Shai (SHA)

Enhancing Satoshi's Vision

“Proof-of-work is essentially one-CPU-one-vote.”

Abstract

This paper introduces a novel approach to cryptocurrency mining, realigning with Satoshi Nakamoto's original vision of "one-CPU-one-vote." We propose an innovative utilization of a Verifiable Delay Function (VDF) to create a more accessible and decentralized mining process. Shai (SHA) is a fork of Bitcoin that will utilize the ShaiHive mining algorithm outlined in this paper. It will target 2-minute block times. The total amount of coins will be ~5,354,956 SHA. Tail emission will kick in at block 888420 (~4 years); the block reward becomes 0.1 SHA/block during tail emission. The initial block reward will be 11 SHA and each block it will decrease towards 0.1 SHA/block, following a specific equation detailed later in this paper. The smallest denomination is called a Kismet. 1 SHA = 100,000,000 Kismet (KIS).

In the context of UTXO-based systems, digital collectibles such as inscriptions and fungible tokens like runes offer expanded use cases and contribute additional value to the network. However, the viability and trustworthiness of these enhancements depend critically on the emission characteristics of the assets involved. Flaws or imbalances in asset distribution could foster skepticism regarding their long-term sustainability. Furthermore, the utility of these technologies hinges on the nature of the underlying assets. This centralization of mining power stands in opposition to the communal desire for equitable resource distribution, which is crucial for ensuring fair price discovery. This paper aims to outline Shai's strategic objectives and its approaches to achieving these goals, promoting a decentralized and fair infrastructure that produces desirable assets.

Introduction

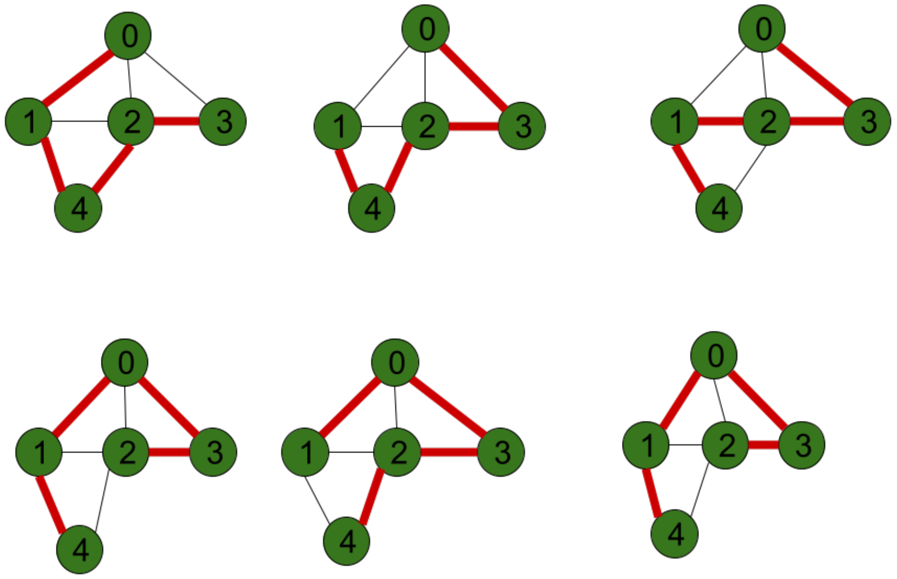
Introduced by an unknown entity under the pseudonym Satoshi Nakamoto, Bitcoin emerged as a groundbreaking digital currency, operating independently of central banks. Through its white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System,' Bitcoin was conceptualized as a decentralized, peer-to-peer network that enabled direct digital transactions without the need for intermediaries. This innovation laid the foundation for a new era of digital currencies and blockchain technology, challenging traditional financial models and sparking a global conversation on the future of money and privacy in the digital age.

