Quantum capabilities Working Group

1. Motivation

The goal is to start testing quantum capabilities in the LACChain network, as an effort towards making it quantum safe (resistant to quantum computers). As it was addressed in our publication last year[1], there are different areas where quantum computers threaten blockchain technology, all of them related to the use of RSA and ECC cryptography both by the internet and by blockchain software. We want to start exploring how to move towards a new generation of quantum-safe blockchain technology.

2. Main Goals

- Issuance of W3C Verifiable Credentials[2] using post-quantum cryptography to authenticate nodes.
- Encapsulate TCP/RPLx communication with quantum keys using OpenSSL.
- Use certificates to sign transactions by writer nodes.

3. Participants

- Tech Lead: Diego López León
- Coordinator: Antonio Leal Batista
- Supervisor: Marcos Allende Lopez
- Partners:
  - Cambridge Quantum Computing
  - Idemia
  - Technical Institute of Monterrey
  - Consensys
  - Everis
  - IADB

4. Detailed description

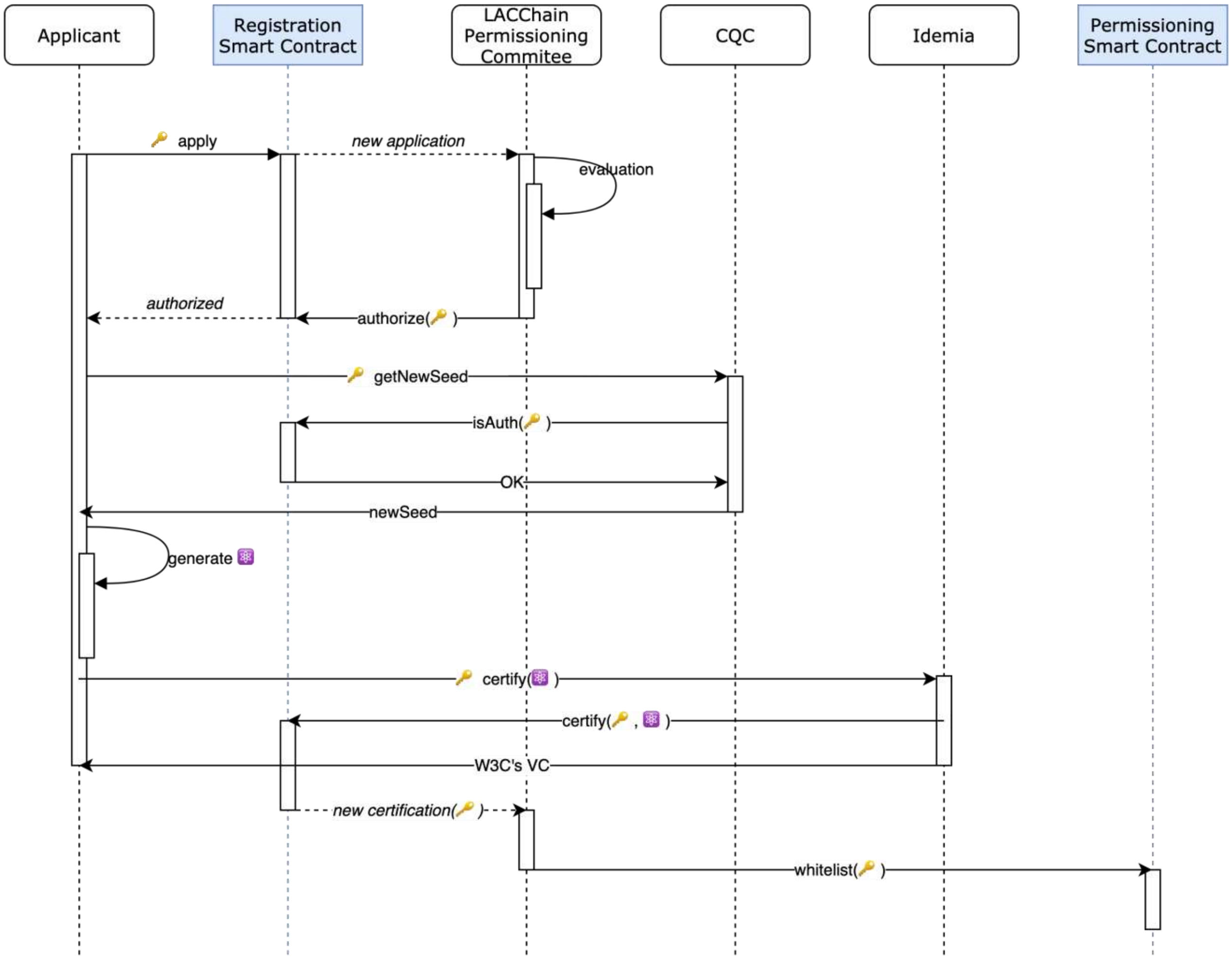
4.1. Verifiable Credentials provisioning

