Nexellia Whitepaper

"Empowering the Individual Miner: A GPU-Focused Approach"

Nexellia is a fork of the Kaspa blockchain

Executive Summary: The Kaspa blockchain stands as an innovative endeavor, adopting the GhostDAG protocol to craft a Directed Acyclic Graph (DAG) infrastructure. This structural shift from the traditional blockchain sequence substantially elevates the network's capacity and speed, accommodating simultaneous block additions and brisk transaction throughput. Kaspa is engineered to prioritize swift transactions and high bandwidth while upholding the tenets of decentralization and security, thereby establishing a dynamic foundation for diverse blockchain applications and scenarios.

Issue Identification: Kaspa's original architecture was amenable to ASIC hardware, inadvertently favoring large-scale mining operations and subsequently influencing the network's decentralized nature. ASIC miners, with their high-powered and purpose-built equipment, can overshadow standard computer setups, which may lead to a disproportionate aggregation of mining influence within a select group of industrial miners. Such centralization conflicts with the egalitarian ethos of blockchain, a technology envisaged to disseminate authority amongst its users uniformly.

The concentration of mining capabilities not only presents potential risks regarding the governance and security of the network but also introduces significant hurdles for solo miners. This creates a discord with the open and democratic philosophy intrinsic to blockchain communities. Kaspa's objective, therefore, is to nurture a harmonious and dispersed mining landscape, ensuring the stability, inclusivity, and adherence to the decentralized blueprint of blockchain infrastructure.

Solution Synopsis: Nexellia introduces a pivotal change with its GPU-focused divergence, directly challenging the prevalence of ASIC mining conglomerates. This pivot towards GPU mining democratizes the mining process by capitalizing on the widespread availability of GPU hardware, in contrast to the more specialized and less accessible ASICs. Diminishing the performance gap between ASICs and GPUs democratizes the mining process, spurring broad-based involvement and fostering a more equitable network. This not only advances the principle of collective participation and network durability but also fortifies the security framework, remaining true to the decentralized essence of blockchain philosophy.

Introduction:

Contextualizing the Kaspa GhostDAG Paradigm

Kaspa's inception in the realm of blockchain signifies a remarkable leap forward, with its pioneering GhostDAG protocol at the forefront. This novel protocol veers away from the established blockchain blueprint, opting instead for a Directed Acyclic Graph (DAG) configuration. GhostDAG's framework diverges from the sequential chain model, enabling concurrent inclusion of multiple blocks which substantially bolsters the network's scalability and expedited transaction execution. This innovative setup advances the network's performance while concurrently safeguarding security and upholding the distributed nature of blockchain, thus mitigating prevalent constraints of traditional blockchain infrastructures.

Cryptocurrency Mining Dynamics

The landscape of crypto mining has been evolving, now predominantly under the influence of ASIC operations. These devices, engineered for optimal mining efficiency, have eclipsed the capabilities of GPU and CPU mining solutions. This trend has culminated in the ascent of industrial-scale mining enterprises capable of deploying the expensive ASIC infrastructure. Such centralization presents a threat to the network's integrity and stands in opposition to the founding principle of decentralization within blockchain's architecture. Moreover, it erects financial and competitive barricades for independent or small-scale miners, rendering their engagement in mining increasingly impractical.

The Imperative for Evolution

Pivoting towards GPU-centric mining is critical to preserve the network's vitality and its decentralized character for various reasons:

Mining Democratization: Given their prevalence in standard computing devices, GPUs offer a more attainable entry point for solitary miners and smaller operations, facilitating wider participation in the mining process.

Enhanced Decentralization and Fortified Security: A broader mining constituency, enabled by GPU accessibility, ensures a more dispersed distribution of mining activity, essential for diminishing the risks of concentrated attack vectors and potential network compromises.

Embracing Inclusivity and Enduring Practices: Leaning on GPUs paves the way for a more inclusive mining community, encompassing enthusiasts and modest mining undertakings. It's a stride towards enduring mining practices, often more energy-conserving than ASIC-based mining.

