Karlsen Network whitepaper

"GPU-Centric GhostDAG: Empowering Small-Scale Miners"

Abstract:

Karlsen network is a fork of the Kaspa blockchain

Brief Overview: Kaspa is a groundbreaking blockchain project that leverages the unique GhostDAG protocol to create a Directed Acyclic Graph (DAG) structure, differing from traditional linear blockchains. This approach significantly enhances scalability and transaction speed, allowing for parallel block additions and rapid transaction processing. While focusing on high throughput and reduced confirmation times, Kaspa maintains a strong commitment to decentralization and security, positioning itself as a versatile and robust solution for a wide range of blockchain applications and use cases.

Problem Statement: Kaspa addresses a significant issue in the blockchain space: the dominance of ASIC (Application-Specific Integrated Circuit) mining farms, which has a profound impact on decentralization. ASIC mining farms, equipped with specialized hardware, often outperform individual miners using standard computers, leading to a concentration of mining power in the hands of a few large-scale operators. This centralization contradicts the fundamental principle of blockchain technology, which is to distribute power and control evenly among its participants.

The centralization of mining power not only raises concerns about network control and vulnerability to attacks but also poses barriers to entry for individual miners, thus eroding the inclusive and democratic ethos of blockchain networks. By addressing this issue, Kaspa aims to foster a more balanced and decentralized ecosystem, ensuring that the network remains secure, inclusive, and aligned with the original vision of distributed ledger technology.

Solution Overview: The Karlsen project introduces a GPU-centric fork as a solution to the dominance of ASIC mining farms, aiming to empower small-scale miners and enhance decentralization. This strategic shift to GPU mining makes participation more accessible to individuals, as GPUs are more commonly available than specialized ASIC hardware. By reducing the efficiency advantage of ASICs, this approach levels the mining field, encouraging widespread participation and ensuring a more distributed network. This not only promotes inclusivity and sustainability but also bolsters network security, aligning with the core principles of decentralization inherent in blockchain technology.

Introduction:

Background on Kaspa GhostDAG

The original Kaspa project is a notable innovation in the blockchain domain, distinguished primarily by its GhostDAG protocol. This protocol marks a departure from traditional blockchain structures, adopting a Directed Acyclic Graph (DAG) layout. Unlike the linear, single-chain design of conventional blockchains, GhostDAG allows for multiple blocks to be added in parallel, significantly improving scalability and transaction processing speed. This unique architecture not only enhances throughput but also maintains robust security and decentralization, addressing some of the core limitations faced by standard blockchain systems.

Mining Landscape

The current state of cryptocurrency mining is characterized by the increasing dominance of ASIC mining. ASICs, being highly specialized and efficient for mining purposes, have gradually outpaced GPU and CPU miners. This shift has led to a concentration of mining power in large-scale mining farms, which can afford the costly ASIC setups. This centralization poses risks to the network's security and contradicts the decentralized ethos of blockchain technology. It also creates barriers for individual or small-scale miners, as the high entry cost and competitive disadvantage against ASIC farms make it less viable for them to participate.

Need for Change

A shift towards GPU mining is essential for the health and decentralization of the network for several reasons:

1. **Democratization of Mining**: GPUs are more accessible and widely used in regular computers, making it easier for individuals and small miners to participate in the mining process.
2. **Decentralization and Security**: By enabling more miners to participate, GPU mining helps in distributing the mining power more evenly across the network. This decentralization is crucial for reducing the risk of central points of failure and potential 51% attacks.
3. **Inclusivity and Sustainability**: A GPU-focused approach is more inclusive, allowing a broader community of enthusiasts and small-scale miners to contribute to the network. It also tends to be more sustainable and energy-efficient compared to the high-power requirements of ASIC mining.
4. **Resistance to ASIC Dominance**: Shifting to GPU mining can counter the monopolization of mining by large ASIC farms, ensuring the network remains resilient and aligned with the decentralized principles of blockchain technology.

The transition to GPU mining as proposed by the Karlsen project represents a strategic move to uphold the decentralized, inclusive, and secure nature of blockchain networks, addressing the challenges posed by the current ASIC-dominated mining landscape.

Project Goals:

Decentralization

GPU mining significantly contributes to a more decentralized network in several ways:

1. **Distributed Mining Power:** GPUs are more universally accessible than ASICs, meaning a larger number of individuals can participate in mining. This distribution of mining power across a broader base of participants prevents the concentration of power in the hands of a few large-scale ASIC miners, thereby promoting a more decentralized network structure.
2. **Reduced Risk of Centralization:** The centralization of mining activities in ASIC farms poses a risk to blockchain networks, as it can lead to a small number of entities gaining disproportionate control over the network. By enabling GPU mining, this centralization risk is mitigated, as it becomes economically and technically feasible for more players to join the mining process.