Despite its decentralized ethos, the Bitcoin network faces significant challenges, notably the centralization of mining. Originally intended to be accessible to anyone with a computer, Bitcoin mining has evolved into an industry dominated by players with specialized, high-powered hardware and access to cheap electricity, often concentrated in specific geographic regions. This centralization not only contradicts the foundational principle of decentralization but also raises concerns about network security, manipulation risks, and the potential for regulatory interference. Additionally, the environmental impact of energy-intensive mining operations has become a contentious issue, prompting debates on the sustainability of Bitcoin's proof-of-work consensus mechanism.

The ShaiHive mining algorithm addresses centralization issues within the Bitcoin network by introducing a unique speed bump mechanism, acting as a lottery step through the search for Hamiltonian cycles in a graph and the presentation of certificates. This mechanism is implemented using a Verifiable Delay Function (VDF), where the VDF itself is the graph search for Hamiltonian cycles. To the best of our knowledge, Hamiltonian cycles have never been applied to blockchain mining in this manner.

This innovative use of Hamiltonian cycles introduces a novel challenge that equally impacts all miners. Hamiltonian cycles are essentially journeys through a graph where every point is visited exactly once before returning to the starting point. Named after the mathematician William Rowan Hamilton, these cycles are more than just theoretical curiosities—they represent an NP-complete problem, meaning that finding a solution is computationally intensive and challenging. NP-complete problems are significant in computational theory because their difficulty scales rapidly with the size of the input, making them ideal for creating computationally fair challenges in a decentralized network. See figure 69 for an example of some paths traveled.

Figure 69



Background

Bitcoin's current operating mechanism is based on a Proof-of-Work (PoW) algorithm, a pivotal concept that underpins the entire Bitcoin network. Proof of Work (PoW) is a consensus mechanism that enables the decentralized verification and recording of transactions on the Bitcoin blockchain. In this system, miners compete to find a result of SHA-256, computed twice, whose output is less than a specific number. The first to succeed is rewarded with newly minted bitcoins and transaction fees. This specific number is called the difficulity target and in bitcoins case it is adjusted every two weeks.

The security and integrity of the Bitcoin blockchain hinge on its Proof of Work (PoW) system, which makes altering any aspect of the blockchain extremely resource-intensive. However, this security comes at a high cost due to the significant energy consumption required for mining. Large-scale mining farms with powerful, specialized hardware (ASICs) have an advantage, leading to the centralization of mining power and posing risks to Bitcoin's decentralized nature.

Verifiable Delay Functions (VDFs) play a crucial role in cryptographic applications, particularly in blockchain and cryptocurrency, by enforcing a time-lock on computations. These functions take a predetermined amount of time to compute, preventing advanced hardware from gaining an undue advantage. VDFs are time-consuming to compute but quick and easy to verify, maintaining fairness, efficiency, and security within the network. By combining delayed computation with rapid verification, VDFs help preserve the integrity and democratic ethos of decentralized systems.

Building on these innovations, PID Controllers (Proportional-Integral-Derivative Controllers) can further enhance blockchain performance by optimizing difficulty targeting and adjusting the target after every block. A PID controller continuously adjusts control inputs based on error values to maintain stability and accuracy. By responding to current errors (proportional), accumulated past errors (integral), and predicting future errors (derivative), it ensures smooth and consistent system performance. In cryptocurrency mining, a PID controller dynamically adjusts mining difficulty, stabilizing block production, and adapting to network hash rate fluctuations. Shaicoin utilizes a combination of PID Controller and Digishield inspired logic for its network, leveraging the strengths of both approaches to maintain a stable and efficient mining environment. This hybrid method provides robust responsiveness to hash rate variability.

Proposed Mining Algorithm

In our novel mining algorithm, the first sha256 hash of the block is found with the yet-to-be-found Verifiable Delay Function (VDF) solution set to USHRT_MAX. This graph hash that was constructed plays a dual role. Firstly, it determines the size of a grid for a graph, within predefined minimum and maximum limits. This grid normalization ensures the graph's dimensions are always within the set range. Secondly, the graph hash is instrumental in populating this graph with nodes and edges.

