Performing Post-Quantum Transactions on IoTeX (an EVM-compatible chain)

Teik Guan Tan, Praveenaa Umapathy
pQCee

Xinxin Fan
IoTeX

Introduction

Elliptic Curve Cryptography (ECC) is used widely in blockchains to protect its users, assets and transactions. However, the vulnerability of ECC to quantum computers means that blockchains must also migrate to quantum-safe implementations.

In the on-going collaboration [1] between pQCee and IoTeX, we have already worked on addressing real-world challenges beyond simply replacing ECC with a quantum-safe cryptosystem. These include (i) identifying additional migration requirements that are specific to blockchains; (ii) designing new quantum-safe transaction flows that are backwards-compatible to existing blockchains; and (iii) proposing architecture improvements that can optimize on gas usage and performance.

In this poster, we extend the work by demonstrating quantum-safe transactions on the IoTeX testnet. The transaction shown is signed using the classical Elliptic Curve Digital Signing Algorithm (ECDSA) but augmented with a quantum-safe zero-knowledge proof to ensure that such transactions cannot be spoofed even with a quantum computer. A link to the transaction on the IoTeX testnet as well as the video carrying out the transaction are included.

Post-Quantum Challenge for Blockchains

The blockchain is a decentralized computing paradigm made popular by Bitcoin, a cryptocurrency that was introduced by Satoshi Nakamoto in the early 2000s and has grown over the past 20+ years to one of the most successful distributed systems to date. The combined transaction volume on the various public blockchains (such as Bitcoin, Ethereum, Solana, BNB, etc) far exceed hundreds of millions per day, with transaction value already comparable with more traditional VISA and Mastercard payment networks.

A very large majority of blockchains rely on ECDSA or its variants to ensure the integrity, authenticity and non-repudiation of transactions originating from the wallets to the validating nodes. When cryptographically-relevant quantum computers (CRQC) are available within the next 3 to 10 years, a malicious actor will be able to exploit the cryptographic weakness of ECDSA and create fake digital signatures to effect fraudulent transactions on the blockchains resulting in a catastrophic erosion in trust. Yet, completely replacing the use of ECDSA with newer quantum-safe digital signing algorithms such as MLDSA or SLHDSA may not be as straight-forward[2]. This is because of:

Large Number of Legacy Users

- There are hundreds of millions of public blockchain wallets (e.g., over 50 million Bitcoin, 100 million Ethereum wallets). To get the wallet owners to migrate will result in more scammers trying to take advantage of the confusion.
- Many of these wallet owners may not be keeping up with technology or sufficiently savvy to know how to carry out the migration

Linkage of Key with Wallet Address

- The wallet address is a hash of the ECDSA public key. Changing the algorithm will result in a mismatch of the address, which will impact transactions and Smart-contracts that have hardcoded addresses

Addressing these additional requirements is critical to the success of migrating public blockchains to post-quantum readiness.

Quantum-safe Backwards compatibility

Blockchains already have built-in agility to support new quantum-safe transaction signing algorithms by (1) introducing new wallet types and what verification algorithms are linked to these new wallet types; and (2) doing a hard-fork to disable unsafe wallet types. Hence, how quickly can the millions of users transfer assets from the existing (quantum-unsafe) wallets to these quantum-safe wallets given the relatively short migration period becomes the challenge. If not migrated in time, the existing assets become lost or destroyed which will likely result in unhappiness or worse impact to the user community.

The need to include a quantum-safe backwards compatibility mechanism to authenticate users with quantum-unsafe wallets is crucial in the migration process:

- **Longer migration timeline.** Blockchains can allow users more time to migrate their wallets which will result in better management of potential scams and user experience. This is also useful if the "Q-Day" quantum timeline happens faster than expected.
- **Support legacy smart contracts.** Smart contracts that have hardcoded wallet addresses can continue to operate since the wallet owners can be quantum-safely authenticated.

