Quantum-Seeded Blockchain Consensus for Secure P2P Energy Trading

Yi Feng
Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University Hong Kong, China
annieyi.feng@connect.polyu.hk

Ziqing Zhu
Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University Hong Kong, China
ziqing-yancy.zhu@polyu.edu.hk

Siqi Bu *
Department of Electrical and Electronic Engineering, The Hong Kong Polytechnic University Hong Kong, China
siqi.bu@polyu.edu.hk

***Abstract*—While blockchain provides a decentralized and transparent framework for peer-to-peer (P2P) energy markets, existing consensus mechanisms fail to simultaneously satisfy the low-latency and high-security requirements of real-time energy trading. We propose the novel Quantum-Seeded VRF (QSV) consensus mechanism, where VRF is a verifiable random function. QSV integrates physical-layer randomness from Quantum Key Distribution (QKD) into the leader election process. It enhances security against computational manipulation and bias by replacing predictable pseudo-random generators with quantum-derived randomness, ensuring fair market participation. The practical viability of QSV is evaluated through extensive P2P market simulations. The results confirm robustness to grinding attacks and a significant reduction in imbalance costs across multiple market scenarios. Consequently, QSV improves fairness and the timeliness of transaction finality in P2P energy markets by combining physical-layer randomness with a low-latency finality mechanism.**

***Index Terms*—Quantum Key Distribution, Blockchain, P2P energy trading**

I. Introduction

The accelerating transformation of modern energy systems, driven by rapid deployment of distributed renewable generation and local storage, has reshaped how electricity is produced, traded, and managed at the distribution level [1]. Historically, distribution networks have depended on centralized authorities to coordinate generation, balancing, and market-clearing results. That centralized model presents significant risks for distributed resources: single points of control, opaque clearing and reconciliation processes, and limited opportunities for P2P energy trading. As more households and businesses become prosumers, P2P energy markets have emerged. P2P market features frequent and bidirectional power flows that are tightly coupled to physical delivery. These characteristics increase operational complexity and raise strict requirements for the timely finalization of trades [2]. To meet these needs, blockchain has been proposed for P2P markets [3], [4]. It lets participants maintain a shared, tamper-evident ledger of trades without a single trusted intermediary, enabling transparent trade resolution, automated billing, and direct trade between peers [5], [6].

However, deploying blockchain in real-time P2P energy markets faces a latency problem at the consensus layer. The consensus mechanism is responsible for agreeing on the definitive order and validity of transactions [7]. Any delay in finalizing a transaction on the blockchain, caused by high latency or low throughput, can lead to a mismatch between the digitally recorded trade and the physical delivery schedule. For instance, if a trade is finalized after its intended delivery window has passed, it creates an imbalance between the scheduled energy exchange and the actual power flow in the grid. Grid operators must then activate expensive reserve power to correct this imbalance, incurring imbalance costs that are ultimately borne by market participants. Therefore, most existing consensus protocols, with their high latency, cannot support large-scale, time-sensitive P2P energy trading [8], [9].

Moreover, existing consensus models suffer from a security problem rooted in pseudo-randomness. To achieve low latency, many protocols employ Verifiable Random Functions (VRFs) for leader election, as demonstrated in [10]–[12]. In these consensus models, leader election is the process of selecting a single validator node that is temporarily granted the authority to propose the next block of transactions for the network to approve. This approach avoids the slow, energy-intensive computational races found in Proof-of-Work, enabling faster block creation. However, their security relies on pseudo-randomness derived from public on-chain data. This creates a critical vulnerability: an adversary with sufficient computational power can pre-compute election outcomes by 'grinding' through potential inputs, thereby biasing the process to their advantage [13]. This risk of computational manipulation is unacceptable in P2P energy trading. Therefore, P2P energy trading requires a fast consensus mechanism founded on an unpredictable source of randomness to prevent computational manipulation.

