Enabling Secure Offline Microgrid Energy Trading Using Commitment Hashes on PureChain

Kalibbala Jonathan Mukisa [1], Love Allen Chijioke Ahakonye [2], Dong-Seong Kim [1] *, Jae Min Lee [1] *
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
* NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National of Technology*, Gumi, South Korea
(kjonmukisa, loveahakonye, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—This study presents an offline-capable blockchain-based peer-to-peer energy trading framework for microgrids. It uses PureChain, a private network that utilizes cryptographic commitment hashes and asynchronous settlement, to ensure security and efficiency. This approach demonstrates resistance to double spending, relay attacks, and decentralized energy management.**

***Index Terms*—PureChain, Commitment Hash, Offline transactions, Microgrid**

I. Introduction

The integration of distributed renewable energy sources has revolutionized traditional electricity markets, enabling prosumers to engage in energy trading, where excess energy is sold to the grid or peers [1]. Blockchain-based peer-to-peer energy trading offers a decentralized solution for managing microgrid energy. However, recent approaches using non-fungible tokens (NFTs) for offline transactions face limitations, such as the inability to split tokens for partial energy trades [2]. Furthermore, intermittent network availability introduces risks such as double spending, replay attacks, and signature forgery, which threaten transaction integrity and hinder broader adoption.

In the work by Wang et al. [2], efficient off-chain micropayment mechanisms are introduced to reduce online dependencies. Jia et al. [1] leverage blockchain and deep reinforcement learning to optimize trading strategies in microgrids. Building on recent findings in energy trading via blockchain, this study presents an offline-capable, blockchain-based peer-to-peer (P2P) energy trading system that utilizes Ethereum smart contracts, cryptographic signatures, and commitment hashes on a PureChain private blockchain [3]. The system enables users to negotiate and sign trades without continuous connectivity, ensuring secure on-chain settlement upon reconnection [4]. With a focus on security against double spending, replay attacks, and signature forgery. The proposed concept enhances the efficiency and resilience of decentralized energy markets, advancing secure and autonomous trading in microgrids.

Proposed Methodology

Figure 1 provides a high-level overview of our methodology, which is built on top of the private PureChain network. Each house operates as a light node in this design, and all

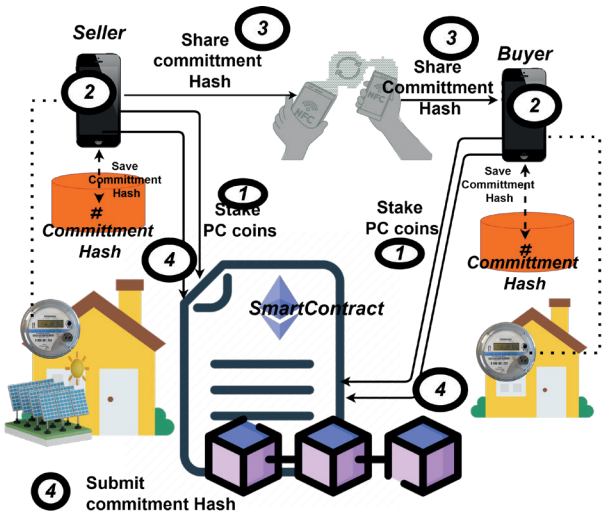

Fig. 1: Proposed System Diagram

participants are identified by their public keys. A quorum of validators enforces network security. Each user's mobile wallet remains synchronized with its associated smart meter, maintaining an up-to-date record of the staked balance. Should a prosumer lose connectivity, the wallet continues to track available collateral and decrements the stake only when transactions are ultimately submitted on-chain.

Our protocol unfolds in three sequential phases. During **Phase I: Collateral Staking**, each participant locks a predefined stake into an Ethereum smart contract to guarantee the integrity of subsequent trades and deter malicious behaviour. After that, in **Phase II: Offline Commitment**, the seller and buyer negotiate trade parameters such as energy volume fully off-chain. They jointly compute a commitment hash encapsulating these values. Each party cryptographically signs the hash with its private key, ensuring non-repudiation and alignment with decentralized security best practices.

Finally, in **Phase III: Asynchronous Settlement**, once network connectivity is restored, either party can submit the signed commitment and trade details to the on-chain contract. The contract's ECDSA-based verification logic authenticates both signatures and records each settlement in a dedicated mapping, thereby ensuring one-time settlement per trade and

safeguarding against double spending and replay attacks.

