PHICOIN (PHI): The PoW High-Performance Infrastructure

Phicoin Dev Team
version: v0.2
devteam@phicoin.net

***Abstract*—PHICOIN (PHI) is a high-performance cryptocurrency based on the Proof-of-Work (PoW) mechanism. It aims to provide ordinary users with decentralized participation opportunities through an improved and innovative mining algorithm and fair design principles. PHI addresses the challenges of centralization in cryptocurrency mining by enhancing resistance to ASIC and FPGA devices and promoting fair participation. This paper outlines the technical specifications, mission, and roadmap for PHI, highlighting its potential to become a foundational infrastructure for PoW cryptocurrencies.**

***Index Terms*—Cryptocurrency, Proof-of-Work, Decentralization, Mining Algorithm, GPU Mining, Blockchain**

I. Introduction

In the early days of Bitcoin (BTC), the Proof-of-Work (PoW) mechanism provided ordinary people with a fair and decentralized opportunity to participate [1]. However, as the mining industry evolved, the widespread use of FPGA and ASIC devices turned mining into a centralized business, making it increasingly difficult for average individuals to profit from PoW mining.

BTC mining has become more specialized and centralized, raising the barrier to entry and hindering the essence of decentralization. Additionally, Bitcoin's low transactions per second (TPS) and lack of effective scalability make it insufficient for modern financial applications.

Since Ethereum (ETH) transitioned to the Proof-of-Stake (PoS) mechanism [2], many traditional GPU miners have lost stable mining income. Specialized ASIC devices have dominated the traditional Ethash mining market, and large-scale professional mining farms use outdated graphics cards (like RX470). These GPUs, large in scale and centralized like ASICs, create obstacles for ordinary people to participate, further impeding decentralization.

Moreover, large miners with access to cheap electricity resources have further monopolized the mining market, leading to centralization among miners and transactions, leaving ordinary users with virtually no chance to participate.

These issues have resulted in the market lacking a truly fair, decentralized, high-performance, and scalable PoW cryptocurrency. To address these long-standing pain points, we introduce PHICOIN—the PoW High-Performance Infrastructure cryptocurrency, aiming to become a foundational infrastructure for PoW cryptocurrencies.

We envision PHICOIN as a PoW cryptocurrency with high performance, capable of swiftly phasing out outdated equipment while maintaining continuous mining opportunities. It offers fair participation to everyone, allowing individuals to use their own equipment to contribute collectively and maintain the network. This project will belong to all participants, emphasizing complete decentralization and ensuring that the infrastructure is maintained by everyone.

II. Solution

PHI is a high-performance cryptocurrency based on the PoW mechanism. It aims to provide ordinary users with decentralized participation opportunities through an improved and innovative mining algorithm and fair design principles.

PHI's mining algorithm, **Phihash**, is based on the Ethash cache structure and incorporates the randomness of the KawPow/ProgPow algorithms [3]. It uses the Permuted Congruential Generator (PCG) technology to increase the unpredictability of branches. Additionally, we employ lookup table technology to ensure accurate branch hits, further enhancing the algorithm's randomness and resisting replication attacks from ASIC and FPGA devices.

Fig. 1. Bitmain Antminer S21 XP Hydro 473.00 Th/s @ 5676W [4]

An FPGA (Field-Programmable Gate Array) is an integrated circuit that can be programmed after manufacturing to perform specific tasks efficiently, offering flexibility but requiring specialized knowledge to configure. An ASIC (Application-Specific Integrated Circuit), on the other hand, is a chip designed for a specific purpose, such as cryptocurrency mining, delivering superior performance at the expense of flexibility.

