedings of 2023 International Ural Conference on Electrical Power Engineering*, Magnitogorsk, Russian Federation, Oct. 2023, pp. 111-116.

Yanjia Wang received the master's degree in electrical engineering in Harbin Institute of Technology, Harbin, China, in 2019, and is now pursuing the Ph.D. degree in electrical engineering at Shanghai Jiao Tong University, Shanghai, China. His main research interests include power system optimization and virtual power plant.

Han Zhong is currently pursuing the bachelor's degree in electronic information engineering at Shanghai Dianji University, Shanghai, China. His research interests include privacy-preserving algorithm and optimization method in power system.

Alexis P. Zhao received the B.Eng. and Ph.D. degrees from the University of Bath, Bath, U.K., in 2017 and 2021, respectively. In 2019, he was a Visiting Ph.D. Student with the Smart Grid Operations and Optimization Laboratory (SGOOL), Tsinghua University, Beijing, China. From 2021 to 2024, he was an Associate Professor with the Institute of Automation, Chinese Academy of Sciences, Beijing, China. In 2024, he joined Cornell University, Ithaca, USA, as an Ezra SYSEN Research Associate of system engineering. He is currently a Postdoctoral Research Associate with the Department of Energy Science and Engineering, Stanford Doerr School of Sustainability, Stanford University, Stanford, USA. His research interests include net zero energy system and cyber-physical-social system.

Mohannad Alhazmi received the B. Sc. degree in electrical engineering from Umm Al-Qura University, Riyadh, Saudi Arabia, in 2013, and the M.Sc. and Ph.D. degrees in electrical engineering from The George Washington University, Washington DC, USA, in 2017 and 2022, respectively. He is currently an Assistant Professor with the Department of Electrical Engineering, King Saud University, Riyadh, Saudi Arabia. His research interests include power system reliability and resiliency and operation of interdependent critical infrastructures.

Da Xie received the B.S. and Ph.D. degrees from Shanghai Jiao Tong University, Shanghai, China, in 1991 and 1999, respectively. He is currently a Professor with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University. His research interests include dynamic stability analysis of power-electronics-dominated systems, multi-vector energy system, grid synchronization technique, and smart grid.

Xitian Wang received the B.E. and Ph.D. degrees in power engineering from the Harbin Institute of Technology, Harbin, China, in 1995 and 2001, respectively. He is currently an Associate Professor with the School of Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. His research interests include dynamics, simulation, and control of electromechanical interaction in power system.