VHASH

PROOF OF NFT

Whitepaper
Jan 24, 2025

Jon Miles and Keith Pitcher
NFT Loyalty Systems Inc. dba VHASH

jon.miles@vhash.xyz
keith.pitcher@vhash.xyz

Introduction

Cryptocurrency creation is out of reach for most people. The technical and resource requirements for Proof of Work mining and Proof of Stake validation are cost-prohibitive and technically complex for the everyday person.

Because of this, the VHASH team has deployed Proof of NFT (PoN), introducing a transformative mining mechanism that enables NFTs to function as virtual cryptocurrency miners through VHASH (virtual hash power).

Key Features

- The world's first virtual mining system & virtually mined crypto
- Enables a new trait for NFTs to function as virtual miners
- Near zero technical and resource barriers to entry
- Requires only a 12-word seed phrase for participation
- No continuous internet connection, electricity, or owned device is needed
- Democratizes and decarbonizes cryptocurrency mining
- Time-based fraud-resistant system
- Simple and enjoyable UX based on art and identity

Proof of NFT (PoN) represents the next step toward genuinely user-centric decentralized cryptocurrency creation, making mining and crypto creation accessible to the global population while addressing key environmental and technical barriers of traditional mining and token creation paradigms.

Proof of NFT (PoN) is currently deployed on Ethereum using ERC 721 NFTs. Future expansion to EVM-compatible Layer 2 solutions and high-speed Layer 1 blockchains will further enhance the accessibility and affordability of crypto creation.

Proof of NFT and virtual mining represents a vibrant addition to a crypto industry worth hundreds of billions of dollars across NFTs, hardware-based mining, and tokens ranging from memes to governance.

The VHASH team is committed to educating and informing. Whether you're new to blockchain or working professionally, this whitepaper provides valuable insights into how Proof of NFT shapes the future of crypto creation.

Table of Contents

Blockchain Simplified

A basic understanding of Bitcoin, the world's first real cryptocurrency, helps one understand why the VHASH team has deployed Proof of NFT.

Bitcoin was designed as a decentralized digital payment system that enables peer-to-peer value transfer without relying on central authorities or financial institutions.

This is important because carrying cash domestically or internationally is subject to regulations and potential civil asset forfeiture. At the same time, sending money electronically for legitimate commercial or private purposes is expensive and highly regulated.

Bitcoin works because it has a blockchain. What is a blockchain?

> *Blockchain is a decentralized database technology that records and verifies transactions in a secure, transparent, and immutable manner. Simply put, blockchains are networks of computers that have a copy of the same ledger, verifying transactions as a group and updating the ledger automatically. Blockchain is not new and has existed conceptually since 1991, three years before many people had their first email address.*

Bitcoin's Promise - Consensus-Created Cryptocurrency

A key characteristic of Bitcoin is the cryptocurrency itself. Bitcoin is the reward for those participating in the Bitcoin blockchain who process and validate transactions. Because of this, Bitcoin is the world's first consensus-created cryptocurrency.

Bitcoins are created using Proof of Work (PoW) technology. Proof of Work (PoW) is a consensus mechanism where miners solve complex cryptographic puzzles to validate transactions and add new information blocks to the blockchain. These competing computers get Bitcoin as a reward. It is very secure because each transaction creates a unique and interconnected layer on which other transactions are verified.

Ethereum - Smart Contracts and Token Standards

Ethereum is an environmentally friendly decentralized blockchain platform that serves as a cryptocurrency and a global computing infrastructure. Unlike Bitcoin, which primarily functions as digital money, Ethereum was designed to be programmable and versatile. Thousands of projects and businesses work on Ethereum. Ethereum started as a Proof of Work system but moved to another technology called Proof of Stake. Instead of computers competing for a reward, Ethereum "nodes" are paid to validate transactions.

Ethereum's energy consumption dramatically reduced following "The Merge" in September 2022. By moving from Proof of Work to Proof of Stake, Ethereum reduced its energy impact by 99.98%.

