BunkerCoin: A Low Bandwidth, Shortwave Radio-Compatible Blockchain Protocol

Anatoly Yakovenko

April 1st, 2024

Abstract

The rapid evolution of blockchain technology has demanded innovative solutions that extend beyond conventional digital landscapes. This paper introduces BunkerCoin, a groundbreaking blockchain protocol designed to operate under the constraints of low bandwidth networks, specifically through shortwave radio channels. At the heart of BunkerCoin is the adoption of a recursive Poseidon hash function, which underpins a novel proof of elapsed time (PoET) verifiable delay function (VDF). This VDF serves as the cornerstone for miners to identify a 'golden ticket'—a unique sequence of bits that not only signifies the discovery of a valid block but also correlates with the miner's public key and the duration for which a specific amount of coin has been held.

To ensure the integrity and confidentiality of this process, BunkerCoin leverages a recursive Zero-Knowledge Proof (ZKP), constructed using the Groth16 proving scheme. This allows miners to validate the existence of the golden ticket and concurrently seal the transaction block's hash without revealing the ticket itself. The propagation of these blocks over shortwave radio is meticulously engineered to accommodate the protocol's 300-byte Maximum Transmission Unit (MTU), with each block being disseminated through a series of 32:96 erasure coded frames over a fixed five-minute interval, ensuring reliability and redundancy.

Central to the protocol's consensus mechanism is the Nakamoto-style longest chain rule, which harmonizes with the unique transmission and validation processes to uphold network security and integrity. BunkerCoin's architecture not only challenges traditional blockchain paradigms but also paves the way for secure, decentralized communications in bandwidth-constrained environments worldwide, marking a significant leap forward in the field of distributed ledger technology.