Spectre Network Whitepaper

May, 2024

Abstract
Spectre Network introduces a novel approach to achieving scalability, privacy, and decentralization. Integrating cutting-edge cryptographic protocols such as the PHANTOM Protocol, GhostDAG [1], and the upcoming GhostFACE protocol, Spectre Network is designed to provide a comprehensive privacy-centric blockchain solution. These technologies synergize to create a robust platform for secure, anonymous, and high-speed digital transactions, embodying a pure "ghostchain" — a fully anonymous and decentralized network.

1. Introduction

Spectre Network is an advanced blockchain initiative engineered to synergize scalability and privacy, merging the rapid confirmation times of Kaspa's GhostDAG [1] with the stringent privacy features of Monero [7], encapsulated within a unique architectural framework. This platform ensures user anonymity, secure transactions, and equitable mining, laying the groundwork for a fully decentralized digital currency.

2. Technology Overview

1. The SpectreX Algorithm

Central to the Spectre Network is the SpectreX algorithm, a sophisticated CPU-only mining protocol designed to enhance network security while promoting equitable mining opportunities. Drawing from the strengths of AstroBWTv3 [2], the SpectreX algorithm is structured around the following three pivotal steps:

1. **SHA-3 Hashing**: This initial step involves the processing of transaction data through the SHA-3 [3] hashing algorithm, ensuring data integrity and providing a secure, immutable record of transaction information.
2. **AstroBWTv3 Proof-of-Work**: At the heart of the SpectreX algorithm, AstroBWTv3 [2] introduces a bandwidth-hard proof-of-work that is particularly resistant to ASIC and multi-core CPU optimizations. This feature is critical for maintaining fairness and decentralization within the mining process.
3. **HeavyHash Finalization**: The finalization step employs HeavyHash, further securing the network against external threats and specialized mining hardware, thereby enhancing the blockchain's overall resilience.

2. Explaining AstroBWT

AstroBWT [2] stands distinct from traditional cryptographic mining algorithms due to its foundation in Information Theory and the Compression Domains. Unlike conventional static mining algorithms that rely on data-dependent branches, loops, or conditions, AstroBWT [2] is underpinned by robust mathematical proofs and extensive research, ensuring its effectiveness and resistance to optimization.

3. What is BWT?

The Burrows-Wheeler Transform [4] (BWT) is a data transformation algorithm pivotal in data compression. It rearranges data into runs of similar characters, thereby enhancing the efficiency of other compression algorithms. The BWT [4] operates by rearranging the input data string into a matrix of cyclically shifted strings, sorting this matrix, and extracting the last column of the sorted matrix as the BWT [4] output. This process significantly aids in compression by grouping similar characters together, enhancing overall compression performance.

4. Characteristics and Advantages of AstroBWT:

- **Mathematical Rigor**: Built on a solid theoretical foundation, AstroBWT [2] provides a stark contrast to many other CPU mining algorithms that may lack a rigorous mathematical basis.
- **Resistance to Hardware Optimization**: Despite extensive efforts over decades to optimize BWT [4] for GPUs or FPGAs, these hardware implementations have not significantly outperformed CPUs. This resistance ensures a level playing field in mining efforts.
- **Wide Applicability**: The significance of AstroBWT [2] extends beyond cryptocurrency. Major technology providers like Intel and NVIDIA have developed optimized implementations of BWT [4], highlighting its importance in various fields beyond cryptocurrency, such as bioinformatics, signal processing, and DNA sequencing.

5. Potential for Scientific Advancement

The optimization of AstroBWT [2] for hardware such as FPGAs, ASICs, or GPUs could have far-reaching implications. Significant performance enhancements in AstroBWT [2] could catalyze advancements in fields that heavily rely on BWT, potentially leading to breakthroughs in scientific research and practical applications. This cross-pollination of technology not only solidifies AstroBWT's role in resisting centralization in mining but also contributes to broader scientific progress.

