Cyberscope

Audit Report

Ozone Chain

September 2022

Github https://github.com/Ozone-chain Ozonechain & ozonechain_quantum/tree/testnet

Audited by © cyberscope

Table of Contents

Review

Github	https://github.com/Ozone-chain/Ozonechain
Commit	296025865fd49fb8600b12f149e2578e06f732f3
Github	https://github.com/Ozone-chain/ozonechain_quantum/tree/testnet
Commit	77d06a9f7384205e36ef4c3d75f1dc4c913590c2
Licence	Apache License 2.0
Forked	https://github.com/hyperledger/besu
Programming Language	Java

Introduction

Ozonechain is an Apache 2.0 licensed, MainNet compatible, Ethereum client written in Java.

Ozonechain includes a command line interface and JSON-RPC API for running, maintaining, debugging, and monitoring nodes in an Ethereum network. Users have the ability to use the API via RPC over HTTP or via WebSocket. Ozonechain also supports Pub/Sub. The API supports typical Ethereum functionalities such as:

- Ether mining.
- Smart contract development.
- Decentralized application (dapp) development.

The Ozonechain is enriched with extra security features that are based in the randomization that quantum principals provide. There are two basic concepts that has been implemented. The Post Quantum Cryptography (PQC) and Quantum Random Numbers (QRN).

Quantum

Ozone chain uses quantum security technologies like post-quantum cryptography (PQC) and quantum random number generators (QRNG) to secure its digital assets.

Quantum Random Numbers (QRN)

Ozone chain uses QRNs in its cryptographic protocols to generate seeds, initial random values, nonces (salts), blinding values and padding bytes and perform hashing and encryption.

The QRNs are created by single photon splitting. A laser produces a stream of the elementary particle, photon. The photons generated from the laser are used to generate the random numbers.

Post-quantum cryptography (PQC)

Ozone chain uses a variant of Post Quantum Cryptography called lattice based cryptography.

Ozone chain uses a standardized and NIST-approved public-key encryption and key-establishment algorithm called NTRU.

Ozone nodes communicate with each other through a specially created bi-directional quantum tunnel that deploys lattice based cryptography to encrypt and decrypt data.

Quantum Resistant Certificate

Quantum cryptography is cryptographic algorithms (sometimes referred to as quantum-resistant), usually public-key, that are thought to be secure against a cryptanalytic attack by a quantum computer. The problem with currently popular algorithms is that their security relies on one of three hard mathematical problems:

- The integer factorization problem
- The discrete logarithm problem
- The elliptic-curve discrete logarithm problem.

The Ozone Chain algorithms are trying to address these issues with advanced techniques, in the boundaries of a non-quantum computing system.

Blockchain

Private networks

The users can create or join a private, permissioned network. Use private networks to develop enterprise applications requiring secure, high-performance transaction processing.

Public networks

Run Ozonechain as an execution client on Ethereum Mainnet and Ethereum public testnets, such as Goerli and Sepolia.

