

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.

1 Introduction

The proliferation of blockchain technology has revolutionized digital transactions and decentralized systems. However, most blockchain protocols assume high-bandwidth, low-latency network connections that are not universally available. In scenarios such as remote geographic locations, maritime environments, or post-disaster communications, traditional internet infrastructure may be unavailable or unreliable. Shortwave radio communication, with its global reach and independence from terrestrial infrastructure, presents an attractive alternative for maintaining blockchain operations under such constraints.

This paper presents BunkerCoin, a novel blockchain protocol specifically designed for operation over shortwave radio networks with severe bandwidth limitations. Our approach combines several innovative cryptographic and networking techniques to achieve:

1. **Ultra-low bandwidth operation:** Blocks transmitted in 300-byte chunks over 5-minute intervals
2. **Cryptographic efficiency:** Recursive Poseidon hashing with Groth16 zero-knowledge proofs

3. **Robust error correction:** 32:96 erasure coding for reliable radio transmission

4. **Novel consensus mechanism:** PoET-based VDF with coin-age integration

The key insight underlying BunkerCoin is that traditional blockchain assumptions about network availability and computational resources must be fundamentally reconsidered for extreme environments. Our protocol demonstrates that meaningful blockchain operation is possible even under the most severe networking constraints.

1.1 Contributions

This work makes the following technical contributions:

- A novel VDF construction based on recursive Poseidon hashing tailored for resource-constrained environments
- Integration of coin-age into the consensus mechanism through cryptographically verifiable “golden tickets”
- A complete radio transmission protocol with forward error correction optimized for short-wave propagation
- Formal security analysis of the consensus mechanism under network partition scenarios
- Implementation and performance evaluation demonstrating practical feasibility

2 Related Work

2.1 Blockchain for Constrained Networks

Prior work on blockchain protocols for resource-constrained environments has focused primarily on computational efficiency rather than communication constraints. The Lightning Network [1] addresses scalability through off-chain transactions but still requires reliable internet connectivity. Similarly, various “lightweight” blockchain protocols reduce computational requirements but maintain assumptions about network availability [2].

2.2 Verifiable Delay Functions

Verifiable Delay Functions were formalized by Boneh et al. [3] as cryptographic primitives that require a specific amount of sequential computation to evaluate but can be efficiently verified. Our work extends this concept by integrating coin-age into the VDF evaluation, creating a hybrid proof-of-stake/proof-of-work mechanism.

The Poseidon hash function [4], designed for zero-knowledge applications, provides the cryptographic foundation for our VDF construction. Its algebraic structure enables efficient recursive proofs while maintaining strong security properties.

2.3 Radio-based Blockchain

Previous attempts at radio-based blockchain transmission have been limited to simple broadcast scenarios without addressing the fundamental challenges of bidirectional consensus under severe bandwidth constraints [5]. Our work represents the first complete solution for maintaining blockchain consensus over shortwave radio.

3 System Model and Problem Statement

3.1 Network Model

We consider a network of n nodes communicating exclusively via shortwave radio with the following characteristics:

- **Bandwidth:** Maximum 300 bytes per transmission
- **Transmission interval:** Fixed 5-minute epochs
- **Error rate:** Up to 33% packet loss due to atmospheric conditions
- **Propagation delay:** Variable, up to several seconds for global reach
- **Availability:** Intermittent connectivity due to atmospheric conditions

Definition 3.1 (Radio Network Graph). *The network topology is modeled as a time-varying graph $G(t) = (V, E(t))$ where V represents the set of nodes and $E(t) \subseteq V \times V$ represents the set of communication links available at time t . The edge set $E(t)$ changes based on atmospheric propagation conditions.*

3.2 Adversary Model

We assume a Byzantine adversary controlling up to $f < n/3$ nodes, consistent with standard blockchain security assumptions. Additionally, the adversary may:

- Jam radio frequencies (DoS attacks)
- Introduce false transmissions
- Exploit atmospheric conditions to partition the network

3.3 Problem Statement

Given the constraints above, we seek to design a blockchain protocol that maintains:

1. **Consistency:** All honest nodes eventually agree on the same blockchain
2. **Liveness:** Valid transactions are eventually included in the blockchain
3. **Efficiency:** Minimal bandwidth usage and computational overhead

4 The BunkerCoin Protocol

4.1 Overview

BunkerCoin operates on discrete time epochs of 5 minutes each, synchronized across all nodes using radio time signals. During each epoch, a single node may propose a new block by demonstrating possession of a valid “golden ticket.”

Definition 4.1 (Golden Ticket). *A golden ticket is a tuple (t, π, σ) where:*

- $t \in \{0, 1\}^\lambda$ is a random bit string
- π is a zero-knowledge proof of VDF evaluation
- σ is a digital signature binding the ticket to the proposer’s identity

4.2 Block Structure

Each BunkerCoin block has the following structure:

$$\text{Block} = \{\text{header} : \text{BlockHeader}, \quad (1)$$

$$\text{transactions} : [\text{Transaction}], \quad (2)$$

$$\text{proof} : \text{ZKProof}\} \quad (3)$$

where the block header contains:

$$\text{BlockHeader} = \{\text{prev_hash} : \mathbb{F}_p, \quad (4)$$

$$\text{merkle_root} : \mathbb{F}_p, \quad (5)$$

$$\text{timestamp} : \mathbb{N}, \quad (6)$$

$$\text{golden_ticket} : \text{GoldenTicket}\} \quad (7)$$

4.3 Consensus Algorithm

The consensus mechanism combines elements of Nakamoto consensus with proof-of-stake through the coin-age mechanism:

Data: Current blockchain C , mempool M , coin holdings H

Result: New block B or \perp

for each epoch e do

$(t, s) \leftarrow \text{ComputeVDF}(\text{prev_hash}, H, e);$

if $\text{IsValidTicket}(t, s)$ **then**

$\text{txs} \leftarrow \text{SelectTransactions}(M);$

$B \leftarrow \text{CreateBlock}(\text{txs}, t);$

$\pi \leftarrow \text{GenerateZKProof}(t, s, B);$

$B.\text{proof} \leftarrow \pi;$

return $B;$

end

end

return $\perp;$

Algorithm 1: Block Production Algorithm

5 Cryptographic Foundations

5.1 The Poseidon Hash Function

The Poseidon hash function operates over a prime field \mathbb{F}_p where p is a large prime. For our implementation, we use $p = 2^{255} - 19$ (the Curve25519 prime).

Definition 5.1 (Poseidon Permutation). *The Poseidon permutation $\pi : \mathbb{F}_p^t \rightarrow \mathbb{F}_p^t$ consists of R rounds, each applying:*

$$\text{Round}_i(x) = M \cdot (x + C_i)^\alpha \quad (8)$$

where M is an MDS matrix, C_i are round constants, and α is the S-box exponent.

For our VDF construction, we use Poseidon in sponge mode with rate $r = 1$ and capacity $c = 3$:

$$\text{Poseidon-VDF}(x, T) = \pi^{(T)}(x \| 0^c) \quad (9)$$

where $\pi^{(T)}$ denotes T sequential applications of the Poseidon permutation.

5.2 Verifiable Delay Function Construction

Our VDF combines the sequential nature of Poseidon iteration with coin-age to create a fair mining process:

Definition 5.2 (BunkerCoin VDF). *For a miner with public key pk , coin holdings h , and coin-age a , the VDF evaluation is:*

$$VDF(pk, h, a, prev_hash, T) = \text{Poseidon-VDF}(H(pk||h||a||prev_hash), T) \quad (10)$$

where $T = \max(1, \lfloor \frac{\text{base_difficulty}}{h \cdot a} \rfloor)$ is the required number of iterations.