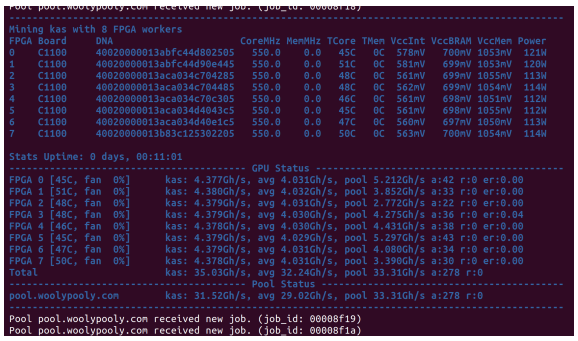

Fig. 2. Xilinx C1100 mining ETHash/ETChash at 4.37Gh/s [5]

The use of FPGA and ASIC devices contributes to the centralization of mining due to several factors. First, the technical barriers to entry are high, as developing and optimizing FPGA configurations or designing ASIC chips requires expertise in hardware programming, chip design, and algorithm tuning. [6] Second, development and operational costs are significant, with ASIC manufacturing involving high upfront capital investment, making it accessible primarily to large organizations. Finally, maintenance and infrastructure requirements—such as specialized cooling systems, power management, and data center facilities—further restrict participation to professional operators with access to industrial-grade setups.

This centralization poses a threat to the decentralized nature of blockchain networks, as large-scale mining farms can dominate the hashrate by leveraging optimized hardware and access to cheap electricity [4]. Such concentration of computational power increases the risk of network control, undermining both security and fairness. PHI aims to mitigate these risks by designing an algorithm that remains accessible to ordinary users with consumer-grade equipment, ensuring equal opportunities for participation and long-term network decentralization.

To achieve fairer participation, we have increased the memory requirement over 4 GB, ensuring that only users with modern GPUs can participate in mining. This approach not only prevents participation from outdated GPUs held by large miners—which are power-hungry, large-scale, and highly centralized, causing resource monopolization—but also effectively reduces their impact on the mining process. [7]

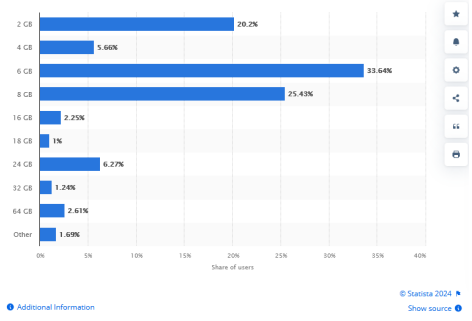

Fig. 3. Video random-access memory (VRAM) share among Steam users as of March 2024

We have also added FP32 logic computation branches in the mining algorithm, fully utilizing the high floating-point computing capabilities of GPUs. FP32 arithmetic has long been the backbone of GPU performance, playing a crucial role in applications from gaming to deep learning. GPUs excel at high-throughput FP32 computations by leveraging their parallel architectures, with thousands of cores capable of simultaneously performing floating-point operations. For example, Nvidia's Pascal architecture (2016) delivered 10.6 TFLOPS of FP32 performance, while more recent architectures like Ampere have pushed FP32 throughput to unprecedented levels. [8]

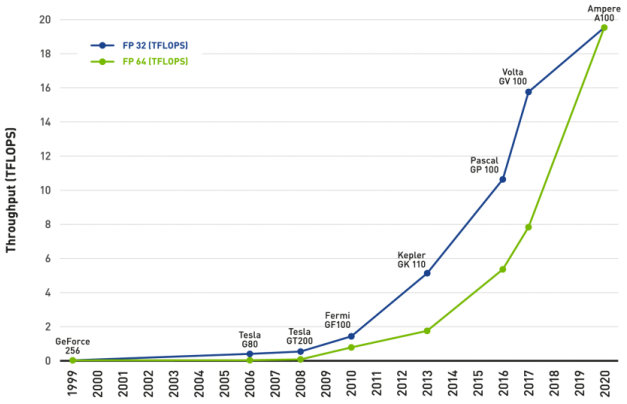

Fig. 4. Single GPU performance scaling [8]

As seen with Huang's Law, which states that GPU performance has been doubling annually since 2012.

Furthermore, GPUs are a consumer-friendly technology, driven by mass-market demand for applications such as VR, 8K, and 16K displays. As these technologies become mainstream, GPUs will become essential parts of personal computing setups, ensuring wide accessibility. This accessibility is crucial for promoting fairness and decentralization in networks like cryptocurrency mining. When every individual can participate with widely available consumer hardware, it mitigates centralization risks posed by specialized hardware like ASICs.

By incorporating FP32 operations, our mining algorithm not only enhances computational efficiency but also provides gaming users with an opportunity to earn rewards without additional investment. This design taps into the vast installed base of consumer GPUs, encouraging decentralized participation and ensuring that the network remains fair and resilient.

III. Mission and Goals

PHI's mission is:

- **Decentralization and Fair Participation**: Ensure that every user, whether an ordinary gaming PC user or a small miner, can fairly earn rewards in the PHI network.
- **High Performance**: Provide superior transaction speed and performance to meet the needs of modern financial applications.

- **Becoming the Infrastructure for PoW Cryptocurrencies**: Offer high-performance infrastructure for PoW cryptocurrencies, supporting more applications in the future.

IV. Technical Highlights

A. General Information

- **Full Name**: PHICOIN
- **Description**: The PoW High-PerformanceInfrastructure
- **Genesis Block**: The Times 11/06/2024: Donald Trump wins US election 2024 to become 47th president.
- **Symbol**: Φ

B. Blockchain Specifications

- **Block Time**: 15 seconds.
- **Block Size**: 4 MB
- **TPS**: 1,092 TPS
- **DAG Size**: > 4 GB
- **DAG Increasing**: 25% / year
- **Total Supply**: unlimited
- **Halving**: Yearly
- **Halving Times**: 2

According to Huang's Law, the performance of GPUs has been increasing at a rate faster than Moore's Law. This trend is evident not only in computational power but also in memory capacity. Over the past two decades, the memory capacity of entry-level graphics cards has grown at an impressive average annual rate of 25.64%. In 2004, the NVIDIA GeForce 6200 offered only 64MB of memory, while by 2024, the NVIDIA RTX 3050 boasts 6GB, representing a nearly 100-fold increase.

This rapid evolution in GPU memory and performance is crucial for supporting the demands of modern applications, from real-time rendering and machine learning to blockchain operations and cryptographic computations. PHI Coin leverages these advancements to enhance network scalability, security, and efficiency. With GPUs becoming increasingly powerful, PHI Coin ensures its infrastructure remains future-proof by capitalizing on cutting-edge technologies for mining, encryption, and decentralized computing.

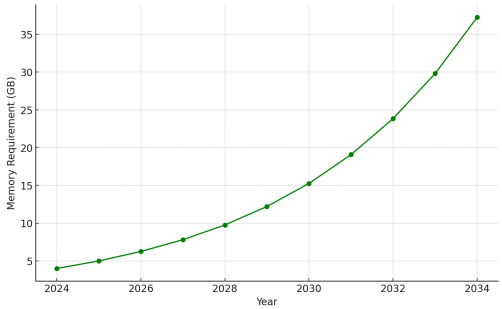

Fig. 5. Evolution of GPU Memory Requirement Over 10 Years

The chart above illustrates the planned evolution of GPU memory requirements for PHI coin mining over 10 years. Starting at 4 GB in the first year, the memory requirement increases by 25% every year, reaching 40 GB by the 10th year.

Unlike Bitcoin's halving model, PHI Coin adopts an alternative approach by increasing hardware requirements over time. Mining activities are always anchored to the memory capacity of entry-level devices, ensuring that as gamers and consumers naturally upgrade their equipment, they remain eligible to participate. This strategy guarantees fair participation across all timeframes, as everyone can access the network equally using readily available consumer-grade hardware.

We encourage continuous participation while phasing out outdated GPUs as the DAG file grows. By gradually raising the memory threshold, PHI coin ensures that miners remain competitive and profitable while maintaining a sustainable and up-to-date mining ecosystem. This thoughtful upgrade cycle not only extends the lifespan of the mining ecosystem but also supports the ecological balance of the network by discouraging outdated and inefficient hardware.

ALL VIDEO CARDS	MAY	JUN	JUL	AUG	SEP	
NVIDIA GeForce RTX 3060	6.19%	5.66%	5.88%	5.51%	5.86%	+0.35%
NVIDIA GeForce RTX 4060	2.82%	3.02%	3.47%	3.41%	4.58%	+1.17%
NVIDIA GeForce RTX 4060 Laptop GPU	2.84%	3.58%	3.21%	4.55%	4.37%	-0.18%
NVIDIA GeForce RTX 4060 Ti	2.31%	2.45%	2.84%	2.90%	3.66%	+0.76%
NVIDIA GeForce GTX 1650	4.52%	4.16%	4.00%	3.91%	3.64%	-0.27%
NVIDIA GeForce RTX 3060 Ti	3.84%	3.56%	3.58%	3.43%	3.57%	+0.14%
NVIDIA GeForce RTX 3070	3.70%	3.36%	3.52%	3.15%	3.31%	+0.16%
NVIDIA GeForce RTX 2060	3.75%	3.40%	3.43%	3.14%	3.30%	+0.16%
NVIDIA GeForce RTX 3060 Laptop GPU	3.37%	3.36%	3.00%	3.50%	3.00%	-0.50%
NVIDIA GeForce RTX 4070	2.46%	2.38%	2.76%	2.52%	2.91%	+0.39%

Fig. 6. Steam Hardware Survey: September 2024

Based on Steam's data, GPUs with 6GB, 8GB and 12GB of memory are increasingly becoming mainstream, reflecting gamers' growing demand for more powerful hardware capable of handling modern titles and higher resolutions. This shift highlights the importance of keeping mining requirements aligned with these trends, ensuring that participants with popular mid-range and high-end GPUs can continue to mine PHI coin efficiently. [9]

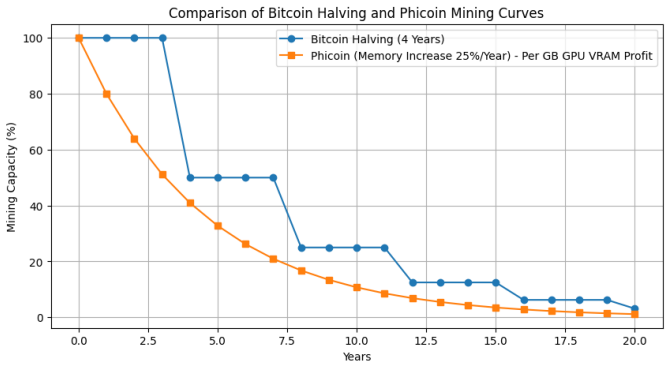

Fig. 7. Comparison of Bitcoin Halving per block and Phicoin Mining Curves per GB vram

This chart compares the mining reward models of Bitcoin and Phicoin over 20 years. The Bitcoin Halving Curve shows that the block rewards decrease by half every four years,

resulting in a stepped decline in mining capacity. In contrast, the Phicoin Curve demonstrates that with an annual 25% increase in memory requirements, the mining capacity per GB of GPU VRAM gradually decreases over time.

The Phicoin memory-increase model functions similarly to Bitcoin's halving mechanism in terms of coin supply control. However, Phicoin's model has a unique advantage: the rising baseline hardware requirements align with the natural technology upgrade cycle. As people upgrade to more powerful GPUs for gaming, watching high-definition content, or other computational needs, they naturally acquire the required hardware without incurring additional burdens. This process eliminates outdated equipment and ensures fairness within the network by continuously leveling the playing field.

C. Mining Algorithm: Phihash

Phihash combines the cache structure of Ethash and the randomness of KawPow/ProgPow to enhance resistance against ASIC and FPGA devices. Key features include:

1) Permuted Congruential Generator (PCG): PCG is an efficient and easy-to-implement pseudo-random number generator with excellent randomness and low memory usage [10]. This randomness enhances the unpredictability of the mining process, thereby increasing resistance to ASIC and FPGA devices.

Feature	PCG32	KISS99	PCG32 Advantage
Simplicity	Simple state update using multiplication and addition. Easy to understand.	Combines multiple generators (LFSR, XORShift), making it complex.	Simple structure, difficult for ASIC to optimize.
Quality of Random Numbers	High-quality randomness, avoids low entropy regions. Suitable for cryptography and simulations.	Lower quality due to correlations between combined generators. Shorter period.	Higher quality randomness, better for unpredictable applications.
Performance of Generation	High performance with optimized generation. Efficiently executed by modern CPUs and GPUs.	Multiple operations for each generation, resulting in lower performance.	Faster generation with lower overhead, benefits from parallelism.

Fig. 8. Performance and Quality Comparison between PCG32 and KISS99

2) FP32 Computation: FP32 (single-precision floating-point) logic computation leverages the high floating-point computing power of GPUs. This design better utilizes modern GPUs' advantages, improving mining efficiency and fairness, allowing ordinary users to earn considerable rewards in the PHI network.

```
# Pseudocode PhiHash steps:
1. Input: 'phi_seed', 'kernel
2. Initialize Random State:
   - seed0 = phi_seed & 0xFFFFFFFF
   - seed1 = phi_seed >> 32
   - fnv_hash = 0x811c9dc5
   - pcg_rnd_state = {
       state: fnv1a(fnv_hash, seed0),
       inc: fnv1a(fnv_hash, seed1) | 1
     }
3. Create DAG Load and Cache Sequences:
   - mix_seq_dst = [i for i in range(
       PHIPOW_REGS)]
   - mix_seq_cache = [i for i in range(
       PHIPOW_REGS)]
   - shuffle(mix_seq_dst, pcg_rnd_state)
   - shuffle(mix_seq_cache, pcg_rnd_state)
4. Set Kernel-Specific Constants:
   if kernel == KERNEL_CUDA:
     define_cuda_constants()
   else:
     define_other_kernel_constants()
5. Generate DAG Structure and Perform Inner
    Loop Cofmputations:
   - dag = [uint32_t(0)] * PHIPOW_DAG_LOADS
   - for loop in range(NUM_LOOPS):
       - offset = get_global_offset(loop,
           pcg_rnd_state)
       // Cache Access:
       - src = mix_seq_cache[i % PHIPOW_REGS]
       - dest = mix_seq_dst[i % PHIPOW_REGS]
       - offset = pcg32(pcg_rnd_state) %
           PHIPOW_CACHE_WORDS
       - data = c_dag[offset]
       - mix[dest] = merge(mix[dest], data,
           pcg32(pcg_rnd_state))
       // Random Mathematical Operations:
       - src1, src2 = get_unique_sources(
           PHIPOW_REGS, pcg_rnd_state)
       - random_op = pcg32(pcg_rnd_state) %
           NUM_MATH_OPS
       - if random_op == FP32_TANH_OP:
           mix[dest] = FP32_TANH(mix[src1],
               mix[src2])
         else:
           mix[dest] = perform_math_operation(
               mix[src1], mix[src2], random_op
               )
       // Merge DAG Data to Registers:
       merge_dag_data(mix, data_dag, pcg32(
           pcg_rnd_state))
6. Return compute_hash(mix)
```

Listing 1. Pseudocode for PhiHash

V. Tokenomics

A. Coin Emission & Inflation Control

PHI's supply strategy ensures that 100% of the tokens are generated through mining, adhering to the principle of fair distribution. To maintain long-term sustainability and encourage continuous participation, PHI is designed as an unlimited-supply cryptocurrency. However, to control inflation after the second year, we introduce a carefully structured issuance plan.

In the first month, PHI will launch a Testing Mining phase, focused on testing internal blockchain parameters and stability. During this phase, the network will use the Kawpow algorithm to resist ASIC mining, ensuring a fair start for all participants. At the end of this phase, 210,240,000 PHI will be distributed to all participants based on their contributions during testing.

Once the mainnet goes live, the PHI earned during the Testing Mining phase will be fully allocated to participants. Following the mainnet launch, the issuance schedule is as follows: - First year: Each block generates 5 Φ. - Second year: Block rewards halve to 2.5 Φ. - Subsequent years: Block rewards stabilize at 2.5 Φ, without further reduction.

This issuance plan ensures a controlled inflation rate after the Testing Mining phase. The inflation rates for the first three years are: - 4.76% after the first year, - 2.32% after the second year, - 2.22% after the third year.

These inflation levels are carefully calibrated to foster sustainable growth, ensuring the longevity and viability of the PHI project. Block rewards start at 5 Φ per block, halving in the first year, and then remaining fixed 2.5 Φ per block. This design aims to incentivize early participants by increasing the initial supply and gradually reducing inflation to achieve supply stability, forming a more predictable supply structure.

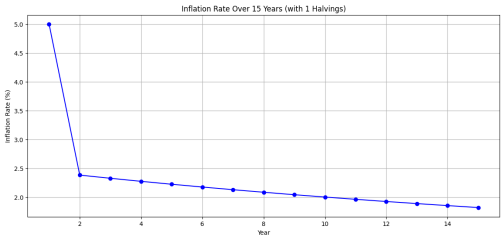

Fig. 9. Phicoin's Inflation Rate Over the Next 15 Years

By gradually reducing the minting amount and block rewards, PHI provides strong incentives for early adopters while ensuring a low-inflation stable model in the long term, supporting the healthy ecological development of the currency.

B. Coin Distribution

All PHI tokens are generated exclusively through mining, ensuring that the network remains decentralized and fair. 95% of the mined tokens are allocated directly to miners, creating a robust incentive structure that rewards participants and ensures fairness.

To support the essential operations of the project, PHI collects a 5% mining fee, which is allocated as follows: - 3% is dedicated to maintaining core infrastructure, including the operation of fundamental nodes, blockchain explorers, and continuous airdrop activities to foster engagement and participation. - 2% is reserved for developer incentives, encouraging innovation and continuous improvements within the ecosystem.

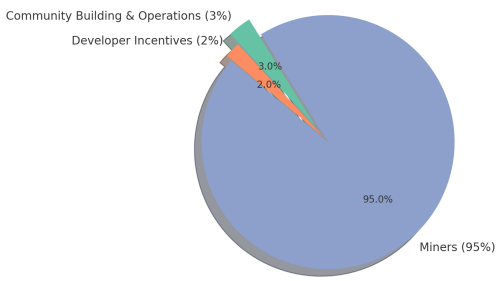

Fig. 10. Phicoin Distribution

Importantly, these coins are not distributed all at once. Instead, they are gradually released alongside mining activities, ensuring sustainable development and incentivization over the long term. We are committed to fostering an environment of fairness and sustainable growth, ensuring that PHI is a decentralized, participatory project.

We aim to ensure continuous mining opportunities for the community. Even after the second halving, Phicoin's issuance will not converge to zero. As the size of the DAG file increases, older, less efficient GPUs will naturally phase out, allowing miners with newer hardware to remain profitable. Our vision is to create a dynamic ecosystem where innovation and sustainability thrive, ensuring that both early supporters and long-term participants can benefit from mining Φ for years to come.

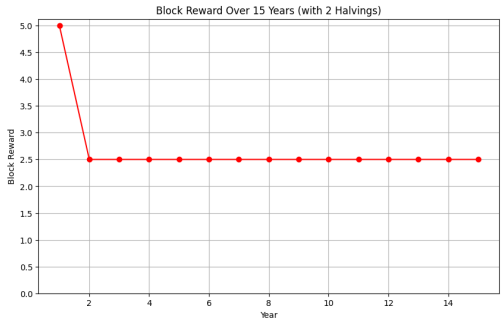

Fig. 11. Block rewards for each block over the next 15 years

VI. Roadmap

A. Phase 1: Testing Mining Phase

Launch the Testing Mining pool, using the Kawpow algorithm for 30 days to create a fair starting point for all participants. This phase focuses on testing network parameters and stability, ensuring a robust and decentralized foundation for the PHI blockchain.

B. Phase 2: Launch Phase

Deploy the mainnet along with core infrastructure, including the blockchain explorer, wallets (desktop, mobile, and web versions), and other foundational tools. These resources ensure that users can safely manage their PHI assets and monitor the network's operations.

C. Phase 3: Bridging Phase

Develop cross-chain bridges between PHI and major blockchain networks such as Solana and Ethereum. This phase will allow PHI to integrate with decentralized exchanges (DEX), enhancing liquidity and expanding its use cases.

D. Phase 4: Sustainable Development Phase

Once the mainnet is live and cross-chain bridges are established, PHI will continuously generate new blocks, providing a sustainable PoW infrastructure for all participants. PHI aims to become a long-term, decentralized option within the broader cryptocurrency landscape.

E. Note on Centralized Exchange (CEX) Listings

Listing on centralized exchanges (CEX) can be costly, requiring both substantial funds and coins. While we will explore the option of accepting donations to facilitate CEX listings, our primary focus is on building a strong and efficient

network. We believe that with a robust user base and well-developed infrastructure, PHI can thrive as a sustainable, evergreen PoW project. It will offer a fair participation option to all cryptocurrency enthusiasts and establish itself as a viable alternative in the blockchain ecosystem.

We hope that PHI can become an excellent PoW choice, encouraging CEXs and market makers to proactively integrate PHI into their platforms.

VII. Future Outlook

In the short term, we aim for PHI to develop into a GPU-based mining project that offers continuous and sustainable rewards. PHI is designed to be fair, high-performance, and capable of sustainable generation, ensuring that participants—regardless of their size or resources—can benefit equitably from the network. In the long term, we envision PHI becoming a foundational infrastructure in the world of Proof-of-Work (PoW) cryp- tocurrencies. Lastly, my favorite quote encapsulates our project: We (the PoW miners) will never go out of style.

VIII. Acknowledgments

Sincere thanks to Bitcoin (BTC), Ethereum (ETH) and Ravencoin (RVN) for pioneering the PoW mechanism, providing a good foundation for GPU mining and expanding the usability of classic blockchains.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” 2014.
[3] K. H. Gobbetti and E. D. F. Rebufello, “ProgPoW: Mitigating the ASIC Advantage,” IfDefElse, 2018.
[4] WhatToMine, “ASIC Miner Profitability Ranking,” [Online]. Available: https://whattomine.com/asics. [Accessed: Oct. 10, 2024].
[5] "Xilinx C1100 FPGA mining"
[6] Xilinx, "Varium™ C1100 Blockchain Accelerator Card"
[7] Statista, “Video random-access memory (VRAM) share among Steam users as of March 2024,” 2024.
[8] William J. Dally, Stephen W. Keckler, and David B. Kirk, “Evolution of the Graphics Processing Unit (GPU),” *IEEE Micro*, vol. 41, no. 6, pp. 42-51, 2021. doi: 10.1109/MM.2021.3113475.
[9] Steam, “Steam Hardware and Software Survey: September 2024,” 2024.
[10] M. E. O’Neill, “PCG: A family of simple fast space-efficient statistically good algorithms for random number generation,” in *Proceedings of the 2014 International Conference on Computational Science*, 2014.
[11] B. Blackwell *et al.*, “Ravencoin: A Peer to Peer Electronic System for the Creation and Transfer of Assets,” 2018.