To overcome these shortcomings, we leverage quantum mechanics by using Quantum Key Distribution (QKD) to provide unpredictable, physical-layer randomness that replaces algorithmic pseudo-randomness in leader election [14]. While current research on quantum and blockchain technologies focuses on applications like quantum signatures or storage, the potential of using QKD-derived randomness to secure the consensus layer has been largely overlooked. Our approach leverages physical-layer randomness from QKD for leader election, achieving two critical properties simultaneously: verifiable fairness through an unpredictable selection process, and low-latency finality essential for P2P markets. The contributions are summarized as follows:

(1) To provide an unpredictable and secure leader election, we propose a physically grounded randomness-driven consen-

979-8-3315-8138-1

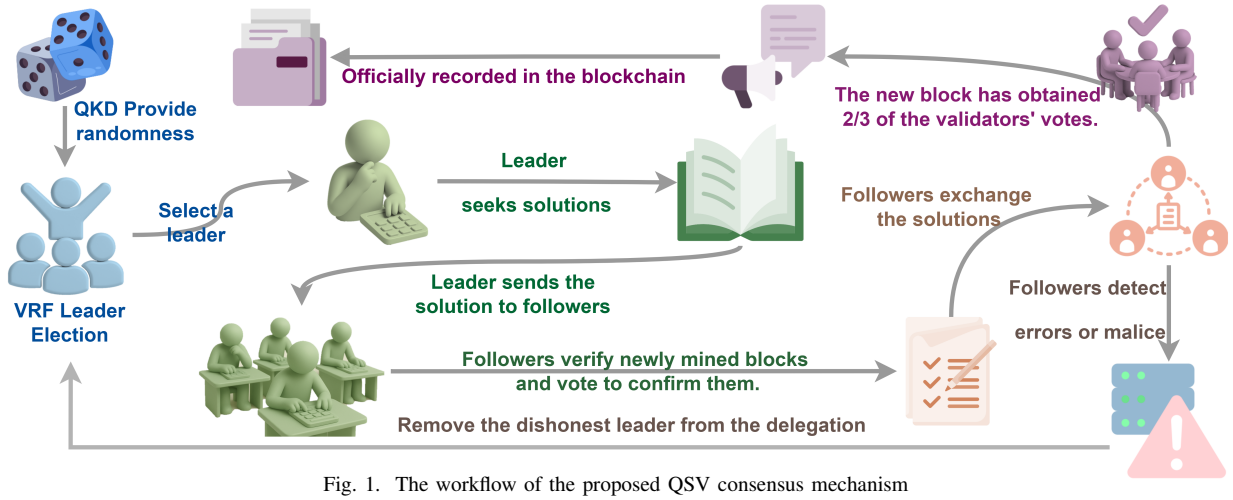

Fig. 1. The workflow of the proposed QSV consensus mechanism

sus protocol. We design a Q-Seed VRF (QSV) consensus, a novel consensus framework that employs physical-layer entropy as the foundation for leader election. The proposed scheme inherently enhances fairness and strengthens security by preventing bias through the use of physical randomness rather than algorithmic pseudo-randomness.

(2) To achieve near real-time finality for P2P trading, we design a lightweight finality model that achieves rapid block finalization. The model's low latency is realized by integrating the QKD-driven leader election with a minimal-message validation scheme. The fairness of the quantum-seeded leader election prevents consensus delays caused by forks or manipulation, while the lightweight validation process significantly reduces the communication overhead inherent in conventional PoS and BFT systems.

(3) We empirically validate the framework through multi-scenario P2P market simulations that model the entire workflow, from the generation of physical-layer randomness via QKD to its application in the QSV consensus. The results demonstrate the framework's robustness against grinding attacks, thereby preserving market fairness. Furthermore, the simulations confirm a significant reduction in imbalance costs under volatile conditions, such as high renewable penetration and network stress, validating the practical viability of QSV.

II. QSV Consensus on P2P Markets

In this section, we present the QSV consensus framework as shown in the Fig.1. Inspired by Proof-of-Work (PoW) and Proof-of-Stake (PoS), we propose a lightweight consensus protocol, termed QSV consensus, to determine how distributed nodes reach agreement on energy transactions. To ensure that the leader election remains unpredictable and verifiable, QSV relies on high-quality random seeds obtained from a physically grounded entropy source, rather than relying solely on algorithmic pseudo-random generators. QSV derives this seed from QKD and releases it as a signed broadcast seed (a signed public seed message) to the network. Validators use the published seed as the input to the VRF to elect the leader for each round, while other nodes only verify the signature and the VRF proof in proposed blocks.

Once the leader is elected, it collects pending transactions and assembles them into a candidate block. The leader then constructs a valid block that satisfies the current consensus conditions (e.g., block validity, timestamp alignment, and reference linkage) and broadcasts this proposal to all validator nodes. These nodes, referred to as followers, independently verify the correctness of the received block, including its transaction integrity, cryptographic signatures, and linkage to the previous block. Each follower subsequently exchanges validation messages with peers to ensure consistency. Through this exchange process, followers can also detect malicious behavior or computational errors originating from the leader. Any dishonest or inconsistent leader is immediately removed from the active validator set, preserving the reliability of the network under Byzantine conditions.