Fundamental Building Blocks

An important user-centered element of blockchains is the wallet system. It has three main components.

- Wallet address: Unique identifier for sending and receiving assets
- Public key: Used for identity verification, like a public account number
- Private key: Acts as a password for accessing and managing assets

The most important string of numbers and characters is called the *private key*. It is the equivalent of a password in everyday banking. Wallets, public keys, and private keys look like this:

Wallet Address:
f2a684661702d3aa72af2b8e3ed09b8ac75dc5cd2826872d20aa0683c4059723

Public Key:
84c387ad9eac63b2b145169fd193f4d0a5b14e515b851262c5678690bec43632096582
8a8ccc5470d242f8e4f114fbeeba58973b388373f3f976626b436b990d

Private Key:

9fb731d7ee1883bb1c0612af37b544d4eaa7cfbe0d1a8a2d8728777ef9eeba89

As these alpha-numeric strings are not human-friendly, blockchain developers have made a system to retrieve the Private Key based on a 12-word seed phrase that looks like this simulated seed phrase:

YANKEE BANANA CREDIT SIERRA GOLF COPPER CAPTAIN ECHO
BRIDGE MANGO LIMA VICTOR

The 12-word seed phrase is the decoder ring to get your private key. If you can memorize your 12-word seed phrase, you have access to your wallet on the blockchain anywhere on the internet. Seed phrases are so important that individuals should remember to:

- Store this seed phrase securely
- Never share it with anyone
- Keep multiple offline backups
- Verify all words are spelled correctly

If someone has access to your seed phrase, they can remove all the value you have in that specific wallet. Once a seed phrase is compromised, the wallet is useless, and you cannot reset the private key.

Tokens - Fungible and Non-fungible

The last major hurdle to understanding blockchains is tokens. There are two types.

Fungible Tokens

- Interchangeable with identical value (like cryptocurrencies)
- Can be divided into smaller units
- Each unit is identical to every other unit
- Examples: Bitcoin, Ethereum, or traditional currencies

Non-Fungible Tokens (NFTs)

- Unique and non-interchangeable
- It cannot be divided into smaller units
- Each token has distinct attributes and value
- Represent ownership of specific digital or physical assets

In short, fungible tokens are all the same. Non-fungible tokens are unique. A good example of a fungible token is the U.S. dollar. There are trillions, and they are all the same.

The Benefits of Proof of NFT

Promise and Problems

Bitcoin's fundamental promise was to enable permissionless, decentralized, and censorship-resistant creation, storage, and transfer of value.

In the early days of Bitcoin, there was a promise that anyone could mine Bitcoin, and for early adopters, there was a sense of community. The reality is that profound technical knowledge was and is required to mine Bitcoin and other Proof of Work coins and to understand what they meant conceptually. Bitcoin was started in 2009, and still today, most people don't know how it works.

With the transition from GPU chips to ASICs, PoW mining quickly became a resource-intensive and highly competitive industry. Vendors often did not deliver the technology ordered. Electricity and heat became real factors, and larger entities started the process of consolidation that we see today.

Mining Bitcoin requires significant technological and financial resources, an "always on" internet connection, and 24-hour monitoring. As a result, most of humanity is locked out of Bitcoin creation and can only buy Bitcoin.

Bitcoin has evolved into a massive store of value, a digital gold. Still, it has not developed into a payment solution because its transactions are slow and expensive, taking anywhere from 10 to 90 minutes. Newer and faster blockchains, up to 1,000,000 TPS (transactions per second), have come to the marketplace as potential solutions for blockchain-based transactions. For reference, the VISA network processes 24,000 TPS.

Bitcoin is also very energy-intensive, resulting in significant carbon emissions. This is partly due to increasing demand and the energy mix of Bitcoin mining.