Countering ASIC Hegemony: Transitioning to GPU mining presents a counterbalance to the monopolistic tendencies of significant ASIC mining entities, reinforcing the network's robustness and fidelity to blockchain's decentralized ethos.

Nexellia's proposition to adopt GPU mining epitomizes a deliberate tactic to maintain blockchain networks as decentralized, accessible, and safeguarded ecosystems, directly addressing the tribulations introduced by the prevailing ASIC-centric mining paradigm.

Project Objectives:

1/Distributed Artificial Intelligence Network on BlockDAG

The development of a distributed artificial intelligence (AI) network, where each node of the BlockDAG acts as an autonomous AI agent. These agents will collaborate on various tasks such as machine learning, data processing, and decision making, within a BlockDAG structure that offers efficiency, transparency, and security.

Advantages:

- **Distributed Learning:** Utilization of BlockDAG for collaborative and distributed learning.
- **Security:** Security enhancement through the decentralization of BlockDAG.
- **Real-Time Processing:** Ability to efficiently process data in real-time due to the speed of BlockDAG,
- **Interoperability:** Use of smart contracts to ensure interoperability.

Challenges :

- **Data Protection:** Ensuring the security of private data.
- **Handling Large Volumes:** Ability to process and manage large volumes of data.
- **Regulatory Compliance:** Adherence to legal and regulatory standards.

Applications:

- **Smart Cities:** Management of urban infrastructures such as lighting and traffic (traffic lights), as well as city energy systems, all driven by AI.
- **Healthcare:** Secure analysis of medical data to prevent data leaks, and use in pandemic prevention through the analysis of virus hotspots.
- **Finance:** Applications in trading and real-time financial analysis, leveraging the speed and accuracy of AI.
- **Gaming:** Enhancing gaming experiences with AI-driven ecosystems, supported by the secure and efficient framework of BlockDAG.

Innovations:

The structural alignment of BlockDAGs with neural networks used in current AI models creates a unique opportunity to combine the benefits of BlockDAG with the capabilities of AI. This paves the way for revolutionary applications, transforming key sectors such as gaming, urban planning, healthcare, and finance.

2/Enhancing Network Distribution

Emphasizing GPU mining has multifaceted impacts on network distribution:

- **Equitable Distribution of Mining Capabilities:** The widespread accessibility of GPUs democratizes mining, allowing a multitude of participants to mine. This counters the monopolization of mining capacity by large-scale ASIC operators and nurtures a more evenly distributed network topology.
- **Curtailing Centralization Tendencies:** ASIC-dominated mining clusters threaten the equitable nature of blockchain networks by potentially allowing a limited number of entities to wield excessive influence. GPU mining counteracts this, making it more accessible and practical for a diverse cohort to engage in mining activities.

Promoting Miner Inclusivity :

- **Cost-Efficiency:** GPUs, typically more budget-friendly, present a spectrum of economic options in contrast to ASICs. This cost-efficiency empowers individuals or small groups to partake in mining endeavors.
- **Broad Availability:** Given their common application in personal computing and entertainment systems, GPUs are more attainable for the average user than the niche ASIC equipment.
- **Multi-Purpose Functionality:** Beyond their designated function, GPUs provide multifunctional utility, including gaming, graphic processing, and mining various digital currencies. Their multi-use capability renders them particularly attractive for novice miners.

Reinforcing Network Security :

- **Mitigating Majority Attacks:** A decentralized mining framework, bolstered by the prevalence of GPU miners, diminishes the probability of majority attacks, where the controlling mining party may attempt to alter the blockchain. A dispersed mining populace impedes the feasibility of such dominance.
- **Amplifying Stakeholder Diversity:** A network that benefits from an expansive miner base inherently gains a multitude of vested protectors, enhancing the network's overall fortitude and defense mechanisms.
- **Flexibility and Sturdiness:** Networks underpinned by GPU miners can exhibit greater adaptability and sturdiness. GPUs' algorithm-agnostic nature allows for swift adjustments in response to protocol alterations or hashing changes dictated by security enhancements.