When more than two-thirds of the validators have approved the correctness of the proposed block, the block is considered finalized and is officially recorded in the blockchain ledger. This loop process then restarts with a new round of randomness generation and VRF-based leader election, enabling the system to continuously produce secure and verifiable blocks in near real time.

III. System Model and Security Analysis

In this section, we formalize the system model and security objectives for analyzing QSV, and summarize the timing assumptions, randomness properties, buffering analysis, and security arguments.

A. Network Entities and Architecture

The market is comprised of a network of key participants, which are grouped into logical entity sets:

(i) Market Participants (Operational Nodes, N): This set represents the core entities engaged in energy trading. It primarily includes Prosumers (e.g., households with rooftop solar panels and battery storage) who both generate and consume electricity, and consumers who only consume.

(ii) Validators (V): This is a subset of the Market Participants responsible for maintaining the distributed ledger and executing the consensus protocol.

(iii) Adversaries (A): This set represents potentially Byzantine participants from set N who may attempt to manipulate the market, for example, by trying to influence the leader election to prioritize their own transactions.

In this architecture, QKD generates a public random seed R(t) for the consensus process. The seed is released to the network as a signed broadcast seed. Validators use the seed R(t) to run the VRF-based leader election. End users (prosumers/consumers) do not require direct access to QKD; they submit transactions and verify standard digital signatures as usual.

B. Timing and Communication Model

To follow typical sub-second control intervals adopted in real-time microgrid coordination, the simulation operates in discrete control cycles of 120 ms, each representing one market update cycle.

A logical communication link between nodes i and j has a baseline delay d_c and a bounded jitter ξ_{ij}, such that

$$\mathrm{RTT}_{ij} = d_c + \xi_{ij}, \quad 0 \le \xi_{ij} \le \xi_{\max} = 20 \text{ ms} \tag{1}$$

The expected time to complete a handshake or block proposal round is modeled as

$$\mathbb{E}[T_{\text{op}}] = \mathrm{RTT}_{ij} + \mathcal{O}(1) \tag{2}$$

where $\mathcal{O}(1)$ represents lightweight cryptographic computation that is negligible compared to propagation delay.

C. Model of QKD-Derived Randomness

A QKD session generates a raw bit sequence of length L_0 at time t. The quantum channel exhibits a bit error rate $\epsilon_q(t)$ (QBER). The remaining uncertainty of the raw bits conditioned on the observed error is expressed by the δ_s-smooth min-entropy:

$$H_{\min}^{\delta_s}(X|E) \ge L_0[1 - H_b(\epsilon_q)] - \log_2 \frac{1}{\delta_s} \tag{3}$$

where $H_b(\cdot)$ denotes the binary entropy function.

After privacy amplification via a universal hash extractor, the resulting uniform key length L_e satisfies

$$L_e \le L_0[1 - H_b(\epsilon_q)] - 2\log_2 \frac{1}{\delta_s} - \Gamma \tag{4}$$

where Γ is an implementation margin (typically 64 bits), under standard QKD post-processing. For instance, with $L_0 = 256$, $\epsilon_q = 0.015$, $\delta_s = 2^{-40}$, Eq.(4) yields an upper bound of $L_e \approx 84$ bits of usable uniform randomness, sufficient for short-term consensus seeding. In practice, the consensus seed can be obtained by concatenating multiple extracted blocks.

D. Randomness Buffering and Availability Analysis

As the QKD source generates random bits continuously while the consensus layer consumes them in bursts, a buffering mechanism at the seed publisher (the module that releases the signed broadcast seed to the network) is required to ensure sustainable operation. The seed publisher maintains a finite-capacity queue with size C_{buf}, replenishment rate μ (bits/s), and consumption rate λ (bits/s). The load factor is defined as $\phi = \lambda/\mu$. In our simulation, we set $\mu = 5 \times 10^6$ bits/s (effective rate entering the buffer), and each transaction consumes $k = 256$ random bits. Therefore, the consumption rate satisfies $\lambda = \lambda_{\text{tx}} k$, where λ_{tx} denotes the transaction arrival rate (tx/s).