Accessibility

GPU mining lowers entry barriers for small-scale miners in several ways:

1. **Affordability:** GPUs are generally more affordable and have a broader range of price points compared to ASICs. This makes it more feasible for individuals or small groups to invest in mining equipment.
2. **Availability:** GPUs are widely used in personal computers and gaming setups, making them more readily available to the average consumer compared to specialized ASIC hardware.
3. **Versatility:** Unlike ASICs, which are designed for a specific algorithm, GPUs are versatile and can be used for various purposes, including gaming, graphics rendering, and mining different cryptocurrencies. This versatility adds to their appeal for small-scale miners.

Network Security

GPU mining enhances network security in the following ways:

1. **Resistance to 51% Attacks:** A more decentralized network, achieved through widespread GPU mining, reduces the risk of a 51% attack. In such an attack, an entity with majority control of the network's mining power can manipulate the blockchain. A distributed mining base makes it more challenging for any single entity to gain such control.
2. **Diverse Participant Base:** With more participants in the mining process, the network benefits from a wider range of stakeholders invested in its security and integrity. This diversity helps in maintaining a robust and secure network.
3. **Adaptability and Resilience:** GPU-based networks can be more adaptable and resilient. Since GPUs are not tied to a specific algorithm, they can quickly adapt if the network decides to change its underlying protocol or hashing algorithm for security reasons.

GPU mining plays a crucial role in promoting decentralization, lowering barriers to entry for mining, and enhancing the overall security of the network. This approach aligns well with the foundational principles of blockchain technology, ensuring that networks remain open, inclusive, and secure.

Technical Specifications:

Karlsen uses the Blake3 algorithm inside its hashing algorithm. Blake3's speed advantage comes from its algorithmic efficiency, parallelism, and optimization for common hardware. The lack of ASICs for Blake3 is due to its relatively recent introduction, the lack of a strong incentive for developing Blake3-specific ASICs, and its already excellent performance on general-purpose hardware.

Advantage of using Blake3

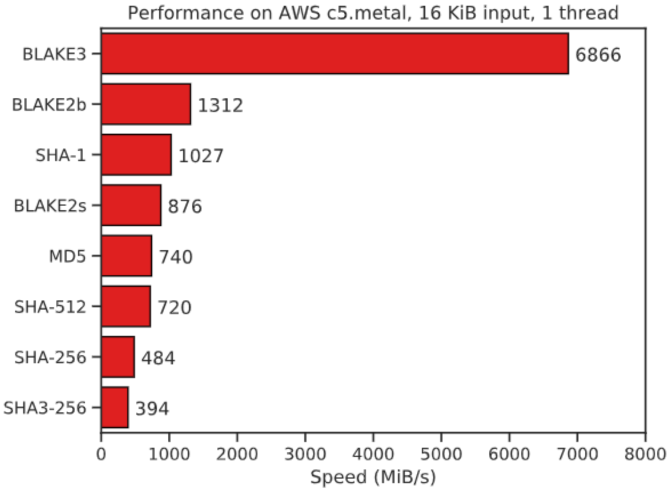
Blake3 is a cryptographic hash function that is designed to be faster than its predecessor, Blake2, as well as other hash functions like Keccak, which is used in the SHA-3 standard. The reasons for Blake3's speed advantage and why ASICs are not currently optimized for it can be broken down into several factors:

1. **Algorithmic Efficiency:** Blake3 is designed with simplicity and efficiency in mind. It uses a simpler round function compared to Keccak. The round function is a core part of the hashing process, and a simpler one can often be computed more quickly. This simplicity translates to less computational work for each hashing operation.
2. **Parallelism:** One of the key features of Blake3 is its inherent support for parallelism. It can process large chunks of data in parallel, taking full advantage of modern multi-core processors. This design significantly speeds up the hashing process on standard computing hardware, such as CPUs and GPUs, which are well-suited for parallel processing. Keccak, while also efficient, does not emphasize parallelism to the same degree.
3. **Optimization for Common Hardware:** Blake3 is optimized for performance on general-purpose hardware like CPUs and GPUs. It takes advantage of the specific architectural features of these processors, such as SIMD (Single Instruction, Multiple Data) instructions, to accelerate its computation.