Transaction signing in EVM chains

Most key generation in wallets follow the Bitcoin Improvement Proposal (BIP) 39 process where a sequence of human-readable words are randomly selected from a 2048-word list, and used as a deterministic Seed phrase (with an optional user-selected password) to derive the actual ECDSA private key. This allows for the concept of cold wallets or paper wallets where users simply store the Seed as a recovery phrase offline, physically secure from the Internet.

$$\text{Wallet Private Key } K_{Prv} = \text{PBKDF2}(\text{Seed} + \text{Pwd})$$
$$\text{Wallet Public Key } K_{Pub} = K_{Prv} * \text{Basepoint } G$$
$$\text{Wallet Addr} = \text{Truncate}(\text{Keccak256}(K_{Pub}))$$

$$\text{Seed} = "s_1\ s_2\ \ldots\ s_n" \text{ where } s_i \in \text{Wordlist}$$
$$\text{Wordlist} = \{\text{abandon, ability, ..., zoo}\}$$
$$\text{Pwd} = \text{User password (can be blank)}$$

To send a message to the chain, the user uses the Wallet Private Key K_{Prv} to sign a hash of the message containing the transaction. This transaction is associated to the wallet address which is determined by the hash of the public key.

Since a CRQC can be used to compute K_{Prv} from the public key K_{Pub}, we require the use of pQCee's patent-pending Signature Pre-image Proof (SPP) to include a zero-knowledge proof (ZKP) of the Seed phrase to accompany the transaction. In our implementation, we have chosen to use the zkSTARK zero-knowledge proof system which is quantum-safe.

$$\text{Quantum-safe Signature} = \text{secp256k1}(\text{Keccak256}(M), K_{Prv}) + \text{SPP Proof}$$

$$M = \text{Message containing the transaction}$$
$$\text{SPP Proof} = \text{zkSTARK}(\text{Seed+Pwd}, M, \text{Wallet Addr})$$

Quantum-safe Transactions on IoTeX

To include the additional SPP Proof protecting the transaction, we implemented a type 0x02 Transaction under EIP-1559 which was introduced to address network congestion and overpricing of transaction fees caused by the historical fee market.

We carried out a live transaction on the IoTeX testnet and the flow is shown in the next section under "SPP Wallet for IoTeX". The SPP Proof is generated using RISC0 and included as an EIP-4844 blob without any change needed to IoTeX. You can explore the transaction by referring to the IoTeX scan:

https://testnet.iotexscan.io/tx/0x9bcfdac80cb2b265bd79a65ffba90bf797cda853d1d4774f3bd9cfde29f53784

We also explored how to optimize the gas usage and performance of the setup. This can be done by (1) introducing new transaction types that augment each existing transaction type with a new parameter **proofUri** which contains the URI of the SPP Proof; and (2) employing Layer-2 zk-Rollup architecture and process augmented legacy transactions in batch. These are shown in Fig 1 and 2 respectively.