Assuming Poisson replenishment and Poisson consumption, the steady-state occupancy distribution is approximated by an $M/M/1/C_{buf}$ model:

$$P_s = \frac{(1-\phi)\phi^s}{1-\phi^{C_{buf}+1}}, \quad s = 0, 1, \ldots, C_{buf} \tag{5}$$

The probability that the buffer becomes empty (no random bits available) is

$$P_{\text{idle}} = \frac{1-\phi}{1-\phi^{C_{buf}+1}} \tag{6}$$

To guarantee availability, we impose $P_{\text{idle}} \le \eta$ for a design target η (e.g., 10^{-6}). This yields the minimum required buffer capacity:

$$C_{buf} \ge \frac{\ln\!\left(1 - \frac{1-\phi}{\eta}\right)}{\ln \phi} - 1 \tag{7}$$

valid for $0 < \phi < 1$. This model allows the system designer to trade off QKD generation rate, consumption intensity, and buffer size to avoid entropy starvation.

E. QSV Consensus: Randomness-Driven Agreement

We propose QSV consensus, a lightweight finality protocol integrating QKD-derived seeds into the leader election process. Given the RTT regime assumed in Section III-B, the block interval is taken as 70 ms to accommodate a proposal-and-vote exchange with sufficient margin for propagation and verification.

At block height t, each validator holds its own VRF keypair and forms a slot-specific seed

$$\sigma_t = \mathrm{Hash}(h_{t-1} \parallel R(t)) \tag{8}$$

where h_{t-1} is the previous block header. $R(t)$ denotes the public random seed derived from QKD-generated entropy and published to the network as a signed broadcast seed for round t. Each validator computes

$$\eta_t = \mathrm{VRF}_{\mathsf{sk}}(\sigma_t) \tag{9}$$

and is elected as leader if $\eta_t < \tau_{\text{th}}$, where τ_{th} is tuned to achieve the desired expected proposer rate. As σ_t incorporates fresh QKD-derived randomness via $R(t)$, the adversary cannot bias or precompute leader outcomes before R(t) is released.

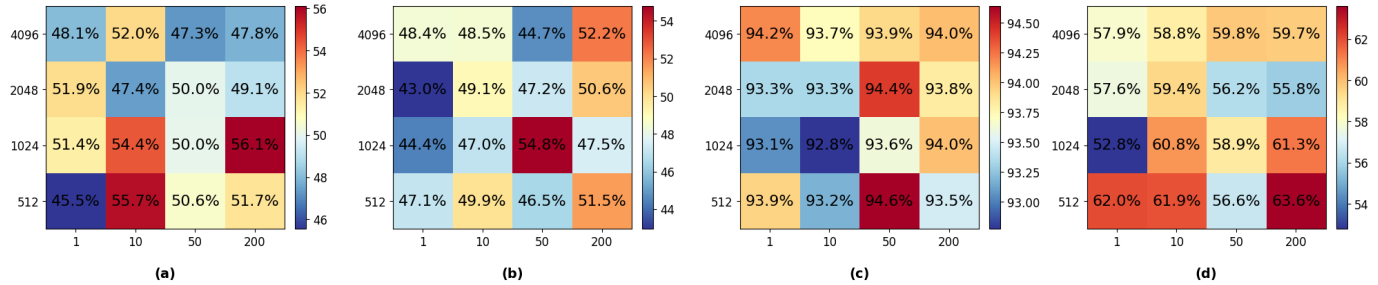

Fig. 2. Heatmaps of QSV improvement over PRNG-based system in imbalance-cost reduction under four scenarios: (a) Baseline, (b) High-renewable, (c) Attack-dominant, and (d) Network-stress. The horizontal axis represents the grinding budget (grind_k) , which denotes the number of attempts or the attack budget an adversary can use for repeated random trials to bias leader election. The vertical axis corresponds to the QKD random buffer capacity, where a larger value means more available quantum random resources. The color scale in each figure shows the average improvement percentage of QSV relative to the PRNG-based system.

Let $X_t \in \{+1, -1\}$ represent block outcomes, where $+1$ indicates an honestly confirmed block and -1 indicates a surviving fork. Define $S_t = \sum_{i=1}^{t} X_i$ as a martingale with bounded increments $|X_{t+1} - X_t| \leq 2$. By the Azuma–Hoeffding inequality,

$$\Pr[S_t \leq -\delta] \leq \exp\Big(-\frac{\delta^2}{2tc^2}\Big) \tag{10}$$

with $c = 2$. For target fork persistence probability 2^{-B}, the confirmation depth satisfies

$$t_{\text{fin}} \geq \frac{B \ln 2}{2(1-2\alpha)^2} \tag{11}$$

where α is the adversarial fraction. For $\alpha = 0.2$ and $B = 40$, one obtains $t_{\text{fin}} \approx 39$ blocks. Under the assumed 70 ms block interval, finality is reached in approximately 2.7 s, consistent with grid-level timing constraints.