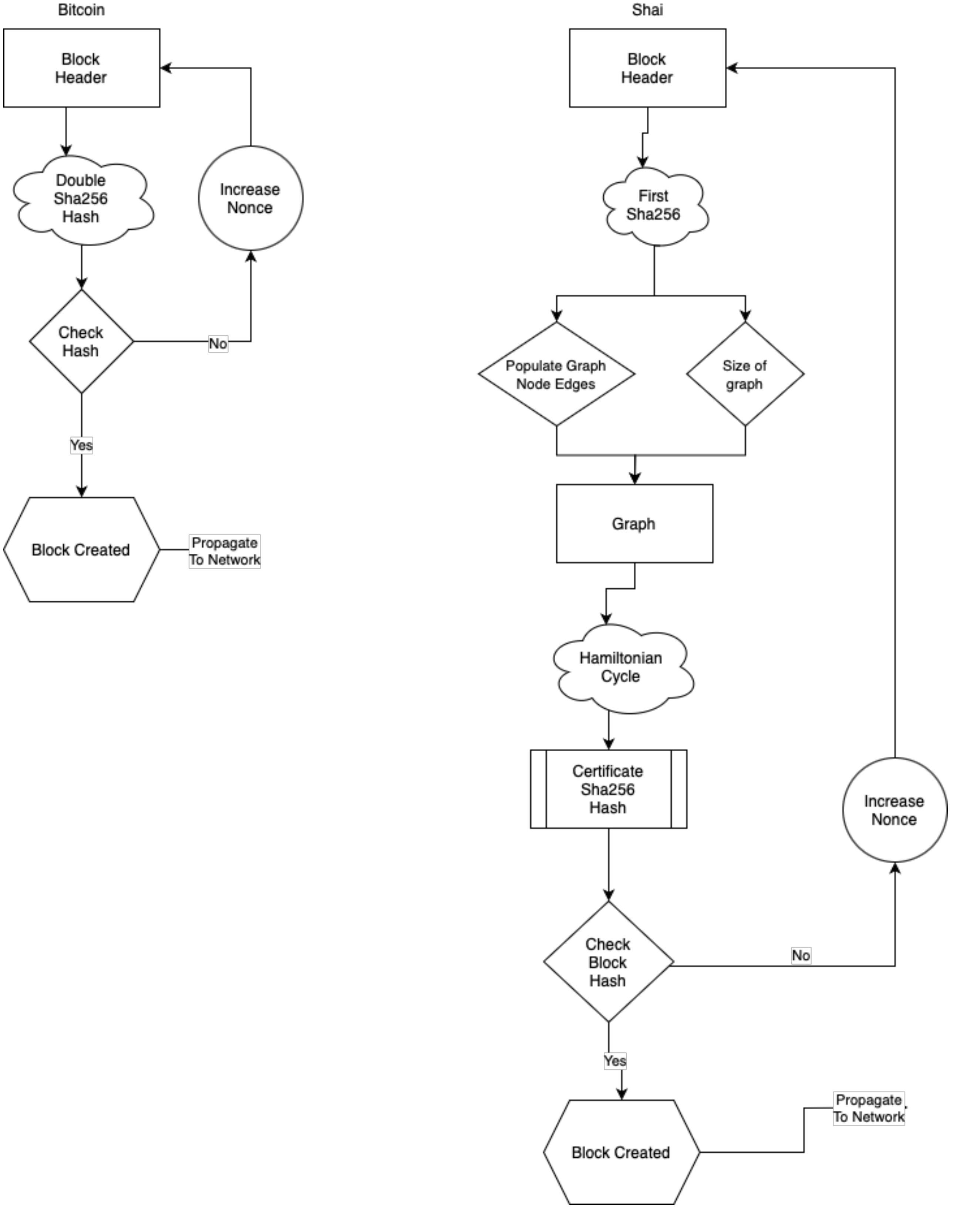
The graph's construction is a meticulous process. For each unique node pair in the grid, the algorithm calculates an index to access elements from the hash string, ensuring it remains within the hash's length. This index helps retrieve two specific characters from the hash, which are then converted into an unsigned integer to determine if an edge between these nodes should exist. An edge is established if this value is less than 128, and due to the graph's undirected nature, symmetry is maintained in its representation.