Ozonechain for private networks

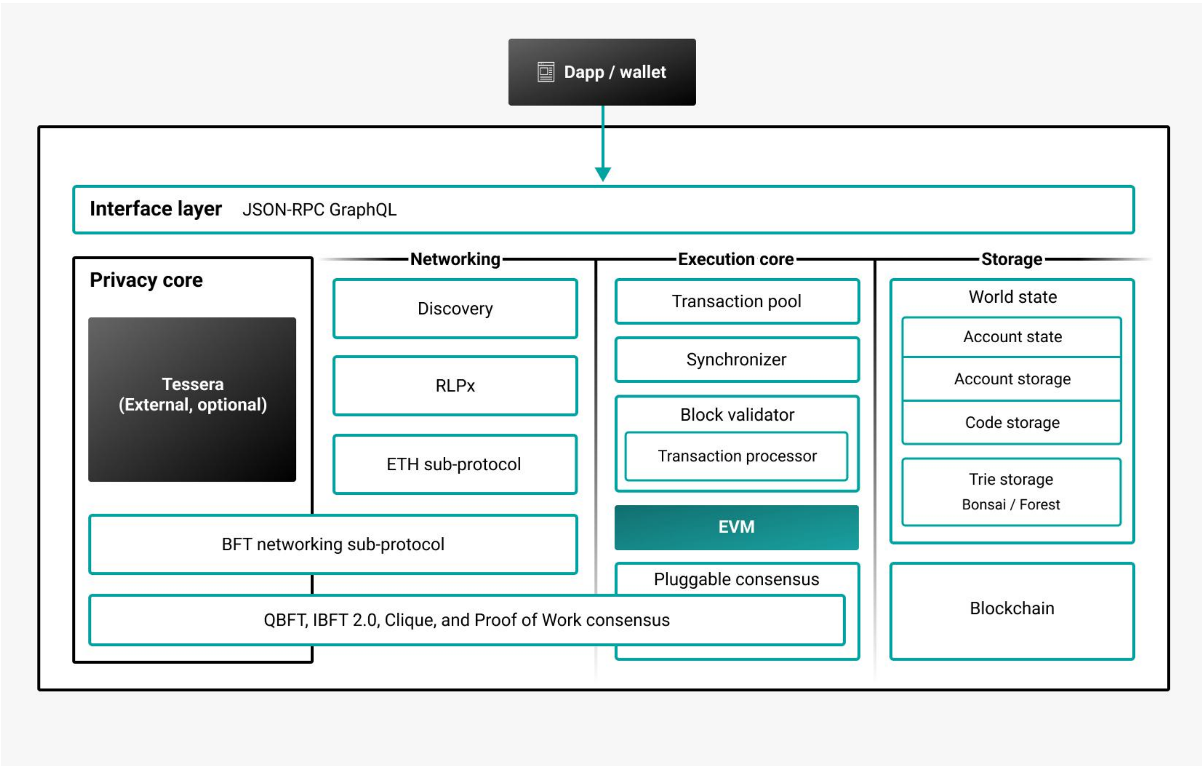
A private network is a network not connected to Ethereum Mainnet or an Ethereum testnet. Private networks typically use a different chain ID and proof of authority consensus (QBFT, IBFT 2.0, or Clique).

Users can also create a local development network using proof of work (Ethash).

Ozonechain supports enterprise features including privacy and permissioning.

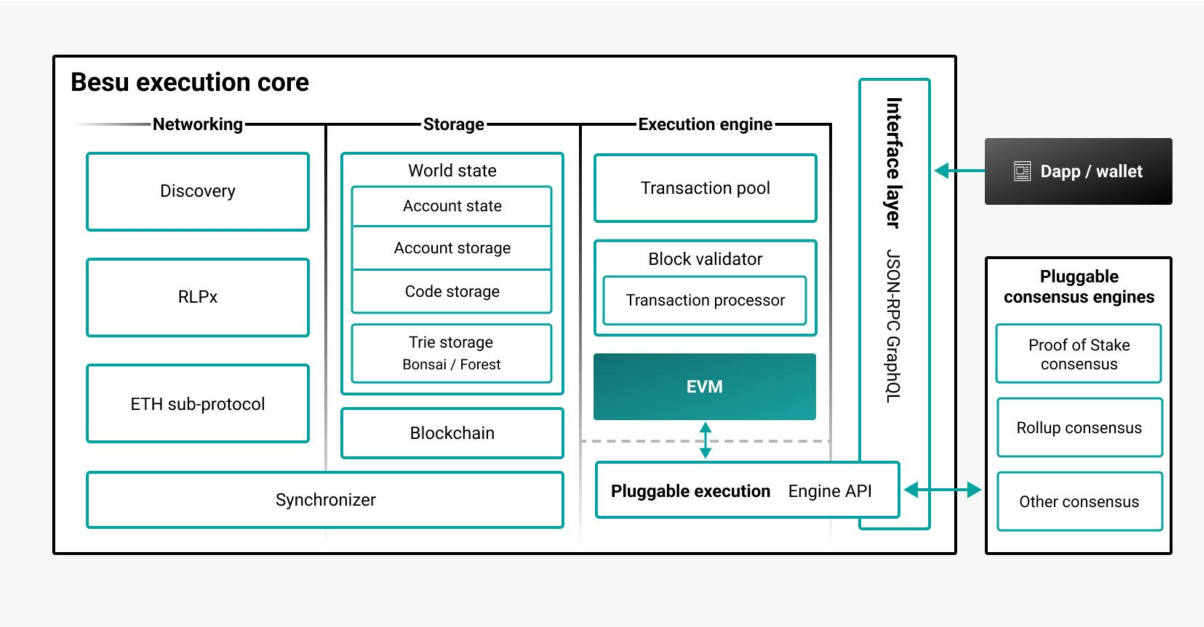
Architecture

The following diagram outlines the high-level architecture of Ozonechain for private networks.



Ozonechain for public networks

Ozonechain serves as an execution client on public proof-of-stake Ethereum networks such as Ethereum Mainnet, Goerli, and Sepolia.