QSV consensus integrates physical-layer randomness with verifiable computation, offering fast, bias-resistant, and auditable agreement for P2P energy market.

IV. Experimental Evaluation

Building on analytical models in Section III, We evaluate QSV's practical viability across three critical dimensions. First, we assess its economic benefits via multi-scenario. Second, we validate its low-latency finality using Monte-Carlo analysis. Finally, we confirm its operational robustness by modeling the randomness buffer to quantify the risk of entropy starvation.

A. Multi-Scenario Case Study

We evaluate QSV under four P2P market scenarios: (i) a Baseline market with stable demand and minor renewable fluctuations; (ii) a High-renewable scenario characterized by large renewable penetration and output volatility; (iii) an Attack-dominant scenario where grinding is the primary stressor, modeling adversarial manipulation of leader election through repeated random trials; and (iv) a Network-stress scenario with increased communication latency and congestion.

The resulting heatmaps depict its improvement over the pseudo-random number generator (PRNG)-based system in imbalance cost, as shown in the figure 2. In P2P trading, imbalance cost refers to financial penalties arising from discrepancies between scheduled on-chain transactions and the actual physical delivery of energy. This cost arises from consensus failures: a grinding attack can induce forks or delay finality, causing a participant's transaction to miss the physical delivery window. This failure forces them into a high-penalty real-time balancing market, converting a consensus-layer vulnerability into a direct financial loss.

In the Baseline scenario, QSV provides a significant 45%-57% reduction in imbalance costs under low grinding budget, highlighting the benefits of quantum-seeded randomness for enhancing settlement consistency.

In the High-renewable scenario, we simulate a residential P2P market with a high penetration of rooftop photovoltaics, where the intermittency of renewable sources leads to significant volatility in energy generation and market prices.The heatmap shows that QSV consistently achieves larger improvements in imbalance cost.

The Attack-dominant scenario directly validates QSV's core security advantage. As grinding budget grows, the PRNG-based system's imbalance cost rises sharply. In this context, an adversary attempts to manipulate the leader election process to become the block leader. With QSV, the improvement remains significant as the quantum-seeded constraint prevents adversaries from biasing leader selection through brute force, thereby protecting market security.

Finally, in the Network-stress scenario, which simulates high communication delay and congestion, QSV maintains lower imbalance costs. This performance is crucial for geographically distributed P2P energy markets with varying communication quality.

B. Monte Carlo Evaluation of QSV Reliability Bound

To quantitatively validate that QSV meets the low-latency requirement for P2P energy trading, this section compares its empirical performance against theoretical reliability guarantees. A significant delay in finality causes trades to be missed, directly leading to imbalance costs.

For each configuration of rounds n and input variance, we generate 10^5 samples and computed the empirical tail probability $\hat{P}_{\text{tail}}(\varepsilon)$, defined as the fraction of trials where the

mean deviation exceeded ε. Fig. 3 compares the analytical Azuma–Hoeffding bound with Monte Carlo estimates of the tail probability. The results show close agreement across time horizons.

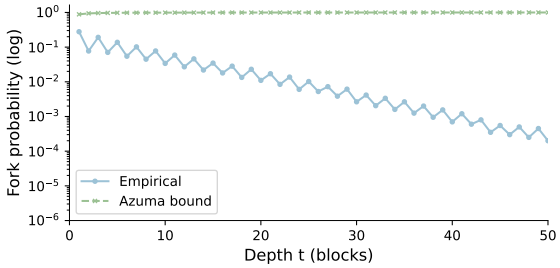

Fig. 3. Azuma Bound vs Empirical Tail Probability

Quantitatively, for $t = 50$ blocks and $\varepsilon = 0.05$, the measured tail probability is approximately 1.3×10^{-4}, while the theoretical prediction is 1.6×10^{-4}, indicating close alignment between empirical and analytical results. Such agreement verifies the soundness of the stochastic formulation and demonstrates that the QSV consensus operates well within its theoretical reliability bound, ensuring temporal stability even under high-variance network conditions.

