Haven Protocol
Whitepaper
V3.0.0

Untraceable transactions meets offshore banking.

1. Introduction

Bitcoin paved the way for electronic peer to peer currency. It was the first digital currency to successfully implement a distributed ledger of transactions based on cryptographic proof over trust. Use of digital currency has since grown at an exponential rate with users valuing privacy, anonymity, ease of use and low fees to transfer currency anywhere in the world in a fraction of the time of traditional methods.

Bitcoin however, due to the rapid scale and unforeseen issues, has suffered drawbacks in many of these areas that users of the currency value. Fees became too expensive, transaction times too long and flaws were found in the anonymity of the protocol.

To its aid, came a wealth of altcoins that intended on fixing some of these issues. New coins could move faster and without need to deal with legacy decisions. Most notable of these new currencies was Monero. A truly anonymous protocol.

2. Haven Protocol

Haven is an untraceable cryptocurrency with a mix of standard market pricing and stable fiat value storage. This is without an unsustainable peg or asset backing. It achieves this with a dual coin blockchain. Users can mint and burn Haven [XHV] for the equivalent USD value worth of Haven Dollars [XHVD].

Haven Protocol's cryptographically unknown supply is used to facilitate the fluctuations in the total supply when users burn Haven [XHV] to create the stable value Haven Dollars [XHVD], while allowing Haven [XHV] to be exposed to the natural price movements of the market.

Haven is a fork of Monero, therefore inheriting the stealth and anonymity that it's famous for. Haven also has the benefit of starting the blockchain from scratch with RingCT for extra privacy. Further, Haven's Offshore Storage means privacy conscious individuals can keep their money in an untraceable currency without being subject to market fluctuations.

With Haven, Offshore Storage allows fiat currency storage without having to convert out of Haven. Colloquially, this is akin to having a Swiss bank account in your back pocket.

2.1 Offshore Storage

What is Offshore Storage?

Offshore Storage is Haven Protocol's core concept that powers the minting and burning of Haven [XHV] for Haven Dollars [XHVD] and vice versa. In short, sending Haven [XHV] to Offshore

Storage (burning), mints the equivalent USD value worth of the burnt Haven [XHV] in Haven Dollars [XHVD]. This balance never leaves the Haven blockchain and as such remains completely untraceable and unlinkable to the user.

Digital currency is a useful way to keep your money out of the traditional banking system - only if you can store it without a constantly fluctuating price and the threat of losing significant value. With Offshore Storage, you get the privacy of cutting edge digital currency with a guarantee on the fiat value. This makes Offshore Storage ideal for storing large amounts of money that you do not want exposed to digital currency volatility out of the traditional system.

How?

Haven uses a system called ‘mint and burn’ to maintain fiat value relationship. In practice this works as follows:

Bob decides he wants to put 200 of his Haven [XHV] into Offshore Storage. When you put [XHV] into Offshore Storage, you are burning [XHV] coins into [XHVD] coins, which represents ‘$USD worth of Haven’. Offshore Storage determines the current market value of that Haven (in [XHVD]) based on a weighted average of volume across supported exchanges. This is done using a price oracle.

If the current value of Haven is $1 USD, Offshore Storage will record a value of $200 USD worth of Haven at Bob’s request. The 200 Haven that was sent is then burned into [XHVD] and the total money supply decreases. If the price of Haven then moves to $2 USD and Bob decides to access his Offshore Storage, he will be returned 100 Haven (100 * $2 = $200 USD as per original value). If the opposite occurs and the price of Haven halves to $0.50 then 400 coins will be minted and sent to Bob (400 * $0.50 = $200 USD as per original value).

At first, minting new coins may make you think the value of the coin would decrease as the total money supply has increased. In practice, this operates a little different.

The ‘mint and burn’ method draws on the quantity theory of money, described in monetary economics in order to avoid inflation and changes in currency valuation based on the movements in the total supply.

The theory states that MV = PT where:
M = Money supply
V = Velocity of money
P = Average price level
T = Volume of transactions

An increase in the money supply should, with a constant velocity and volume of transactions (assumptions of the economic model), cause an increase in the price level (inflation). The problem with this is that the money supply of Haven will always be unknown. Although there are 18.4 million coins (before tail emission) that will be mined, the ‘mint and burn’ lets the money supply fluctuate freely. Velocity of money is also cryptographically unfeasible to determine as the Haven blockchain does not reveal the amount of Haven transferred, nor the wallet addresses they are transferred to. For this reason, the currency is unable to be valued based on total supply.

The cryptographic mechanisms that allow this information to remain hidden are what makes Haven a true spectre to the traditional system. For an in-depth breakdown of ring signatures, ring confidential transactions and stealth addresses that power this untraceability and unlinkability it is suggested to read the papers from the Monero Research Lab (linked at the bottom of this paper) from which the Haven Protocol inherits.

Offshore Storage will be implemented once the network reaches a mature stage with enough exchange support to allow redundancy and accuracy of prices. The current focus is on growth,

stability, privacy and usability for everyday transactions with an easy to use mobile wallet app that anyone can use without prior knowledge of crypto.

2.2 Offshore Storage Use Cases

- Point of sales/payment gateway systems where goods can be bought with Haven and stores can immediately lock the USD/fiat value in to protect from price fluctuations. This has the added benefit of keeping the stores' business and income completely hidden on the blockchain as neither his wallet address or amounts are revealed.

- Storing large amount of money outside of the traditional banking system. Privacy focused cryptos are perfect for this but without a reliable way to maintain value through fluctuations the process of holding could be costly. Sending Haven offshore quite literally, creates cryptographically untraceable US Dollars.

3. Supply & Emission

Total supply: 18,400,000 coins before tail emission and Offshore Storage.
Coin symbol: XHV
Coin Units:
1 picohaven/havtoshi = 0.000000000001 XHV (10^-12 -smallest unit)
1 nanohaven = 0.000000001 XHV (10^-9)
1 microhaven = 0.000001 XHV (10^-6)
1 millihaven = 0.001 XHV (10^-3)
Hash algorithm: CryptoNight_Haven (CryptoNight_Heavy tweak - Proof-Of-Work)
Block time: 120 seconds

4. Further Reading

Haven, being a fork of Monero, inherits all whitepapers and academic studies from the Monero Research Lab which can be found here:

MRL-0001: A Note on Chain Reactions in Traceability in CryptoNote 2.0
https://lab.getmonero.org/pubs/MRL-0001.pdf

MRL-0002: Counterfeiting via Merkle Tree Exploits within Virtual Currencies Employing the CryptoNote Protocol
https://lab.getmonero.org/pubs/MRL-0002.pdf

MRL-0003: Monero is Not That Mysterious
https://lab.getmonero.org/pubs/MRL-0003.pdf

MRL-0004: Improving Obfuscation in the CryptoNote Protocol
https://lab.getmonero.org/pubs/MRL-0004.pdf

MRL-0005: Ring Signature Confidential Transactions
https://lab.getmonero.org/pubs/MRL-0005.pdf