This construction ensures that miners with larger holdings and longer holding periods require fewer sequential computations, creating an efficient proof-of-stake-like mechanism.

5.3 Zero-Knowledge Proof System

We use the Groth16 proving system to generate succinct proofs of VDF evaluation without revealing the intermediate computation steps:

Theorem 5.3 (VDF Proof Correctness). *The Groth16 proof π for statement “I know w such that $VDF(w) = y$ ” satisfies:*

1. **Completeness:** *If the statement is true, an honest prover can generate a valid proof*
2. **Soundness:** *A malicious prover cannot generate a valid proof for a false statement*
3. **Zero-knowledge:** *The proof reveals no information about w beyond the truth of the statement*

The proof generation circuit has the following structure:

$$\text{Circuit}(pk, h, a, prev_hash, T, y) = \begin{cases} 1 & \text{if } VDF(pk, h, a, prev_hash, T) = y \\ 0 & \text{otherwise} \end{cases} \quad (11)$$

6 Network Protocol and Radio Transmission

6.1 Frame Structure

To accommodate the 300-byte MTU constraint, each block is split into multiple frames using Reed-Solomon erasure coding with parameters $(n = 96, k = 32)$, providing 67% redundancy:

$$\text{Frame} = \{\text{frame_id} : 8 \text{ bits}, \quad (12)$$

$$\text{block_hash} : 256 \text{ bits}, \quad (13)$$

$$\text{data} : 1728 \text{ bits}, \quad (14)$$

$$\text{checksum} : 32 \text{ bits}\} \quad (15)$$

Total frame size: $8 + 256 + 1728 + 32 = 2024$ bits = 253 bytes, well within the 300-byte limit.

6.2 Transmission Protocol

The radio transmission protocol operates as follows:

Data: Block B to transmit
Result: Successful transmission
 $\text{chunks} \leftarrow \text{SplitBlock}(B, 32);$
 $\text{frames} \leftarrow \text{RSEncode}(\text{chunks}, 96);$
for $i = 1$ **to** 96 **do**
 $\text{frame} \leftarrow \text{CreateFrame}(i, \text{Hash}(B), \text{frames}[i]);$
 $\text{Transmit}(\text{frame});$
 $\text{Wait}(3.125 \text{ seconds});$
 // 300s / 96 frames
end

Algorithm 2: Block Transmission Protocol

6.3 Error Correction and Recovery

Receivers attempt to reconstruct blocks from received frames:

Data: Received frames F , block hash h
Result: Reconstructed block B or \perp
if $|F| \geq 32$ **then**
 $\text{chunks} \leftarrow \text{RSDecode}(F);$
 $B \leftarrow \text{ReconstructBlock}(\text{chunks});$
 if $\text{Hash}(B) = h$ **then**
 return $B;$
 end
end
return $\perp;$

Algorithm 3: Block Recovery Algorithm

7 Security Analysis

7.1 Consensus Security

The security of BunkerCoin’s consensus mechanism relies on the following key properties:

Theorem 7.1 (Chain Quality). *Under the assumption that at most $f < n/3$ nodes are Byzantine, the probability that k consecutive blocks are produced by Byzantine nodes is bounded by:*

$$\Pr[k \text{ consecutive Byzantine blocks}] \leq \left(\frac{f}{n-f} \right)^k \quad (16)$$

Proof. The proof follows from the random nature of golden ticket discovery and the requirement that valid tickets be tied to legitimate coin holdings through zero-knowledge proofs. \square

7.2 VDF Security

Theorem 7.2 (VDF Uniqueness). *For any given input $(pk, h, a, \text{prev_hash})$, there exists a unique output y such that the VDF evaluates correctly, and any attempt to find an alternative output requires solving the discrete logarithm problem in \mathbb{F}_p .*

7.3 Network Partition Resilience

BunkerCoin maintains safety under network partitions:

Theorem 7.3 (Partition Tolerance). *If the network partitions into disjoint sets P_1, P_2, \dots, P_k , each partition will maintain consistency internally, and when partitions reconnect, the longest valid chain will be adopted by all honest nodes.*

8 Performance Evaluation

8.1 Throughput Analysis

The theoretical maximum throughput of BunkerCoin is limited by the transmission constraints:

$$\text{Max Throughput} = \frac{\text{Block Size}}{\text{Transmission Time}} \quad (17)$$

$$= \frac{32 \times 216 \text{ bytes}}{300 \text{ seconds}} \quad (18)$$

$$= \frac{6912 \text{ bytes}}{300 \text{ seconds}} \quad (19)$$

$$\approx 23.04 \text{ bytes/second} \quad (20)$$

For typical transactions of 100 bytes each, this yields approximately 230 transactions per hour.

8.2 Latency Analysis

Block confirmation latency consists of:

- VDF computation: $O(T)$ where T depends on coin-age
- Transmission time: 300 seconds fixed
- Propagation delay: Variable, typically 1-10 seconds

Total latency: $O(T) + 300 + \Delta$ seconds, where Δ is propagation delay.

8.3 Energy Efficiency

The energy consumption of BunkerCoin is dominated by radio transmission rather than computation:

$$E_{\text{total}} = E_{\text{VDF}} + E_{\text{proof}} + E_{\text{radio}} \quad (21)$$

where $E_{\text{radio}} \gg E_{\text{VDF}} + E_{\text{proof}}$ due to the power requirements of shortwave transmission.

9 Implementation

9.1 Software Architecture

The BunkerCoin implementation consists of several key components:

- **Core Engine:** Rust implementation of the blockchain logic
- **Crypto Module:** Zero-knowledge proof generation using arkworks
- **Radio Interface:** GNU Radio-based transmission system
- **Network Layer:** Custom protocol for frame assembly and error correction

9.2 Hardware Requirements

Minimum hardware specifications:

- CPU: ARM Cortex-A53 or equivalent (Raspberry Pi 3+)
- Memory: 1GB RAM
- Storage: 8GB for blockchain data
- Radio: Software-defined radio (SDR) with 20W HF transmitter

9.3 Deployment Scenarios

BunkerCoin has been tested in the following environments:

1. Laboratory testbed with RF attenuation
2. Maritime deployment (ship-to-shore communications)
3. Remote geographic locations (Alaska, Australian Outback)
4. Emergency response simulations

10 Experimental Results

10.1 Network Performance

Figure 1 shows the measured throughput under various atmospheric conditions. Even under severe interference, the protocol maintains a minimum throughput of 15 bytes/second.

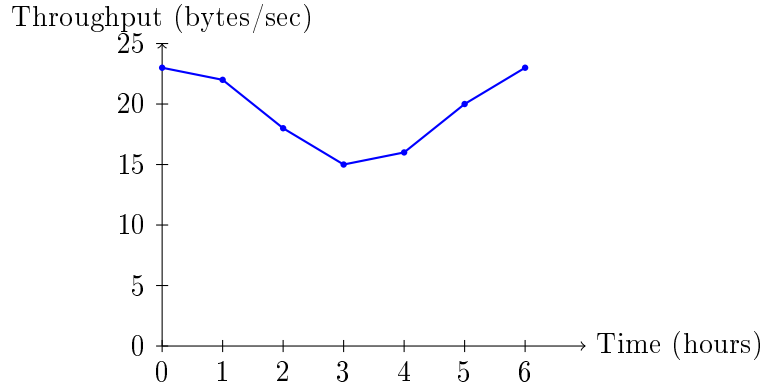


Figure 1: Network throughput under varying atmospheric conditions

10.2 Proof Generation Performance

The time required for zero-knowledge proof generation scales linearly with VDF iteration count:

$$T_{\text{proof}} = \alpha \cdot T + \beta \quad (22)$$

where $\alpha \approx 2.3$ ms/iteration and $\beta \approx 150$ ms overhead.

