Haven

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 it's aid, came a wealth of altcoins that intended on fixing some of these issues. New coins could move faster and not have to deal with legacy decisions. Most notable of these new currencies was Monero. A truly anonymous protocol.

1.1 The Birth of Haven

Haven was born out of Monero inheriting its privacy, anonymity and untraceable/unlinkable transactions the details of which will be described later in the paper.

Standing on the shoulders of giants, Haven pushes out the bleeding edge of the ideal digital currency with enforced anonymity and faster transactions with lower fees. Improvements to the currency however, are only a small part of Haven.

2. Haven Protocol

With Haven, we propose an untraceable, unlinkable currency with native contracts allowing value storage in terms of fiat currency without having to convert out of Haven. Colloquially, this is akin to having a Swiss bank account in your backpocket. This contract is referred to as Offshore Storage.

2.1 Offshore Storage

What is Offshore Storage?

Haven is sent from your wallet to a native smart contract which will hold the balance in terms of the fiat value at the time of the transaction. This balance never leaves the Haven blockchain and as such remains completely untraceable and unlinkable to the user.

Why is this useful?

Digital currency is a useful way to keep your money out of the traditional banking system only as long as you can store it without a constantly fluctuating price and the threat of losing significant value. With Offshore Storage, you get all 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 out of the traditional system that you don't want exposed to digital currency volatility.

How?

Haven uses a system called 'mint and burn' to maintain fiat value relationship. In practice this works as follows.
Bob has a wallet with 1000 Haven and decides he wants to put 200 Haven into offshore storage. If the current value is $1 USD then the contract will promise a return of $200 USD worth of Haven at Bob's request. If the price of Haven 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).
The remaining 100 Haven will be burned decreasing the overall Haven money supply.
If the opposite occurs and the price of Haven halves to $0.50 then 200 coins will be minted and Bob will be returned 400 Haven.

This '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 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 following papers by Cryptonote and MRL of which the Haven protocol inherits.

Ring Signatures and stealth addresses: https://cryptonote.org/whitepaper.pdf
Ring confidential transactions: https://lab.getmonero.org/pubs/MRL-0005.pdf