The strategic pivot to GPU mining is instrumental in advocating for a decentralized structure, easing the path for aspiring miners, and bolstering network security. This strategy resonates with the core tenets of blockchain, ensuring that networks remain expansive, equitable, and resilient.

Technical Characteristics:

In its hashing operations, Nexellia utilizes the Blake3 algorithm. The selection of Blake3 is attributed to its operational efficiency, capability to process data in parallel, and its adaptability to common computing hardware. The limited presence of Blake3-specific ASICs is due to its relatively recent introduction, a lack of compelling reasons for developing dedicated Blake3 ASICs, and its already proficient performance on standard hardware platforms.

Benefits of Implementing Blake3 :

Blake3 stands as a cutting-edge cryptographic hash function, outstripping predecessors like Blake2 and other hash functions including Keccak from the SHA-3 standard. The attributes leading to Blake3's enhanced speed, and the reason for the lack of specialized ASICs for it, encompass various aspects:

- **Streamlined Algorithmic Design:** Blake3 is crafted with an emphasis on straightforward and efficient functioning. Compared to Keccak, its round function is simpler, which is central to the hashing process. This simplicity equates to quicker computation, thereby reducing the processing effort needed for each hash.

- **Built-in Parallelism:** Blake3's architecture inherently supports parallel data processing, effectively utilizing the concurrent processing capacity of contemporary multi-core CPUs and GPUs. This significantly hastens the hashing operation on typical computing hardware, a contrast to Keccak's approach, which does not focus as much on parallelism.

- **Tailored for Everyday Hardware:** Blake3 is optimized for excellent performance on widely-used hardware like CPUs and GPUs. It exploits specific characteristics of these processors, such as SIMD (Single Instruction, Multiple Data) instructions, to enhance its processing speed.

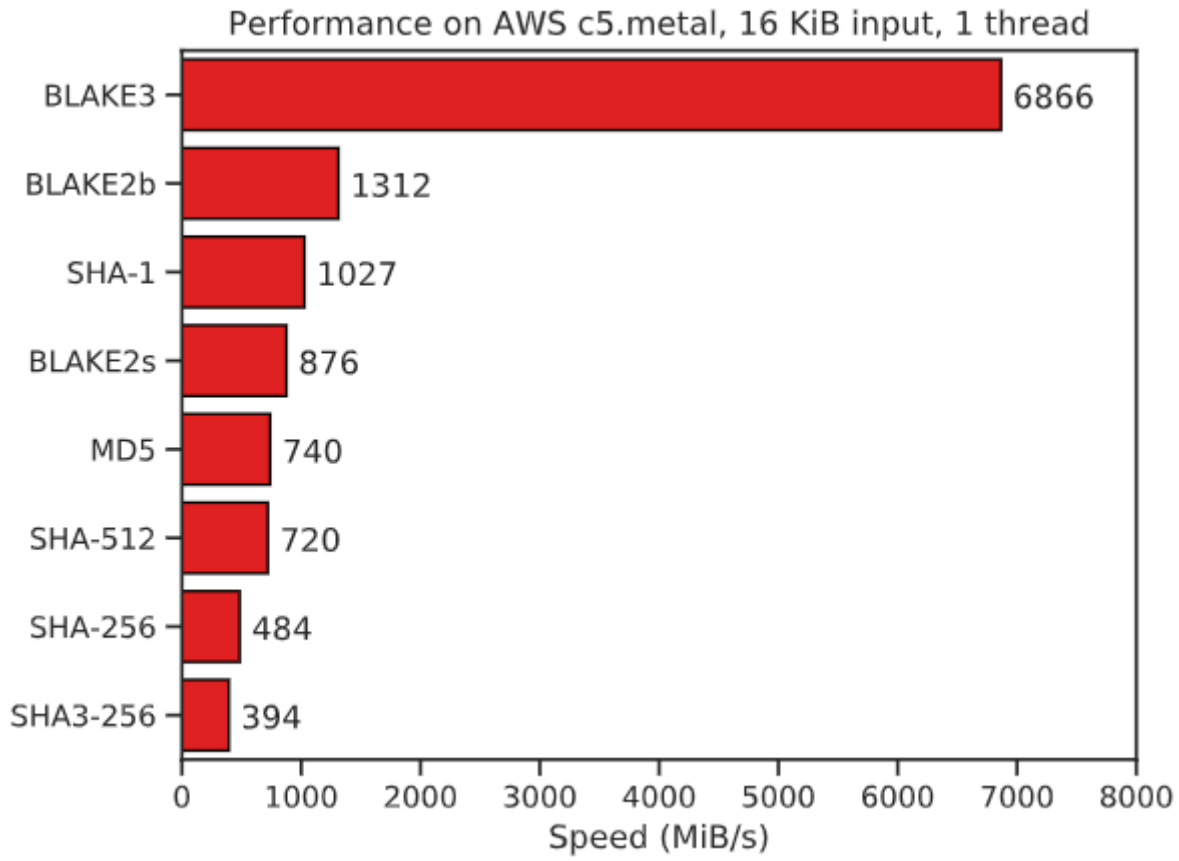
Blake3 and ASICs:

- **ASIC Specialization:** ASICs are designed for highly specialized functions, particularly efficient in executing specific tasks. Presently, cryptographic ASICs are mainly aligned with algorithms that are integral to activities like cryptocurrency mining (e.g., SHA-256 for Bitcoin). Due to Blake3's recent introduction and its limited application in high-demand areas, there has been minimal incentive to develop ASICs specifically for Blake3.

- **Resource-Intensive ASIC Development:** The creation of an ASIC involves significant time and financial resources. It necessitates the design and fabrication of a chip tailored to an algorithm's unique properties. As Blake3 has yet to become a standard in any major application warranting such investment, the drive for developing Blake3-specific ASICs is less pronounced.

- **General-Purpose Hardware Efficacy:** The effective performance of Blake3 on common CPUs and GPUs diminishes the need for ASICs. The advantages of developing an ASIC specifically for Blake3 would be relatively minor when considering the investment and effort required.

The chart below is an example benchmark of 16 KiB inputs on a Cascade Lake-SP 8275CL server CPU from 2019



Source : https://github.com/BLAKE3-team/BLAKE3

Economic Model:

The blockDAG architecture – with rapid block rates – allows more mining decentralization and enables effective solo-mining even at lower hashrates.

Nexellia's monetary policy is simple : Each year, the block reward will divide by two with an initial block reward of 12 NXL.

This will result in a maximum supply of **788,940,000 NXL**.

Please note that the policy determines the number of coins created each second, independent of the block rate. Hence, if there's a change in the block rate in the future, the reward for each block will be modified to ensure the emission rate remains constant.

Total mined at 01/24/2025 : 378,691,200 NXL – (47.97% of the total supply)

Total mined at 01/24/2026 : 586,036,800 NXL – (74.24% of the total supply)

Total mined at 01/24/2027 : 662,709,600 NXL – (83.95% of the total supply)

Total mined at 01/24/2028 : 725,824,800 NXL – (92% of the total supply)

Also, the last block will be mined on **01/24/2055.**

Nexellia emission schedule for the first 10 years

Years	Reward
2024	12
2025	6
2026	3
2027	1,5
2028	0,75
2029	0,375
2030	0,1875
2031	0,09375
2032	0,046875
2033	0,0234375
2034	0,01171875

References:

- **PHANTOM GHOSTDAG A Scalable Generalization of Nakamoto Consensus :**
  https://eprint.iacr.org/2018/104.pdf

- **Blake3 references:**
  https://github.com/BLAKE3-team/BLAKE3
  https://github.com/BLAKE3-team/BLAKE3-specs/blob/master/blake3.pdf