Ozonechain implements the [Enterprise Ethereum Alliance] (EEA) specification. The EEA specification was established to create common interfaces amongst the various open and closed source projects within Ethereum, to ensure users do not have vendor lock-in, and to create standard interfaces for teams building applications. Ozonechain implements enterprise features in alignment with the EEA client specification.

Ozonechain’s features

- The Ethereum Virtual Machine (EVM): The EVM is the Turing complete virtual machine that allows the deployment and execution of smart contracts via transactions within an Ethereum blockchain.
- Consensus Algorithms: Ozonechain implements various consensus algorithms which are involved in transaction validation, block validation, and block production (i.e., mining in Proof of Work). They include:
  - Proof of Authority: Ozonechain implements several Proof of Authority protocols. Proof of Authority consensus protocols are used when participants are known to each other and there is a level of trust between them—in a permissioned consortium network, for example.
  - IBFT 2.0: In IBFT 2.0 networks, transactions and blocks are validated by approved accounts, known as validators. Validators take turns creating the next block. Existing validators propose and vote to add or remove validators. IBFT 2.0 has immediate finality. When using IBFT 2.0, there are no forks and all valid blocks are included in the main chain.
  - Clique: Clique is more fault-tolerant than IBFT 2.0. Clique tolerates up to half of the validators failing. IBFT 2.0 networks require greater than or equal to ⅔ of validators to be operating to create blocks. Clique does not have immediate finality. Implementations using Clique must be aware of forks and chain reorganizations occurring.
  - Proof of Work (Ethash): Proof of Work is used for mining activities on mainnet Ethereum.
- Storage: Ozonechain uses a RocksDB key-value database to persist chain data locally. This data is divided into a few sub-categories:
  - Blockchain: Blockchain data is composed of block headers that form the “chain” of data that is used to cryptographically verify blockchain state; block bodies that contain the list of ordered transactions included in each block; and transaction receipts that contain metadata related to transaction execution including transaction logs.
  - World State: Every block header references a world state via a stateRoot hash. The world state is a mapping from addresses to

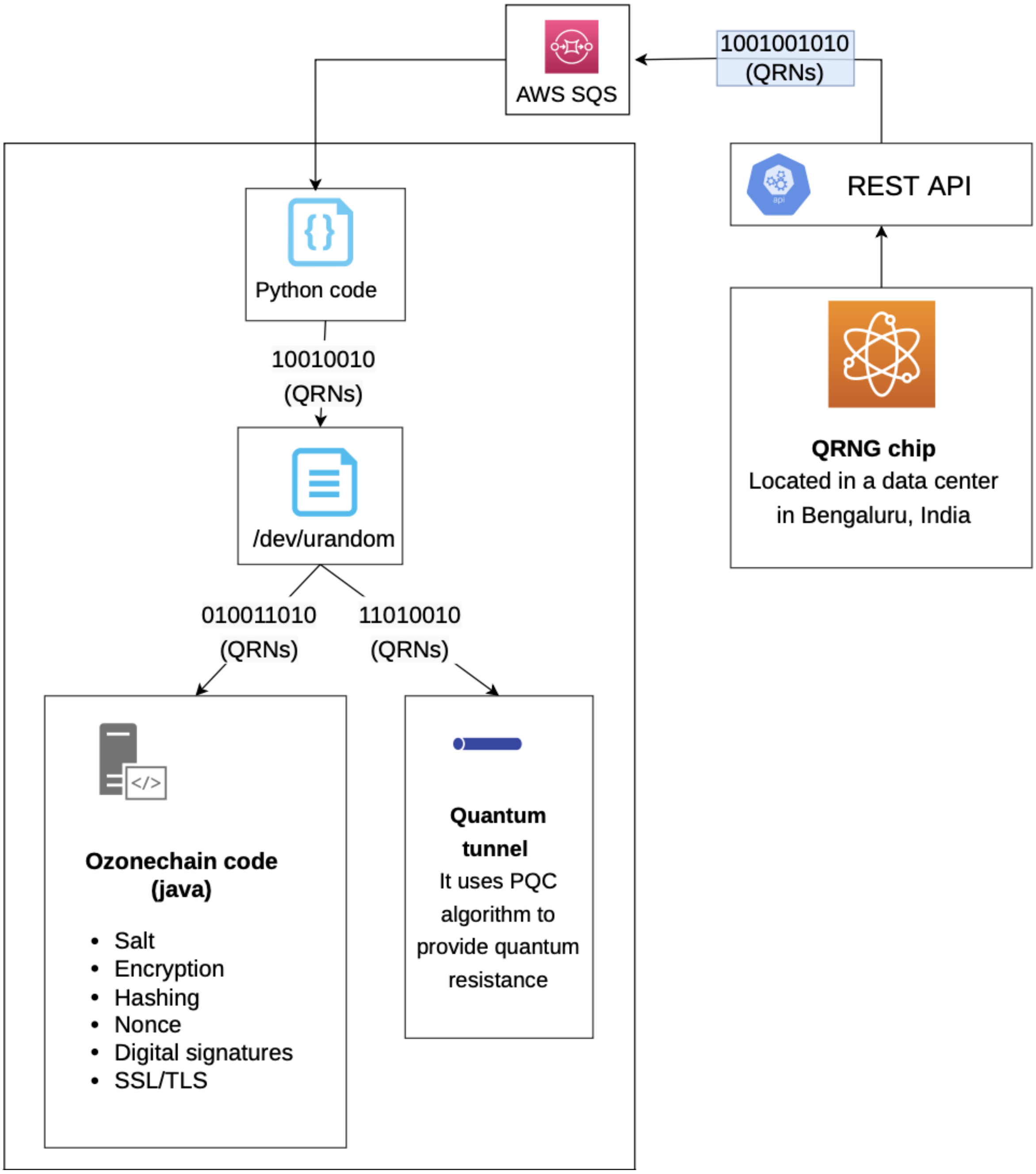
accounts. Externally owned accounts contain an ether balance, while smart contract accounts additionally contain executable code and storage.