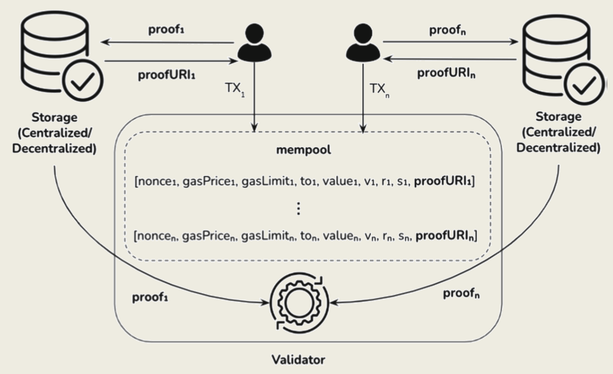


Fig 1. The Process of Augmented Legacy Transactions

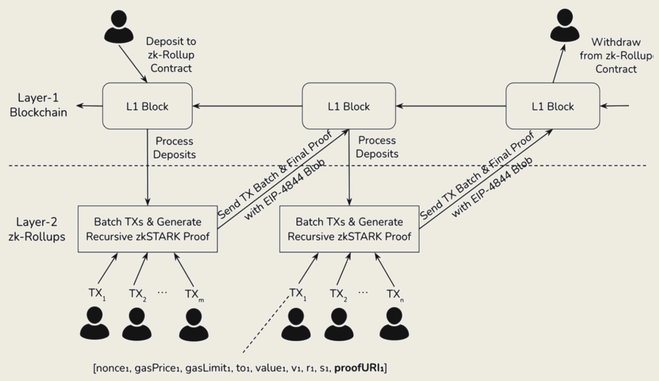
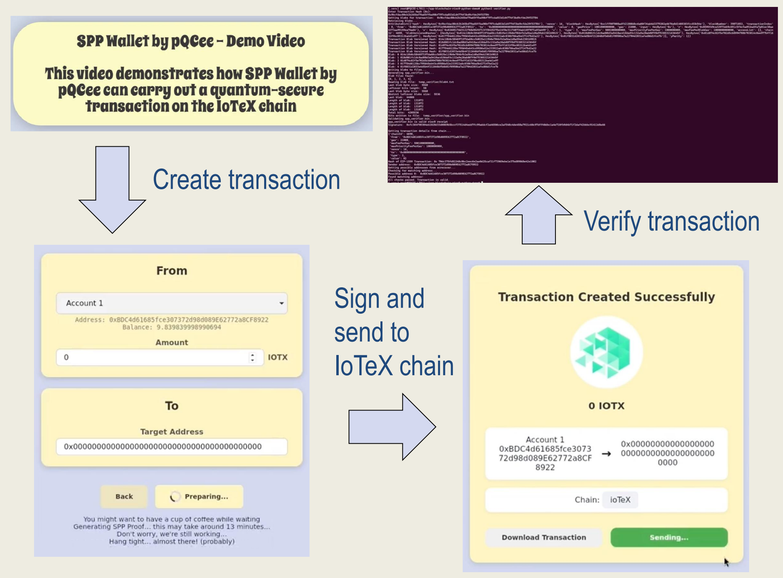


Fig 2. Scalable Process of Augmented Legacy Transactions with zk-Rollups

The technical details of the proposal are captured in the draft EIP-7693 [3] submitted for consideration.

SPP Wallet for IoTeX



The video walkthrough of the SPP Wallet for IoTeX is available at:
https://www.youtube.com/watch?v=Io-q4C2OEIM

References

[1] Fan, Xinxin, Teik Guan Tan, Nicholas Ho, and Shi Hong Choy. "Enabling a Smooth Migration Towards Post-Quantum Security for Ethereum." In *International Conference on Blockchain*, pp. 3-15. Cham: Springer Nature Switzerland, 2024.

[2] Tan, Teik Guan, and Jianying Zhou. "Migrating blockchains away from ECDSA for post-quantum security: a study of impact on users and applications." In *International Workshop on Data Privacy Management*, pp. 308-316. Cham: Springer International Publishing, 2022.

[3] Tan, Teik Guan, Nicholas Ho, Xinxin Fan, Xueping Yang. "Backward Compatible Post Quantum Migration" EIP-7693 Draft. Available at https://github.com/pqcee/EIPs/blob/master/EIPS/eip-7693.md

About IoTeX

IoTeX is the blockchain platform for Real-World AI. Since 2017, its foundational infrastructure has delivered verified, real-time data from the real world to AI systems and decentralized applications. Powering 100+ projects and 40M devices across mobility, robotics, energy, health, and more, IoTeX enables developers to build next-gen AI models and applications that deliver real-world impact.

Xinxin Fan
@Cryptoecc
xinxin@iotex.io
www.iotex.io .

About pQCee

pQCee is a quantum cybersecurity technology provider. We design and build post-quantum products and solutions to strengthen and protect the $trillion digital economy against quantum attacks.

Solutions by pQCee include (i) SafeQuard, for quantum-safe encryption against harvest-now-decrypt-later attacks; (ii) QKDLite, for key management and connectivity to quantum technologies; (iii) PacketQC, for cryptographic discovery, inventory and validation; and (iv) QuICScript, a quantum-simulator for quantum cryptanalysis and threats.

Teik Guan Tan
@tanteikg
teikguan@pqcee.com
www.pqcee.com