6. Mathematical Formulation

Given the operation of BWT [4] as a transformation T applied on a string s to produce a transformed string s', the general form of BWT can be expressed as:

$$s' = T(s)$$

where T denotes the Burrows-Wheeler transformation matrix operation.

AstroBWT [3], an enhanced version of BWT [4], operates under similar principles but incorporates advanced cryptographic hash functions like SHA-3 [3] to enhance security measures. The integration of these functions is represented by:

$$H = \mathrm{SHA3}(s')$$

where H represents the hash output used in the proof-of-work verification process, crucial for blockchain immutability and mining fairness in the SpectreX algorithm.

2.1 GhostDAG Protocol: Enabling Near-Instantaneous Block Times and Scalability

The GhostDAG [1] (Directed Acyclic Graph) protocol serves as the backbone of Spectre Network, facilitating rapid transaction processing, high throughput, and scalability without compromising on security. In this section, we delve into the intricacies of the GhostDAG [1] protocol, its unique features, and its role in revolutionizing blockchain consensus mechanisms.

1. Introduction to GhostDAG

Instead of traditional linear blockchain architectures, this novel consensus approach utilizes a directed acyclic graph to allow multiple block chains to coexist and interlink efficiently. This structure facilitates parallel processing of transactions, boosting the network's efficiency.

The GhostDAG [1] protocol introduces a novel architecture based on a Directed Acyclic Graph (DAG), a significant departure from the linear chain topology found in traditional blockchains. In contrast to a sequential ledger, the DAG structure in GhostDAG [1] allows each block to reference multiple predecessors. This multilateral referencing system forms a complex, graph-like structure without cycles, enabling several key enhancements over traditional blockchain designs:

2. Efficient Parallel Processing

The inherent design of the DAG permits parallel processing of transactions. Since blocks can reference multiple parent blocks, they do not have to be processed in a strict sequential order. This parallelism significantly enhances transaction throughput and overall network scalability. It allows for more rapid validation processes, reducing bottlenecks associated with the linear progression of traditional blockchains.

3. Enhanced Network Scalability

By eliminating the need for sequential block validation, the GhostDAG[1] protocol can handle a higher volume of transactions simultaneously. This scalability is crucial for accommodating growing network demands and ensures that the system remains efficient as it expands.

4. Security Through Blue Block Selection

Central to the GhostDAG [1] protocol is the selection of "blue blocks," which are identified through a strategic procedure that serves as the backbone of the protocol's security mechanism. These blocks represent a subset of well-connected nodes within the DAG and are selected based on specific criteria:

1. **Connectivity**: Blue blocks are those that exhibit high connectivity with other blocks in the DAG, ensuring they are integral to the network's structure.
2. **Timeliness**: Blocks that either only reference outdated blocks from the DAG or are deliberately withheld by their creators are less likely to be classified as blue. Such practices are indicative of potential misbehavior, and excluding these blocks helps maintain the integrity and security of the network.

The exclusion of potentially malicious blocks is crucial for preventing attacks where misbehaving nodes could otherwise compromise the network. By prioritizing blocks that are both timely and well-connected, GhostDAG [1] ensures that only trustworthy and robust blocks contribute to the network's ongoing operations.

Through its DAG structure, the GhostDAG [1] protocol achieves a balance of high throughput, scalability, and security, marking a significant evolution in blockchain technology. This structure not only supports faster and more efficient transaction processing but also fortifies the network against common vulnerabilities faced by traditional blockchain systems.

2.3 Future Implementations with GhostFACE

The introduction of the GhostFACE protocol in Spectre Network signifies a transformative step towards bolstering privacy and confidentiality in transactions. GhostFACE is designed to integrate seamlessly with the existing GhostDAG [1] infrastructure, leveraging advanced cryptographic techniques to enable non-disclosable privacy and anonymous transactions. This section provides a detailed exploration of the cryptographic foundations of GhostFACE, including Pedersen Commitments [5] and ElGamal [6] encryption, and discusses their application in enhancing transaction signing and privacy.