- P2P networking: Ozonechain implements Ethereum's devp2p network protocols for inter-client communication and an additional sub-protocol for IBFT2:
    - Discovery: A UDP-based protocol for finding peers on the network
    - RLPx: A TCP-based protocol for communication between peers via various "sub-protocols":
        - ETH Sub-protocol (Ethereum Wire Protocol): Used to synchronize blockchain state across the network and propagate new transactions.
        - IBF Sub-protocol: Used by IBFT2 consensus protocol to facilitate consensus decisions.
- User-facing APIs: Ozonechain provides mainnet Ethereum and EEA JSON-RPC APIs over HTTP and WebSocket protocols as well as a GraphQL API.
    - JSON-RPC
        - HTTP JSON-RPC Service
        - WebSocket JSON-RPC Service
    - GraphQL
- Monitoring: Ozonechain allows you to monitor node and network performance.
    - Node performance is monitored using Prometheus or the debug_metrics JSON-RPC API method.
    - Network Performance is monitored with Alethio tools such as Block Explorer and EthStats Network Monitor.
- Privacy: Privacy in Ozonechain refers to the ability to keep transactions private between the involved parties. Other parties cannot access the transaction content, sending party, or list of participating parties. Ozonechain uses a Private Transaction Manager to implement privacy.

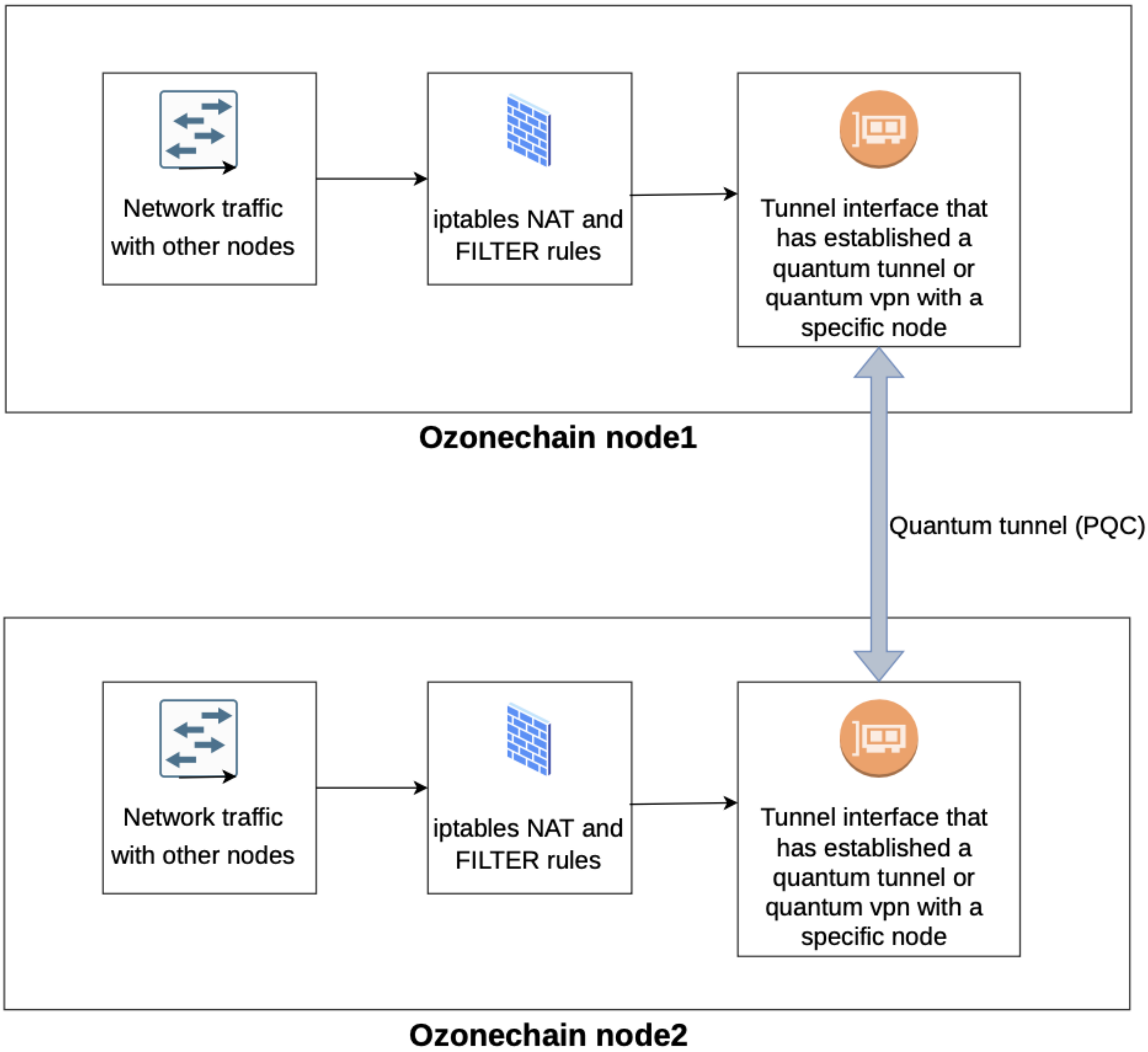
- Permissioning: A permissioned network allows only specific nodes and accounts to participate by enabling node permissioning and/or account permissioning on the network.

Quantum and Blockchain Integration

Random Numbers



Post Quantum Cryptography



- Within a ozonechain validator node, a quantum tunnel network interface (simply called tun interface) is created for each peer node (or peer validator node) it is connected to.
- The tunnel uses IP-in-IP VPN mechanism to communicate securely with other nodes.
- The VPN is implemented using OpenVPN.