Regarding the use of Blake3 with ASICs:

- **Specialization of ASICs:** ASICs are highly specialized hardware designed to perform specific tasks very efficiently. Currently, most ASICs in the cryptographic space are optimized for algorithms that are widely used in applications like cryptocurrency mining (e.g., SHA-256 for Bitcoin). Since Blake3 is relatively new and not as widely adopted for such purposes, there hasn't been a strong incentive to develop ASICs specifically for it.
- **Development Time and Cost:** Developing an ASIC is a time-consuming and expensive process. It requires designing and fabricating a new chip from scratch, tailored to the specific characteristics of the algorithm. Given that Blake3 is not the standard in any major application that would justify the cost (like a major cryptocurrency), there's less motivation for ASIC developers to invest in creating Blake3-specific ASICs.
- **Flexibility of General-Purpose Hardware:** The fact that Blake3 is optimized for general-purpose hardware and can be efficiently run on CPUs and GPUs reduces the need for ASICs. The benefit of developing an ASIC for Blake3 would be marginal, especially when considering the cost and effort involved in its development.

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



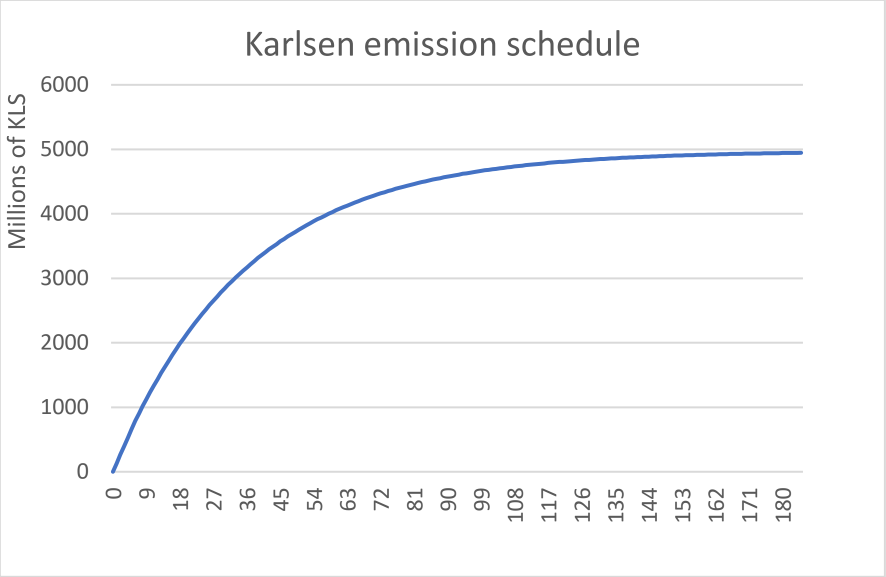
Source : https://github.com/BLAKE3-team/BLAKE3

Economic Model:

The monetary policy of Karlsen closely resembles the Kaspa model, yet it incorporates a more gradual deflation rate to better suit the scale of small GPU miners.

It has two phases :

1. Pre-deflationnary phase : During a six-month period, each block yields a reward of 50KLS. The intended block creation rate is one block per second, although this rate varied during the mainnet's first weeks.
2. Deflationary phase : The block reward undergoes a halving process annually, but this reduction is gradual rather than abrupt. Each month, the reward decreases by a factor of (1/1.4)^(1/12). This calculation is based on an initial block reward of 44 KLS



Karlsen emission schedule

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 supply : approx. 4.961.000.000 KLS

Total mined at 01/01/2025 : approx. 1.7B KLS – (34% of the total supply)

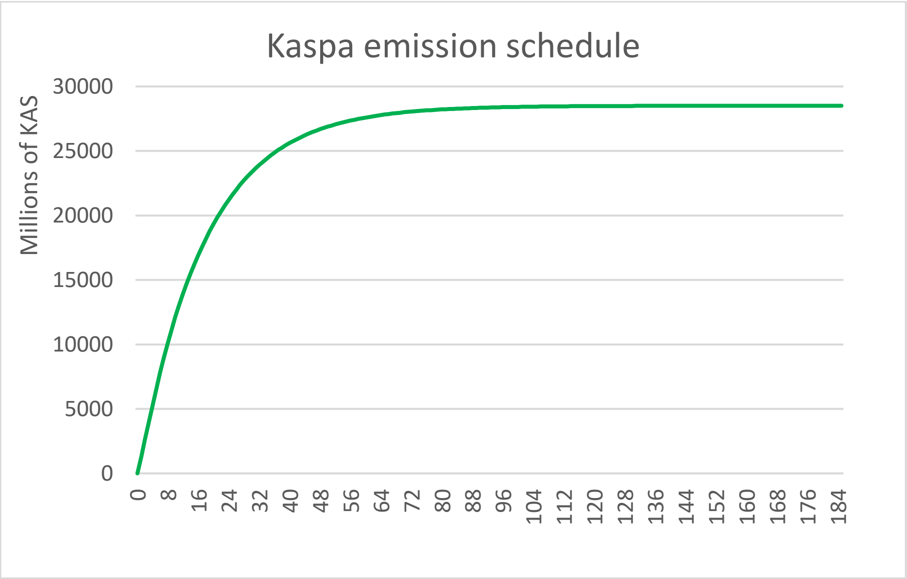
Total mined at 01/01/2026 : approx. 2.6B KLS – (53% of the total supply)