1. Overview of GhostFACE

GhostFACE stands for "Ghost Framework for Anonymity and Confidentiality Enhancement." It is a protocol layer that builds upon the DAG-based structure of GhostDAG [1] to introduce privacy features that are not inherently supported by many DAG or blockchain networks. The primary aim of GhostFACE is to allow users to execute transactions with full anonymity and confidentiality without compromising the network's integrity and scalability.

2. Pedersen Commitments

At the heart of GhostFACE's privacy capabilities are Pedersen Commitments [5], a cryptographic technique used to secure transaction details. A Pedersen Commitment [5] allows one to keep a piece of data secret but commit to it so that it cannot be altered without being detected. This method is particularly beneficial for cryptocurrency transactions as it allows the commitment (or the promise) of a specific transaction amount without revealing the actual value.

The commitment scheme works as follows:

- A user selects a random number rr and calculates the commitment C using the formula $C = g^x h^r$, where:
  - g and g are public bases known to all network participants.
  - x is the value being committed (e.g., the transaction amount).
  - r serves as the blinding factor that ensures the value x remains hidden.

This cryptographic approach ensures that while the transaction's integrity is verifiable by the network, the exact details of the transaction amount remain private.

3. ElGamal Encryption for Enhanced Transaction Signing

To complement the privacy provided by Pedersen Commitments [5], GhostFACE employs ElGamal [6] encryption, a public-key cryptosystem that is inherently malleable and well-suited for secure, anonymous transactions. ElGamal [6] allows for the encryption of messages (in this case, transaction details) that can only be decrypted by the intended recipient using their private key.

In the context of GhostFACE, ElGamal [6] encryption works by encrypting the transaction inputs and outputs, ensuring that only parties directly involved in the transaction can decipher the transaction details. This method is particularly advantageous for:

- Preventing transaction graph analysis, as the linkage between transactions is obscured.
- Ensuring that transaction amounts and recipient details are not exposed to the public.

4. Implementation and Network Integration

The integration of GhostFACE within the Spectre Network involves updating the network nodes to support the cryptographic operations required by Pedersen Commitments [5] and ElGamal [6] encryption. This update is planned to be rolled out as a soft fork, allowing nodes to gradually adopt the new features without disrupting the existing network operations.

5. Future Prospects and Implications

The implementation of GhostFACE is poised to transform the Spectre Network into a fully-fledged privacy-centric blockchain solution. This development is expected to attract a broader user base, particularly from sectors where transaction confidentiality is paramount, such as in financial services, healthcare, and enterprise blockchain applications.

3. Future Vision for Spectre Network

Spectre will add full non-disclosable privacy and anonymous transactions in future, implemented with the GhostFACE protocol built by a team of anonymous crypto algorithm researchers and engineers. Simple and plain goal: `PHANTOM Protocol + GhostDAG + GhostFACE = Spectre`

Spectre will become a ghostchain; nothing more, nothing less. Design decisions have been made already and more details about the GhostFACE protocol will be released at a later stage. Sneak peek: It will use Pedersen Commitments as it allows perfect integration with the Spectre UTXO model and allows perfect hiding. ElGamal [6] will be used for TX signature signing as it has a superior TPS (transactions per second) performance. Any PRs are welcome and can be made with anonymous accounts. No pre-mine, no nonsense.

Feature	**Spectre**	**Kaspa**	**Monero**	**DERO**
PoW Algorithm	SpectreX	kHeavyHash	RandomX	AstroBWTv3
Balance Encryption	Future	No	Yes	Yes
Transaction Encryption	Future	No	Yes	Yes
Message Encryption	Future	No	No	Yes
Untraceable Transactions	Future	No	Yes	Yes
Untraceable Mining	Yes	No	No	Yes
Built-in multicore CPU-miner	Yes	No	Yes	Yes
High BPS (Blocks Per Second)	Yes	Yes	No	No
High TPS (Transactions Per Second)	Yes	Yes	No	No

4. Mathematical and Cryptographic Framework

Spectre Network adheres to rigorous mathematical principles, integrating constants and prime numbers to secure the mining process and transaction verification. The cryptographic strength of the network is rooted in the combined use of SHA-3[3] for data integrity, AstroBWT [2] for resistance against hardware optimization, and the innovative HeavyHash to further secure the network infrastructure.

