# Literature Review: SpaceMint – A Cryptocurrency Based on Proofs of Space

## 1. Introduction

Cryptocurrencies have revolutionized the financial world, with Bitcoin being the most well-known and widely adopted. However, Bitcoin’s Proof of Work (PoW) consensus mechanism consumes enormous amounts of energy, leading to environmental concerns and mining centralization. In response to these issues, the paper “*SpaceMint: A Cryptocurrency Based on Proofs of Space*” by Sunoo Park, Albert Kwon, Georg Fuchsbauer, Peter Gazi, Joel Alwen, and Krzysztof Pietrzak proposes a new cryptocurrency that replaces PoW with Proof of Space (PoSpace). This approach aims to make mining more **energy-efficient**, **cost-effective**, and **decentralized** by utilizing unused disk space instead of computational power.

## 2. Objectives of the Paper

The paper aims to address three critical problems associated with PoW-based blockchains:

* High Energy Consumption – Bitcoin mining requires vast amounts of electricity, making it unsustainable in the long term.
* Mining Centralization – The dominance of mining farms using specialized ASIC hardware reduces network decentralization.
* Barriers to Entry – The high cost of mining hardware prevents small participants from contributing to the network.

The authors propose SpaceMint as a green and fair alternative, allowing individuals to use their available storage instead of investing in costly, power-hungry hardware.

## 3. Methodology

Authors present a detailed design of SpaceMint, explaining how Proof of Space (PoSpace) can replace PoW while maintaining security and fairness. The methodology includes the following key innovations:

## 3.1 Proof of Space as a Consensus Mechanism

Unlike PoW, where miners solve computationally intensive puzzles, PoSpace miners allocate storage and prove they have stored a unique dataset.

The process involves two phases:

1. Initialization: The miner commits a certain amount of disk space by storing cryptographic proofs.
2. Mining: When a new block needs to be added, miners quickly verify their stored proofs to determine the winner.

## 3.2 Preventing Security Risks

The paper also addresses challenges that arise when using PoSpace instead of PoW, including:

* Nothing-at-stake problem: Miners could attempt to mine on multiple chains simultaneously. Solution – Implement penalties for miners who sign conflicting blocks.
* Challenge grinding: Miners could manipulate the blockchain state to gain an unfair advantage. Solution – Use a deterministic challenge function to ensure fair proof selection.

## 3.3 Game-Theoretic Analysis

The authors provide a formal game-theoretic model, proving that rational miners will follow the protocol as an equilibrium strategy. This ensures that SpaceMint remains stable and secure over time.

## 4. Results & Performance Evaluation

The paper includes an experimental implementation of SpaceMint, showing:

* Mining Setup: Initializing 1 TB of disk space takes about one day, but this is a one-time cost.
* Mining Efficiency: Once initialized, mining requires minimal computation – just a fraction of a second per block.
* Energy Consumption: The estimated energy usage is several orders of magnitude lower than Bitcoin.

## 5. Potential Applications

The SpaceMint concept can be applied beyond cryptocurrencies:

* Eco-friendly blockchain networks – Ideal for sustainable, low-energy blockchain applications.
* Distributed storage systems – Can be integrated into decentralized cloud storage platforms.
* Fairer digital economies – Enabling broader participation by reducing mining costs.

## 6. Conclusion

SpaceMint presents a compelling alternative to traditional PoW-based blockchains by leveraging Proof of Space. By reducing energy consumption, making mining more accessible, and addressing centralization risks, it offers a promising direction for the future of cryptocurrency. However, challenges such as network security, adoption barriers, and potential optimizations remain open for future research.