Results Discussion and Analysis

In the experiment, we invoked *submitCommitment* function with the off-chain commitment hash and associated parameters (seller, buyer, energy amount, timestamp, and both ECDSA signatures). As shown in Figure 2, the transaction was mined successfully in block 4, consuming an average of 5200 gas, confirming both the commitment submission and collateral update as in Figure 3.

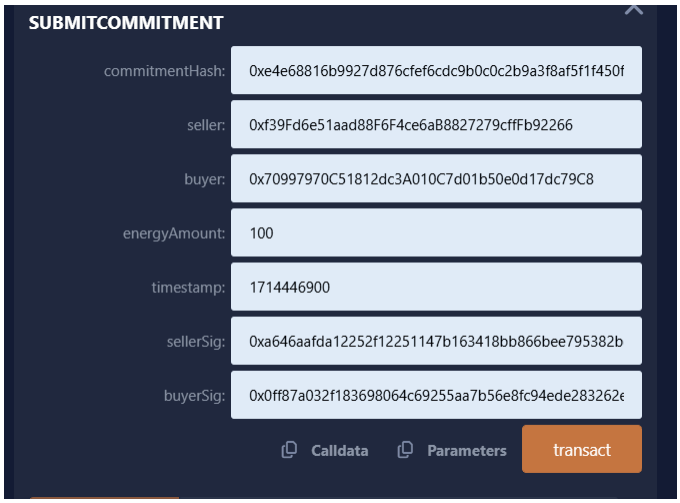

Fig. 2: Remix IDE interface for invoking submitCommitment function

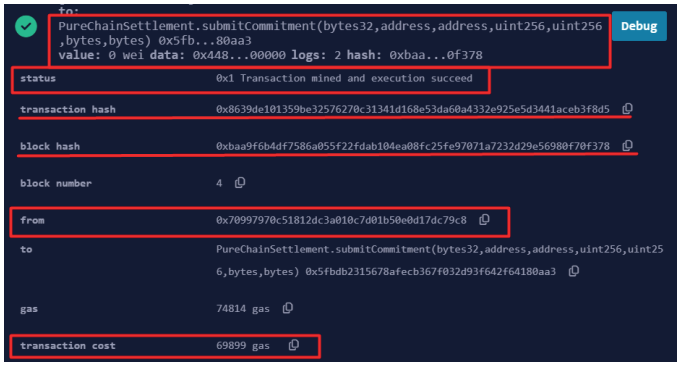

Fig. 3: Transaction receipt in Remix showing successful mining

Figure 4 depicts the on-chain state after the asynchronous settlement of the off-chain commitment. The seller's balance shows 200 PureChain coins, accounting for the 100-coin energy payment and the returned collateral. In contrast, the buyer's balance is 0, indicating that their stake has been fully deducted, including both the trade amount and the bond. The *finalizedCommitments* lookup confirms the commitment hash as true, verifying that the contract has recorded and finalized the transaction once.

Fig. 4: Transaction receipt in Remix showing successful mining

Conclusion

In conclusion, our PureChain-based P2P energy trading system demonstrates robust resistance to double-spending, replay, and signature forgery attacks with efficient settlement and low gas overhead. Its integration of Ethereum smart contracts and cryptographic commitments supports secure, decentralized transactions in intermittently connected microgrids. Consensus protocols need to be optimized, and adaptive security mechanisms need to be integrated. These will ensure the system's adaptability in broader energy markets. The future work of this study is to achieve secure offline real-time analytics integration and AI integration for load balancing.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 25%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 25%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 25%), by the IITP (Institute of Information & Communications Technology Planning & Evaluation)-ICAN (ICT Challenge and Advanced Network of HRD) grant funded by the Korea government (Ministry of Science and ICT) (IITP-2025-RS-2022-00156394, 25%).

References

[1] X. Jia, X. Zeng, J. Xu, L. Yan-hong, Y. Lou, and Z. Xu, "A Microgrid Power Trading Framework based on Blockchain and Deep reinforcement learning," *2023 4th International Conference on Control, Robotics and Intelligent System*, 2023.

[2] N. Wang and C. Chau, "Efficient Off-chain Micro-payment Systems for Blockchain-based P2P Energy Trading," *Companion Proceedings of the 14th ACM International Conference on Future Energy Systems*, 2023.

[3] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, 2024.

[4] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *The 43rd IEEE International Conference on Consumer Electronics (ICCE 2025)*, 2025.