The LACChain Ethereum network uses an on-chain permissioning mechanism provided by the Hyperledger Besu implementation.

[1] https://publications.iadb.org/es/tecnologias-cuanticas-una-oportunidad-transversal-e-interdisciplinar-para-la-transformacion-digital
[2] https://www.w3.org/TR/vc-data-model/

We aim to improve the process for when an applicant gets permission to operate in this network by providing a W3C Verifiable Credential.

In this working group we propose the implementation of a smart contract to support the registration of post quantum signatures for each approved account. It will interact with the permission smart contracts[3] to whitelist the applicant *enode* id once a post quantum credential is certified.



Technical milestones:

- Implement *registration* smart contract
  - This smart contract will receive the application filled with all the necessary information for its evaluation by the LACChain Permissioning Committee. It should emit an event to trigger an internal process.
  - The account sending the application to the smart contract, will be the one whitelisted.

[3] https://github.com/PegaSysEng/permissioning-smart-contracts

- Implement LACChain Permissioning Committee application for tracking and authorize applications.
    - This application should listen to the LACChain Ethereum network for pending applications and feed a dashboard for the LACChain Permissioning Committee to decide. Once the applicant is authorized, the application should mark the account into the *registration* smart contract.
- Implement CQC IronBridge gateway
    - This gateway is an HTTP interface receiving a POST message signed with secp256k1. It should extract the account from the message and check the *registration* smart contract if this account was previously authorized, if authorized the gateway will provide a quantum entropy seed.
- Implement Idemia gateway
    - This gateway is an HTTP interface receiving a POST message with a secp256k1 signed post quantum public key. It should extract the account from the message and if the account is authorized, the gateway should register the post quantum public key in the *registration* smart contract.
    - Once the post quantum public key registration occurs, it should return a W3C Verifiable Credential for verifying both, the secp256k1 and the post quantum key.
- Implement LACChain Permissioning Committee daemon for whitelisting accounts when they have the proper post quantum key certified.

4.2. TCP/RLPx post quantum encapsulation

The RLPx transport protocol is a TCP-based transport protocol used for communication among Ethereum nodes. The protocol carries encrypted messages using the ECIES method and all cryptographic operations are based on the secp256k1 elliptic curve. These operations are easily reversible by quantum computers exposing the network to security breaches.

As the LACChain Network is permissioned, the topology is known and well defined between the core nodes. The idea of this working group is to open quantum-safe TLS tunnels between peers so the RLPx messages can go through it.

Technical milestones:

- Build and install a modified version of the OpenSSL toolkit.
- Investigate 2-way TLS proxy solutions.
    - The selected solution must use the OpenSSL library for cryptography.
- Open a 2-way TLS proxy tunnel between the whitelisted nodes of the LACChain network.
- Write a technical paper describing the solution and its benefits.

4.3. Writer nodes permissioning

The LACChain Ethereum test-net is permissioned and any participant can send transactions to the network. This opens the possibility, e.g, of permissioning an Observer node to behave beyond its assigned capabilities.

A mechanism for solving this is proposed by the Consensus Protocol working group, but under this working group the proposal is to sign the data sent to a smart contract using the post quantum credential associated to the writer node key. Then, this signature can be validated on-chain by the relay smart contract.

Technical milestones:

- Define a proper way to sign a meta-transaction.
- Implement an EVM compatible post quantum signature validation.