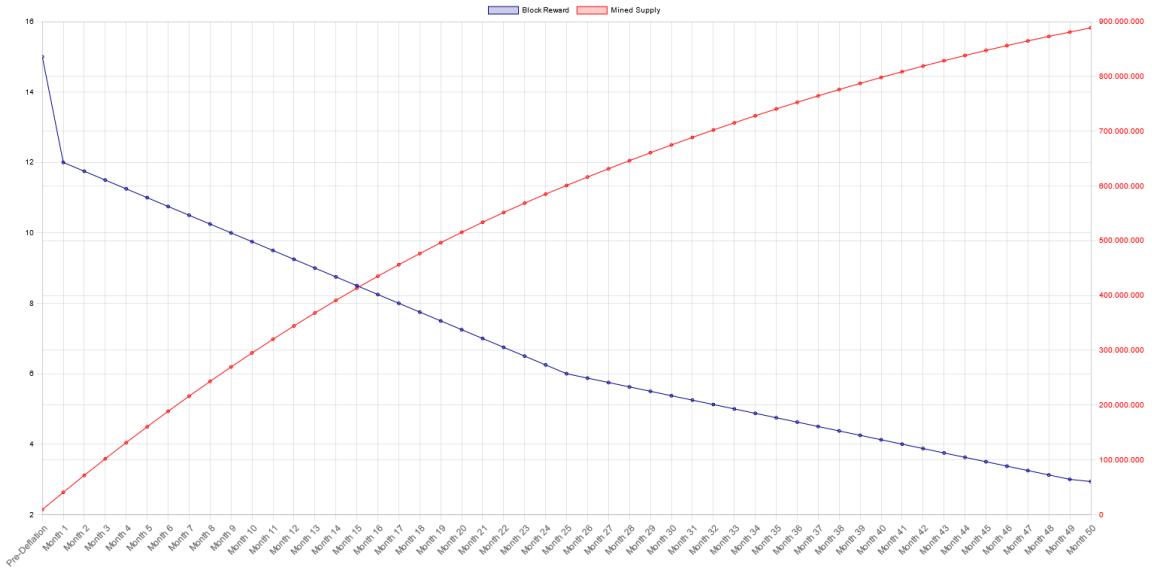
5. Tokenomics

The tokenomics framework of Spectre Network is meticulously architected to balance incentivization with long-term viability and stability. This structure is pivotal for underpinning the broader economic and functional aspects of the network, ensuring both initial adoption and sustained engagement. Below, we elaborate on the specifics of token distribution, mining dynamics, and the underlying economic principles guiding Spectre Network.

1. Maximum Supply and Emission Schedule

Spectre Network is designed with a finite maximum supply of 1,161,000,000 coins. This cap is integral to maintaining scarcity and thereby potentially enhancing the value retention over time. The coins are set to be distributed according to a predetermined emission schedule, which is detailed as follows:

- **After 24 months:** A total of 591,705,000 coins, representing approximately 51.4% of the maximum supply, will have been mined.
- **After 48 months:** Cumulative mining will have yielded 871,778,700 coins, accounting for about 75.7% of the maximum supply.
- **After 64 months:** By this stage, the mining process will have brought into circulation 975,655,800 coins, equating to approximately 84.7% of the maximum supply.