Upon completing the graph construction, the algorithm attempts to find a Hamiltonian cycle, a path through the graph visiting each node exactly once before returning to the starting point. The nodes visited are tracked, and the cycle's solution is replaced in the block.

The block is then sha256 hashed a final time and compared against the current mining target. If it falls below this target, akin to Bitcoin's mining mechanism, it signifies the creation of a valid block. This intricate process, Hamiltonian cycle problem-solving, exemplifies a sophisticated approach to mining that aims to maintain network integrity and decentralization.

In our algorithm, the verification of a potential Hamiltonian cycle, once identified, is a critical and efficient step, vital for the blockchain's integrity. This process, despite the variable duration required to find a cycle depending on the graph's size, ensures rapid validation. It meticulously checks that the cycle’s length corresponds with the graph’s node count, confirming each node is visited exactly once. Moreover, it verifies that a direct edge exists between every pair of consecutive nodes in the cycle. This thorough yet swift verification process is indispensable for quickly ascertaining the validity of proposed solutions, a central component in our Verifiable Delay Function (VDF). This ability to rapidly validate solutions, regardless of the time taken for their discovery, is crucial for the timely confirmation of valid blocks, underscoring the efficiency and security of our mining mechanism. Refer to figure 420 on the following page for our comparison visual.

Figure 420


Bitcoin
Block Header
Double Sha256 Hash
Increase Nonce
Check Hash
No
Yes
Block Created
Propagate To Network
Shai
Block Header
First Sha256
Populate Graph Node Edges
Size of graph
Graph
Hamiltonian Cycle
Certificate Sha256 Hash
Increase Nonce
Check Block Hash
No
Yes
Block Created
Propagate To Network

Benefits

Our innovative mining algorithm champions decentralization by adhering to the "one CPU, one vote" philosophy, allowing individuals with standard computing resources to participate effectively in the network. This approach counters the trend of mining centralization and promotes a more inclusive, decentralized blockchain ecosystem. In terms of security, the algorithm leverages Hamiltonian cycle problem-solving to enhance network integrity, while its efficient verification mechanism, integral to our Verifiable Delay Function (VDF), ensures swift and secure validation of new blocks. Additionally, by reducing reliance on specialized hardware, the algorithm lowers entry barriers for individual miners, making the blockchain more accessible and fostering a diverse and equitable mining community.

Shai's innovative mining approach offers a significant improvement over traditional Bitcoin mining by essentially transforming the mining process into a lottery system where each thread running the algorithm acts like a lottery ticket. This lottery-like mechanism is enabled by the Verifiable Delay Function (VDF), which serves as a speed bump, ensuring that even smaller hash rate CPUs have a fair chance of solving the puzzle and creating a block. The process of solving a Hamiltonian graph and cycle primarily relies on the single-core clock speed, making it less dependent on overall computational power or the number of cores. This unique aspect of the algorithm allows for a fairer distribution of mining power, as it mitigates the advantages of specialized hardware.