C. Randomness Buffer Availability

The entire liveness of the QSV consensus hinges on a continuous supply of quantum randomness for leader election, as it is a finite physical resource. A depletion of the random bit buffer leads to a critical failure state, which we term entropy starvation. Consequently, no new leader can be elected and block production halts, leading to a complete freeze of the P2P market.

To validate the practical viability of the QKD-based randomness supply chain, we first evaluate the performance of the randomness buffering mechanism. This mechanism is critical for decoupling the continuous, steady generation of quantum random bits from the bursty, on-demand consumption by the consensus protocol. We model the buffer as an M/M/1/Cbuf queue, as is described in Section III-D, to analyze the probability of entropy starvation (P_{idle}).

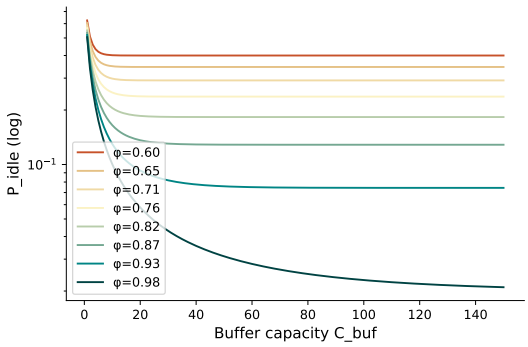

Fig. 4. P_{idle} versus C_{buf} under various load factors ϕ.

As shown in Fig. 4, P_{idle} decays exponentially with C_{buf} across load factors ϕ, confirming the analytical model. The resilience of the system is highly sensitive to ϕ. These results confirm that increasing buffer capacity effectively mitigates outage risk even at $\phi = 0.93$, providing a guideline for system provisioning.

V. Conclusion

This paper presents QSV consensus, a protocol that uses physical-layer randomness from QKD to achieve fairness and near real-time finality in P2P energy trading.

QSV eliminates inherent predictability and computational manipulation risks by replacing algorithmic pseudo-randomness with quantum randomness. Our theoretical analysis, supported by the Azuma-Hoeffding bound, models rapid finality at approximately 2.7 seconds. Simulations demonstrate QSV resilience to grinding attacks and entropy depletion, while reducing imbalance costs across multiple market scenarios. Therefore, QSV is a practical and robust solution for secure P2P energy trading.

References

[1] J. Jasiūnas, P. D. Lund, and J. Mikkola, "Energy system resilience–a review," *Renewable and Sustainable Energy Reviews*, vol. 150, p. 111476, 2021.

[2] T. Sousa, T. Soares, P. Pinson, F. Moret, T. Baroche, and E. Sorin, "Peer-to-peer and community-based markets: A comprehensive review," *Renewable and Sustainable Energy Reviews*, vol. 104, pp. 367–378, 2019.

[3] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019.

[4] P. Arora and R. Nagpal, "Blockchain technology and its applications: a systematic review of the literature," in *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*, 2022.

[5] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and sustainable energy reviews*, vol. 100, pp. 143–174, 2019.

[6] M. Di Pierro, "What is the blockchain?" *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017.

[7] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Applied Sciences*, vol. 11, no. 20, p. 9372, 2021.

[8] A. I. Sanka and R. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *Journal of Network and Computer Applications*, vol. 195, p. 103232, 2021.

[9] M. Bez, G. Fornari, and T. Vardanega, "The scalability challenge of ethereum: An initial quantitative analysis," in *2019 ieee international conference on service-oriented system engineering (sose)*. IEEE, 2019, pp. 167–176.

[10] M. M. Islam, M. M. Merlec, and H. P. IN, "Proof of random leader: A fast and manipulation-resistant proof-of-authority consensus algorithm for permissioned blockchains using verifiable random function," *IEEE Transactions on Services Computing*, vol. 18, no. 3, pp. 1655–1668, 2025.

[11] X. Zhang, R. Li, and H. Zhao, "A parallel consensus mechanism using pbft based on dag-lattice structure in the internet of vehicles," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 5418–5433, 2023.

[12] P. Liu, Y. Xian, C. Yao, P. Wang, L.-e. Wang, and X. Li, "A trustworthy and consistent blockchain oracle scheme for industrial internet of things," *IEEE Transactions on Network and Service Management*, vol. 21, no. 5, pp. 5135–5148, 2024.

[13] K. Kumari and M. K. Murmu, "Leader election in internet of things using blockchain: Issues and challenges," in *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*. IEEE, 2023, pp. 1–7.

[14] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.