> *According to the United Nations, to offset just one year of Bitcoin's emissions (2020-2021), 3.9 billion trees would need to be planted, covering an area equivalent to the Netherlands. From 2016 to 2021, every $1 worth of mined Bitcoin caused 35 cents worth of climate damage, comparable to gasoline (41 cents) and beef production (33 cents), according to Wikipedia.*

In addition to its carbon footprint, education has been a challenge, and billions of dollars have been stolen or irretrievably lost due to seed phrase mismanagement.

Despite these challenges, Bitcoin, an anonymously authored computer system that did not exist 20 years ago, has positively reformed the world's idea of value creation and transfer, changing the face of public and private finance.

Bubbles and Resulting Opportunities

Human history and nature are full of speculative explosions, consolidations, and new ecosystems.

The Tulip mania of the 1630s in the Netherlands had its characteristics, but hundreds of years later, tulips and other types of flowers are a global industry. Similarly, the Dot-Com bubble and famous casualties like Pets.com helped pave the way for PetSmart.com and the consolidation of Amazon.

When Ethereum NFTs came to prominence, there was a massive explosion in valuation, with some collections worth hundreds of millions of dollars. After a bull run, the bottom fell out of the NFT market, and a large percentage of collections “went to zero,” holding little or no value.

Many collectors are still passionate, and the NFT market has expanded to include multiple blockchains. Historically, people have enthusiastically bought and wanted to collect everything, from Beanie Babies to Topps baseball cards. The most rare physical and digital items retain value if the fanbase is enthusiastic.

Because not all collectibles have high valuations based on rarity or desirability, Proof of NFT (PoN) provides a pathway for any NFT collectible, despite its intrinsic value, to have a functional value in creating a new cryptocurrency.

All NFTs are equal in the Proof of NFT (PoN) system. Now, each NFT can have both intrinsic and functional value. The only difference is their VHASH (virtual hash power).

This means a common NFT can hold the same functional power in the Proof of NFT (PoN)system as a rare, expensive one. This democratization transforms NFTs from purely speculative assets into functional tools for cryptocurrency creation, giving every NFT holder equal opportunity to participate in the Proof of NFT (PoN) consensus mechanism, regardless of their NFT's market value.

Rug Pulls and Fraud

Like all commerce, crypto has had its share of profiteers and scammers. Proper security is critical when using the blockchain; the end user must be even more responsible than in traditional retail and finance technology. Scamming can happen at a transaction level or a more significant project level. At the project level, one problem is called a “rug pull” or a “rug.”

A rug pull happens when projects launch, hype the project, get people to buy, and then disappear. Due to the potentially anonymous nature of the blockchain, this can be easy. Sometimes, this happens quickly; sometimes, a project founder may wait months or years. The main element is that purchasers hoping to make money or those who believe in a project are left holding the bag. It can happen with NFT projects, meme coins, or any aspect of crypto.

Many Birds, One Simple Stone

Proof of NFT is about involving more people, community building over time, and seeking to solve the problems of *access to crypto-creation with the tools available today and growing as the toolset changes.*

Whereas mining crypto-currency requires significant technical, financial, and infrastructural knowledge, Proof of NFT (PoN) delivers on Bitcoin's promise by enabling the global population to participate in and create cryptocurrencies with NFTs on their phones with fun and engaging art.

Proof of NFT (PoN) democratizes crypto mining by ensuring that end users do not need always-on electricity or consistent internet connectivity to mine crypto. The only technology required is a 12-word seed phrase, a pencil, and a piece of paper.

Proof of NFT (PoN) also contributes near zero carbon to the atmosphere. We are built on Ethereum, a green blockchain that uses 58,000 times less energy than Bitcoin, so scaling globally does not harm the planet, even while including more people in the process.

Ethereum is a robust and secure system replete with inexpensive NFTs, which can mine VToken, the first Proof of NFT (PoN) cryptocurrency. Introducing a new “trait” called VHASH (virtual hash power) Proof of NFT (PoN) adds new capability to existing non-fungible tokens.

Because Proof of NFT (PoN) mines crypto over time, in this first deployment, 15+ years, it inhibits “rug pulls,” usually done in a few weeks or months. Proof of NFT (PoN) is a time-based system that fosters long-term community creation and long-term thinking for teams that use it.

How Proof of NFT (PoN) Works

Proof of NFT (PoN) and VHASH (virtual hash power) enable any Non-fungible Token (NFT) to be a virtual crypto miner by introducing a new trait. We are initially deployed on Ethereum but plan to deploy to other blockchains.

This additional NFT utility is added using a simple and secure process. Using this process, Proof of NFT (PoN) creates a community over time as the mining process distributes tokens to the miners. This method fosters a well-established, historically grounded process of crypto growth due to continued mining. The Proof of NFT smart contracts hold all tokens and control all distribution of tokens. There is no method other than mining to move tokens from the smart contract to a wallet.

The defining trait of Proof of NFT (PoN) is VHASH (virtual hash power). Unlike Bitcoin, which uses a Proof of Work (PoW) algorithm that involves intense calculations and substantial amounts of electricity to perform those calculations, VHASH is all smart contract-based and uses little actual electricity.

When an NFT is onboarded to the Proof of NFT smart contracts, the NFT is assigned Virtual Hash Power (VHASH). Additional VHASH may be added by the user in the future. The amount of mining is entirely based on the VHASH of an NFT compared to the Total Network VHASH, or the cumulative mining power of every NFT Miner in the system. The more VHASH an NFT has, the more tokens it mines.

As the Proof of NFT (PoN) mining algorithm is performed within a smart contract on a blockchain platform, the mining process differs from traditional Proof of Work (PoW) or Proof of Stake (PoS) methods.

In Proof of Work (PoW) or Proof of Stake (PoS) mining, each block is calculated, and tokens are sent to the corresponding address when each new block is established. Most blockchain platforms, such as Bitcoin and Ethereum, have transaction fees for token transfers.

To minimize user transaction/gas fees, virtually mined Proof of NFT (PoN) tokens are not sent automatically to all miners. The mined tokens are allocated to each miner and wait to be claimed by the user. The token allocation is determined by using the Proof of NFT Epoch System.

Epoch System

The Proof of NFT Epoch System sets the number of tokens distributed in each block. As all mining is virtualized, Proof of NFT (PoN) uses the block height of the underlying blockchain platform. The algorithm uses a set number of blocks, called an Epoch, for token distribution. The system has an Epoch that is roughly one month in duration.

At the start of each Epoch, the whole Epoch is allocated a specific number of tokens. Tokens mined are determined by the number of blocks mined, blocks of the underlying blockchain platform in the Epoch, and the amount of NFT Mining power (VHASH) is used to calculate how many tokens are assigned to the NFT miner. The calculations are percentage-based.

$$\text{Tokens Mined} = \frac{Blocks\ this\ NFT\ has\ mined\ in\ the\ EPOCH}{Total\ Number\ of\ Blocks\ in\ the\ EPOCH} \times \frac{NFT\ VHASH}{Total\ Network\ VHASH}$$

The Epoch System permanently stores specific values, such as the Total Network VHASH, during the Epoch. With this information, the correct amount of Tokens to claim can be calculated even years later. For each Epoch, a timestamp is written onchain. This ensures that as the network hash grows, early adopters are allocated the tokens they mined, regardless of when they claim them.

Claiming Tokens

In many mining algorithms, tokens are automatically sent to users with each block reward. In Proof of NFT (PoN), however, tokens are not automatically sent, and the user must claim them. Proof of NFT (PoN) is designed to claim tokens even years later, allowing users to determine when they want to spend money on transaction fees.

Users may claim the mined tokens anytime, allowing for the optimal timing of claims. For users that do not claim frequently, storing the Total Network VHASH within the Epoch ensures that the token numbers are locked in when the Epoch finalizes and moves to a new Epoch. This means at the end of each Epoch, the token amounts are locked in, written onchain, and waiting to be claimed.

Upgrading an NFT Miner

Mining power in the Proof of NFT (PoN) system adapts dynamically to network competition. When additional miners join the network, each NFT Miner's relative virtual mining power naturally decreases, which leads to lower token earnings. To counteract this reduction and maintain or boost mining rewards, users can enhance their NFT Miner with additional VHASH (virtual hash power).

The upgrade process for NFT Miners is straightforward and accessible. VHASH upgrades can be initiated anytime by the NFT owners or their designated wallet addresses. The dApp (Decentralized Application) interface displays all upgrade options for NFT Miners associated with the user's wallet.

When an upgrade is completed, the NFT Miner displays its existing VHASH amount and a new Pending VHASH amount. This Pending VHASH remains inactive and doesn't contribute to current mining operations until all previously mined tokens are claimed. This prevents retroactive upgrading of virtual hash power.

This two-phase approach ensures accurate reward accounting across Epochs. Once all prior tokens are claimed, the Pending VHASH automatically activates and integrates with the total network VHASH, increasing mining power and higher token earnings.

NFT Mining Security

VHASH is proactively secure, minimizing user exposure to threat vectors. Many web3 apps require users to sign an initial message to the service simply to use the service. VHASH does not. VHASH has simple and secure methods to determine how and when to claim mined tokens based on ownership of the NFT Miner. By default, only the wallet only the wallet with the NFT may claim mined tokens. With a VHASH claim and the corresponding on-network transaction to the VHASH smart contract, the system checks to ensure the initiating wallet owns the NFT Miner or has been designated to claim tokens. If the owner of the NFT claims the tokens that were mined, the tokens will be sent to the owner’s wallet.

VHASH has an option for NFT Miners to have a designated wallet address. The wallet that owns the NFT Miner may set a designee wallet address. This designated wallet address will see the NFT Miner in the dApp (Decentralized Application) and may claim the mined

tokens to the designated wallet. This allows an NFT to be safely stored in a cold wallet, not requiring the NFT even to be potentially accessed online while still giving the user the ability to claim mined tokens. The owner of the NFT or the designee wallet may claim mined tokens if the owner sets them. The designee may claim or add additional VHASH to the NFT Miner. Only the actual owner of the NFT may set or change the designee address.

Tokens Unclaimable / Burned

The processing power of smart contracts constrains Proof of NFT (PoN). While thousands, potentially millions, of NFT Miners work in the existing Epoch system, the smart contracts are limited to somewhat simplistic calculations. The number of tokens mined for each NFT Miner is not calculated until the user checks the token amount or claims the tokens. While the number will always be accurate, the Epoch System allocates tokens that can never be claimed.

The tokens mined calculation is percentage-based. As an Epoch covers a period of multiple blocks, additional NFT Miners will be added during Epochs. An NFT Miner may not be mining 100% of the Epoch. Also, adding NFT Miners and Upgrading VHASH will change the Total Network VHASH. This means that the calculations for tokens mined will not account for 100% of allocated tokens for the Epoch. A simplified example follows.

NFT 1: The NFT has not claimed tokens; it has 100% of the Epoch to claim. The calculation is:

$$Tokens\ Mined\ NFT\ 1\ =\ 100\%\ of\ Epoch\ X\ \frac{NFT\ 1\ VHASH}{Total\ Network\ VHASH}$$

NFT 2: The NFT was added halfway through the Epoch and not claimed. If claimed later, it would only claim 50% of the Epoch. However, the Total Network VHASH includes the VHASH of NFT 2 and is used for all Epoch calculations.

$$Tokens\ Mined\ NFT\ 2\ =\ 50\%\ of\ Epoch\ X\ \frac{NFT\ 2\ VHASH}{Total\ Network\ VHASH}$$

In this simple example, 25% of all tokens allocated to the Epoch would be unclaimable as no specific miner has the right to claim them. This is an oversimplification using only two NFT Miners.

VHASH calculates this unclaimable number after each Epoch is finalized using non-smart contract limited software. This number will be published on the VHASH website as

unclaimable and will reduce the maximum circulating supply of the token. This a natural token burn for the Proof of NFT (PoN) system.

Users who claim frequently can reduce the effect of competition from additional NFTs with VHASH. The Epoch system locks in values, so once an Epoch has passed, any additional VHASH upgrades and new NFT Miners will not change any previously token-mined amounts.

Real-World Uses of Proof of NFT (PoN)

Jointly Created Tokens For Everyone

The first deployment of Proof of NFT (PoN) focuses on creating a new cryptocurrency, VToken, that the entire world can mine and create together. This is designed to create a new, valuable, and helpful token while educating people about the blockchain. Interesting things can happen by setting out to create something together on the blockchain, especially when the venture has low barriers to entry for new users.

Cash Back Value Pool Mining

Major centralized credit card networks like VISA charge a 1.4-2.5% interchange fee per transaction. That cost is paid on every transaction by the vendor. A competing Proof of NFT-enabled blockchain product using new and evolving fast blockchains could easily cut that cost to the vendors, leaving a value pool that can be mined. Proof of NFT enabled NFTs could compete for pieces of that value pool as rewards for supporting that transaction network.

Tokenizing Enthusiasm and Sentiment

While some significant figures have released meme tokens and pulled liquidity out of the market, other organizations and individuals could use Proof of NFT (PoN) to tokenize customer enthusiasm over time. For example, a major pop star could sell VHASH-enabled NFTs that generate tokens that can be used in experiences and have their own independent value on the open market. This would tokenize the excitement of the pop star's fanbase, creating an entirely new asset class—the pop star token.

Another use case could be a university rich in history and iconography that wants to tokenize alumni loyalty, creating an asset of value on the blockchain. Instead of issuing a token with the expectation that it will be bought, they could use Proof of NFT (PoN) to

enrich their community over time, creating both valuable NFT collections and tokenizing the spirit of their university.

Companies with exuberant customers, like any number of AI companies, could use Proof of NFT to include their customers in a pre-IPO raise, tokenizing the excitement of the new technology long before traditional investors can buy stock. More than an ICO, Proof of NFT is a time-based way to tokenize assets.

Loyalty Programs

Most corporate loyalty programs are transactional. Customer spending translates into points that can be used. Proof of NFT enables an entirely new type of loyalty program where customer points are both spendable with the company and have free-floating and tradeable value on the open market, potentially turning what some might view as a liability on the books into an asset with market-based value.

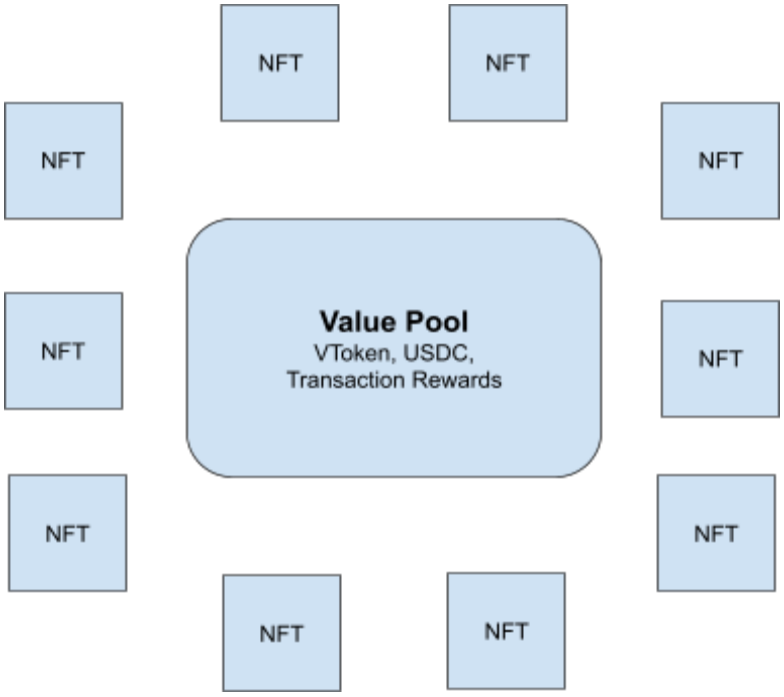
Aid Relief

Aid leaders have long understood that sending "money" rather than blankets and food to foster local economies is better. Post-hurricane recovery efforts like Katrina's "The Road Home" in the United States relied on fiat banking infrastructure to distribute billions of dollars in aid. However, in unbanked parts of the world, Proof of NFT-enabled NFTs could mine USDC from a value pool to distribute aid to circumvent local corruption, providing value directly to those in need. As local vendors adopt blockchain transactions for commerce, the last mile will be solved quickly using mobile cellular, satellite, or SMS-based blockchains.

The Future - Mining From Value Pools

Conceptually, Proof of NFT (PoN) involves NFTs competing for value based on virtual hash power or verified NFTs receiving tokens from a pool of value. The first Proof of NFT deployment is on Ethereum, using ERC 721 NFTs to mine VToken value based on VHASH, virtualized hash power.

However, Proof of NFT Value Pools can hold any token or collection of various tokens with NFTs mining tokens over time. This could be VToken, USDC, or transaction rewards.



Conclusion

Pluribus Currency > Consensus Created Currency

In Latin, pluribus means “out of many.”

While traditional cryptocurrencies have achieved technical decentralization, they remain inaccessible to most people.

Now, through Proof of NFT and VHASH technologies, the strict technical definition of consensus-created crypto is not required. Instead, we propose that Pluribus currency strips away technical barriers and places crypto currency creation in the hands of the many rather than the technically elite.

This is a counterpoint to fiat currency. A government issues fiat currency, but the people make Pluribus currency.

With Proof of NFT (PoN) and VHASH (virtual hash power), we propose a new paradigm for currency creation and tokenization of sentiment. By decoupling mining from energy

and technical requirements and increasing its ease of use and education, consensus-created crypto, or Pluribus cryptocurrency, is now in everyone's hands.

We have always considered Proof of NFT (PoN) and the virtualization of cryptocurrency mining as inevitable. It is the next evolutionary step in a tsunami of constant change.

We hope it helps to rewrite how people create value globally.

Glossary

Core Blockchain Terms

- Blockchain: A decentralized database technology that records and verifies transactions
- Consensus: The method by which transactions are validated
- Proof of Work (PoW): Mining mechanism using computational puzzles
- Proof of Stake (PoS): Validation mechanism using staked tokens
- Proof of NFT (PoN): New mining algorithm using NFTs as virtual miners

Wallet Components

- Wallet Address: Unique identifier for sending/receiving assets
- Public Key: Identity verification code
- Private Key: Password for accessing assets
- Seed Phrase: 12-word recovery phrase

Token Types

- Fungible Tokens: Interchangeable tokens with identical value
- Non-Fungible Tokens (NFTs): Unique, non-interchangeable tokens
- VHASH: Virtual Mining Hash power

VHASH-Specific Terms

- Epoch: Set number of blocks for token distribution
- Total Network VHASH: Cumulative mining power of all NFT Miners
- Designee: Wallet address authorized to claim mined tokens
- Pending VHASH: Newly added hash power awaiting activation

Technical Concepts

- Smart Contract: Self-executing contract with terms written in code
- Block Height: Number of blocks in the blockchain
- TPS: Transactions Per Second
- Pluribus Currency Tokens: Consensus-created cryptocurrency