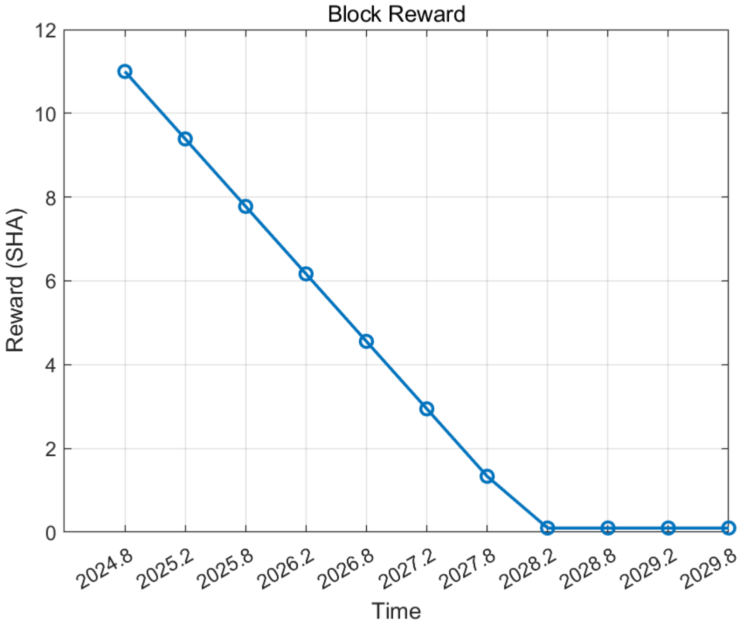
Additionally, the Shai network can benefit from decentralized mining pools like P2Pool, originally built for Bitcoin. P2Pool enables miners to pool their resources while maintaining the decentralized nature of the network, preventing any single pool from gaining too much control. By reintroducing and adapting P2Pool for Shai, we can ensure a more decentralized mining process, where payouts are more consistent and smaller amounts are distributed equitably. This approach not only democratizes the mining process but also preserves network integrity and decentralization, upholding the core principles of a decentralized digital currency.

Storage and Verification

The introduction of our advanced mining algorithm entails an increase in storage requirements, with the Bitcoin block header potentially expanding from the traditional 80 bytes to approximately 4096 bytes. This change, while significant, is justified and feasible in the current technological landscape, where the cost of memory is steadily decreasing. The continual advancements in data storage technology have made larger memory capacities more affordable than ever, mitigating the impact of increased storage needs. Furthermore, the robustness and widespread availability of high-speed internet make the transmission of larger data sizes, such as a 4096-byte block header, a trivial concern. In addition, the easy verification process utilizing the original cycle data ensures that this increase in size does not compromise efficiency. This process allows for quick and reliable verification of the blockchain, maintaining the integrity and speed of transactions. Thus, while the increased storage requirement is a notable change, it is both manageable and justifiable given the decreasing costs of memory and the enhanced capabilities of modern network infrastructures, ensuring the continued reliability and scalability of the blockchain system.

Block Reward

Starts at 11 SHA/Block and every block 1226 Kismets will be taken away from the block reward and it will march towards 0.1 SHA/Block (tail emission) Block 888420 around ~ 5,354,967 SHA will be emitted at this block when tail emission kicks in.



Comparing Past Projects with Similar Goals

Several projects have emerged in the cryptocurrency landscape, each attempting to address the issue of decentralization in mining, which Bitcoin struggles with due to the dominance of ASIC (Application-Specific Integrated Circuit) hardware. Litecoin (LTC), though not a direct Bitcoin fork, was created by Charlie Lee with the intention of being the "silver to Bitcoin's gold." It employs the Scrypt algorithm, initially believed to be resistant to ASIC mining. However, this resistance was eventually overcome, leading to similar centralization concerns as those faced by Bitcoin.

SCash (SCASH), launched in February 2024, represents a commendable effort to restore decentralization in mining by combining the Bitcoin protocol with Monero's RandomX proof-of-work algorithm. This innovative approach aims to bring mining back to home computers, creating a more inclusive mining environment. SCash is dedicated to fostering a community-driven mining landscape by prioritizing general-purpose computing over specialized equipment. While SCash primarily leverages existing technologies, its approach reflects the growing appetite for fair and decentralized mining solutions, indicating an increasing awareness and demand for addressing centralization issues within the cryptocurrency community.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf