Quantum EVM

EVM-compatible blockchain consensus Proof-of-Coherence with physically verifiable quantum randomness

Authors: Andrew Kobal & Valentin Sotov (AILAND Group)
Date: August 2025

Abstract

This document introduces the concept of **Proof-of-Coherence (PoC) Consensus** for Ethereum-compatible blockchains. The key idea is to integrate physical **Quantum Random Number Generators (QRNG)** with an **AI-designed Verifier Function**, capable of distinguishing genuine quantum randomness from pseudo-random data. This provides verifiable physical randomness for blockchain consensus and smart contract execution. Unlike pseudo-random mechanisms, Quantum EVM ensures unpredictability in critical operations such as fair lotteries, auctions, MEV protection, oracle security, and unbiased resource allocation.

Executive Summary

This document describes **Quantum EVM** — a decentralized L2 network for Ethereum, designed to solve the fundamental problem of the absence of true randomness in blockchain. Modern blockchains rely on pseudo-random generators, which creates predictability and vulnerabilities in critical operations: fair lotteries, fair auctions, protection from MEV attacks, and prevention of oracle manipulations.

Quantum EVM solves this problem through a new consensus mechanism **Coherence Consensus**, which integrates verified data from physical quantum random number generators (QRNG) directly into the block creation process. The key element of the system is the **Verifier Function** — a deterministic set of statistical tests created based on deep AI analysis of quantum data during the R&D; phase. This function can distinguish true quantum data from pseudo-random data by physical markers: quantum correlations, specific noise patterns, and temporal characteristics that cannot be simulated programmatically.

Public Statement

This repository serves as a public disclosure (anti-patent) of the idea of **EVM-compatible blockchain consensus Proof-of-Coherence with physically verifiable quantum randomness**.

The main concept — using AI to create a simple verifier function that can determine the authenticity of quantum data from QRNG miners in an EVM-compatible blockchain — was described here in August 2025 by Andrew Kobal & Valentin Sotov (AILAND Group).

The purpose of this disclosure is to make the idea public so that it remains part of the public domain and cannot be patented in a restrictive manner.

References

1. Ernst, J. O., et al. (2025). Reinforcement Learning for Quantum Control under Physical Constraints. Available: https://arxiv.org/abs/2501.14372
2. Tran, D. M., et al. (2021). Experimenting quantum phenomena on NISQ computers using high level quantum programming. Available: https://arxiv.org/abs/2111.02896v2
3. RL4qcWpc: Open-source repository for RL in quantum control. Available: https://github.com/jan-o-e/RL4qcWpc
4. QCSim QuantumEraser: C++ implementation of the Quantum Eraser simulation. Available: https://github.com/aromanro/QCSim/blob/master/QCSim/QuantumEraser.h
5. Ethereum Optimism: Official Optimism GitHub organization and OP Stack implementation. Available: https://github.com/ethereum-optimism
6. Optimism Docs: OP Stack Documentation. Available: https://docs.optimism.io/stack/getting-started