Total mined at 01/01/2027 : approx. 3.3B KLS – (67% of the total supply)

Karlsen emission schedule for the first 2 years

Month	reward	Total mined	Percentage of the supply mined
1	50	131 M	2,66%
2	50	262 M	5,32%
3	50	394 M	7,97%
4	50	525 M	10,63%
5	50	657 M	13,29%
6	50	788 M	15,95%
7	44	904 M	18,29%
8	42,78	1 017 M	20,56%
9	41,60	1 126 M	22,77%
10	40,45	1 232 M	24,92%
11	39,33	1 336 M	27,01%
12	38,24	1 436 M	29,05%
13	37,18	1 534 M	31,02%
14	36,15	1 629 M	32,95%
15	35,15	1 722 M	34,82%
16	34,18	1 812 M	36,63%
17	33,24	1 899 M	38,40%
18	32,32	1 984 M	40,12%
19	31,42	2 067 M	41,79%
20	30,55	2 147 M	43,41%
21	29,71	2 225 M	44,99%
22	28,89	2 301 M	46,53%
23	28,09	2 375 M	48,02%
24	27,31	2 447 M	49,47%

In comparison, the above chart show the Kaspa emission schedule, designed with a short emission schedule and fast deflation rate were designed to address the issue of ASIC dominance.



Kaspa emission schedule

Total supply : approx. 29.000.000.000 KAS

Total mined at 01/01/2023 : approx. 15.3B KAS – (53% of the total supply)

Total mined at 01/01/2024 : approx. 21.9B KAS – (76% of the total supply)

Total mined at 01/01/2025 : approx. 25.1B KAS – (87% of the total supply)

Kaspa emission schedule for the first 2 years

Month	reward	Total mined	Percentage of the supply mined
1	500	1 314 M	4,61%
2	500	2 629 M	9,23%
3	500	3 944 M	13,84%
4	500	5 259 M	18,45%
5	500	6 574 M	23,06%
6	500	7 889 M	27,68%
7	440	9 046 M	31,74%
8	415,30	10 138 M	35,57%
9	391,99	11 169 M	39,18%
10	369,99	12 142 M	42,60%
11	349,22	13 060 M	45,82%
12	329,62	13 927 M	48,86%
13	311,12	14 746 M	51,73%
14	293,66	15 518 M	54,44%
15	277,18	16 247 M	57,00%
16	261,62	16 935 M	59,41%
17	246,94	17 584 M	61,69%
18	233,08	18 197 M	63,84%
19	220	18 776 M	65,87%
20	207,65	19 322 M	67,79%
21	195,99	19 837 M	69,59%
22	184,99	20 324 M	71,30%
23	174,61	20 783 M	72,91%
24	164,81	21 216 M	74,43%

Research and Developments:

- **enhance ASIC resistance and decrease the efficiency of FPGAs** :

  To bolster ASIC resistance and lessen FPGA efficiency in comparison to GPUs, a multifaceted approach can be employed:

  First, by developing complex hashing algorithms that demand extensive memory usage, capitalizing on the inherent strength of GPUs in memory handling. This not only makes ASICs less effective but also enhances the algorithm's resistance to specialized hardware optimizations.

  Simultaneously, integrating a heavy dependence on RAM within the algorithm further tilts the balance in favor of GPUs, which generally excel in memory performance.

  Finally, vigilantly monitoring the mining network is crucial to detect any dominance by ASICs or FPGAs, allowing for timely adjustments to the algorithm to maintain a level playing field.

  This continuous monitoring and adaptation ensure that the mining process remains accessible and efficient for GPU users, thereby preserving the decentralization and security of the network.

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