- The OpenVPN uses NTRU algorithm for secure transmission of data.
- NTRU is a PQC algorithm approved by NIST to be quantum-resistant.

Analysis

Additional objectives for this penetration test were based on industry standard guidelines.

- ✔ Identification of vulnerabilities so that they can be remediated prior to being exploited by an attacker.
- ✔ Direct observation of restricted services or data in the absence of expected access controls.
- ✔ Compromise of an intermediary device used by privileged users to access secure network zones
- ✔ Compromise of the domain used by privileged users
- ✔ Sensitive data leakage or exfiltration.
- ✔ Verification of application logic, session handling, and API security for applications using supplied credentials.
- ✔ Verification that only authorized services are exposed to the network perimeter.
- ✔ Verification of network segmentation of non-privileged and privileged networks.
- ✔ Confirmation of absolute randomness of the random numbers fed to Ozone chain

✔ Attestation of use of post quantum cryptography for inter-node communication.

References

https://en.wikipedia.org/wiki/Post-quantum_cryptography

https://github.com/hyperledger/besu

https://github.com/hyperledger/besu

https://besu.hyperledger.org/en/stable/

https://wiki.hyperledger.org/display/BESU/Hyperledger+Besu

https://whitepaper.ozonechain.io/

Forked Project Issues

https://vulert.com/vulnerability/maven-org.hyperledger.besu:evm-37600

https://github.com/hyperledger/besu/issues?q=is%3Aopen+is%3Aissue+label%3Abug+

Past Forked Project Audits

https://wiki.hyperledger.org/display/SEC/Security+Code+Audits

Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Cyberscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Cyberscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Cyberscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Cyberscope team disclaims any liability for the resulting losses.

About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io