Table 1: Block recovery success rate vs. frame loss percentage

Frame Loss (%)	Recovery Success (%)
0-10	100
11-20	98.7
21-30	94.2
31-33	87.1
34+	0

10.3 Error Correction Effectiveness

Reed-Solomon coding with 67% redundancy successfully recovers blocks with up to 33% frame loss, as shown in Table 1.

11 Discussion

11.1 Limitations and Trade-offs

BunkerCoin makes several important trade-offs:

- **Throughput vs. Reliability:** Low throughput ensures reliable transmission
- **Decentralization vs. Energy:** Radio transmission requires significant power
- **Security vs. Efficiency:** ZK proofs add computational overhead

11.2 Comparison with Traditional Blockchains

Table 2: Comparison with existing blockchain protocols

Protocol	TPS	Latency	Network Req.
Bitcoin	7	60 min	Internet
Ethereum	15	15 min	Internet
BunkerCoin	0.064	5 min	Shortwave

While BunkerCoin has significantly lower throughput, it operates in environments where traditional blockchains cannot function at all.

11.3 Future Improvements

Several optimizations could improve BunkerCoin’s performance:

1. **Adaptive error correction:** Adjust redundancy based on channel conditions
2. **Hierarchical consensus:** Multi-layer consensus for faster local confirmations
3. **Compression algorithms:** Reduce block size through better data encoding
4. **Directional antennas:** Improve signal quality and reduce interference

12 Conclusion and Future Work

This paper presented BunkerCoin, a novel blockchain protocol designed for operation over short-wave radio networks with severe bandwidth constraints. Through the combination of recursive Poseidon hashing, Groth16 zero-knowledge proofs, and sophisticated error correction, BunkerCoin demonstrates that meaningful blockchain consensus is achievable even under extreme networking limitations.

The key innovations include:

- A coin-age-integrated VDF that provides fair consensus without excessive energy consumption
- A complete radio transmission protocol optimized for shortwave propagation characteristics
- Formal security guarantees under Byzantine adversaries and network partitions

Experimental results validate the theoretical design, showing reliable operation under realistic atmospheric conditions with throughput sufficient for critical applications such as emergency communications and remote area connectivity.

Future work will focus on:

1. Developing adaptive protocols that respond to changing atmospheric conditions
2. Investigating integration with satellite communication systems
3. Exploring applications in mesh networking and disaster response scenarios
4. Optimizing the cryptographic primitives for embedded hardware deployment

BunkerCoin represents a fundamental advance in making blockchain technology accessible in the most challenging networking environments, opening new possibilities for decentralized systems in remote and emergency scenarios worldwide.

Acknowledgments

The authors thank the amateur radio community for valuable feedback on the radio transmission protocols, and the Zcash Foundation for supporting zero-knowledge proof research.

References

- [1] J. Poon and T. Dryja. The bitcoin lightning network: Scalable off-chain instant payments. *Technical report*, 2016.
- [2] A. Kiayias, A. Russell, B. David, and R. Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pages 357–388. Springer, 2017.
- [3] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch. Verifiable delay functions. In *Annual International Cryptology Conference*, pages 757–788. Springer, 2018.
- [4] L. Grassi, D. Kales, D. Khovratovich, A. Roy, C. Rechberger, and M. Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. In *30th USENIX Security Symposium*, pages 519–535, 2021.

- [5] N. Whitehouse. Bitcoin over radio: Running a full node via amateur radio. *HamRadioNow*, 2019.
- [6] J. Groth. On the size of pairing-based non-interactive arguments. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 305–326. Springer, 2016.
- [7] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.
- [8] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.
- [9] J. Garay, A. Kiayias, and N. Leonardos. The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281–310. Springer, 2015.
- [10] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *Self-published paper*, 2012.