2. Mining Incentives and Reward Structure

The token distribution strategy is crafted to incentivize early participation by miners while ensuring ongoing network security and participation through the following phases:

- **Initial Phase (0-24 months):** This phase is critical for establishing a robust network of participants and securing a decentralized infrastructure. Over half of the total coin supply is mined during this period, providing significant incentives for early miners and node operators.
- **Growth Phase (25-48 months):** As the network matures, the emission rate is carefully tapered to balance the influx of new coins with economic stability and inflation control.
- **Maturity Phase (49-64 months and beyond):** Approaching the maximum coin supply, the emission rate further decreases, which naturally shifts the miner's incentive from block rewards to transaction fees, ensuring sustainability of network operations.

3. Economic Model

The economic model of Spectre Network adheres to fundamental principles designed to foster long-term growth and stability:

- **Scarcity:** The hard cap on the total supply of coins helps in combating inflation and promoting price stability, which can be critical for both miners and investors.
- **Phased Distribution:** The multi-phased approach in coin distribution not only ensures initial robust participation but also facilitates a gradual transition to a fee-based incentive model.
- **Sustainability:** With a planned decrease in mining rewards, the network is designed to sustain itself on transaction fees, which will become increasingly prominent as the primary incentive for miners.

4. Rewards Distribution Mechanism

Mining rewards in Spectre Network are distributed through a proof-of-work mechanism, employing the SpectreX algorithm. This choice supports a fair distribution of rewards across a broad base of miners, thereby preventing centralization and maintaining network integrity and security. As the network evolves, these rewards are programmed to decrease in alignment with the emission schedule, encouraging a shift towards a transaction-fee-based model.

5. Open Contributions

Spectre Network champions open-source contributions and community involvement. Developers are encouraged to contribute via pull requests, which can be made anonymously, ensuring that the development of the network reflects a wide range of inputs and maintains transparency without compromising privacy.

6. Conclusion

Spectre Network is set to redefine the standards of privacy, security, and scalability in the cryptocurrency domain. Through the strategic integration of its core technologies, Spectre will offer a blockchain solution that is not only fast and secure but fundamentally focused on user privacy. This will establish a new paradigm in how digital transactions are conducted and privacy is maintained in the blockchain space.

7. Future Developments and Roadmap

More detailed information about the implementation stages of the GhostFACE protocol and further enhancements to the SpectreX and GhostDAG [1] protocols will be released to the community as the project progresses. This phased approach ensures that each component is thoroughly tested and integrated, maintaining the network's integrity and leading-edge performance.

Spectre Network invites the global community to join in shaping the future of privacy in blockchain. With no pre-mining and a commitment to transparency and privacy, Spectre is not just a platform but a movement towards a more secure, private, and equitable blockchain ecosystem.

References

1. Yonatan Sompolinsky, Shai Wyborski, Aviv Zohar. PHANTOM GHOSTDAG, 2021
2. DERO AstroBWT CPU Mining Proof-of-Work Algorithm. https://github.com/deroproject/astrobwt
3. NIST. (2015). FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.202.pdf
4. Burrows, M., and Wheeler, D.J. (1994). "A Block-sorting Lossless Data Compression Algorithm", Digital Systems Research Center Research Report.
5. T. Pedersen, "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing," in Advances in Cryptology — CRYPTO '91, Lecture Notes in Computer Science, vol. 576, Springer, Berlin, Heidelberg, 1991, pp. 129-140. Available: https://link.springer.com/chapter/10.1007/3-540-46766-1_9
6. T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, 1985. Available: https://ieeexplore.ieee.org/document/1057074
7. Saberhagen, Nicolas van. (2013). "CryptoNote v 2.0." This foundational whitepaper introduces ring signatures and stealth addresses, pivotal in enhancing transaction privacy and anonymity in cryptocurrencies. Monero, derived from these principles, was established in 2014 through a fork of Bytecoin to ensure equitable and transparent distribution and to further the goals of transaction privacy. Detailed discussions on Monero's technological advancements and its ongoing development can be found in publications by the Monero Research Lab (MRL), accessible at Monero's official website: www.getmonero.org