Havven: a stablecoin system
v0.4

Samuel Brooks, Anton Jurisevic, Michael Spain, Kain Warwick

December 2017

Abstract

There is currently no effective decentralised unit of account. Previous attempts to create stable tokens have either relied on significant centralisation or have been undermined by their complexity. We present Havven, a representative money system which seeks to achieve price stability with respect to an external asset. Havven is a dual-token solution, composed of a stabilised exchange token and the reserve token which backs it. Users are incentivised to maintain this distributed reserve, and to manage the stable token supply so that it is in proportion with the value of the collateral. Because the collateral is encapsulated entirely within the system and distributed among its users, we remove the need for a trusted central authority. Such a stable cryptocurrency, useful for everyday economic purposes, will accelerate the adoption of distributed ledger technology.

Contents

1 Introduction

1.1 Money and Cryptocurrencies

Money has become almost invisible over the past few decades as payment technology has advanced. The technology of money has three key functions: to act as a unit of account, a medium of exchange and as a store of value. In addition, money should ideally exhibit durability, portability, divisibility, uniformity, limited supply, and acceptability. But it is often lost upon users of money that it is itself a technology that can be improved. Specifically, this means improving the performance of our six desirable properties.

Bitcoin is an impressive technological advancement on existing forms of money because it simultaneously improves durability, portability, and divisibility. Further, it does so without requiring centralised control or the enforcement of a nation state from which to derive its value. It is precisely its fixed monetary policy which has protected Bitcoin from debasement and devaluation, allowing it to outperform other forms of money as a store of value, and increased adoption has tended to drive the price up over time. Unfortunately, the fixed money supply has also created the potential for short-run volatility as there is no mechanism within Bitcoin that can dynamically adjust to changing demand.

Bitcoin has thus tended to be a poor medium of exchange and an even worse unit of account. In order for something to perform well as a medium of exchange or unit of account it must remain relatively stable against the price of goods and services.

1.2 Stablecoins

A stablecoin is a cryptocurrency designed for price stability, such that it can function both as a medium of exchange and unit of account. It should ideally be as effective for making payments as fiat currencies like the US Dollar, but still retain the desirable characteristics of Bitcoin, namely transaction immutability, censorship resistance and decentralisation.

Cryptocurrencies are in these ways a far better form of money but have been significantly hindered in their adoption by the volatility of the inflexible monetary policies of decentralised systems. Stability continues to be one of the most valuable and yet the most elusive characteristics for the technology. Clearly, the ability to create alternative and dynamic monetary policies within cryptoeconomic systems is still nascent, and significant research into stable monetary frameworks for cryptocurrencies is required.

1.3 Havven

The Havven stablecoin system is a novel form of representative money in which there is no requirement for a physical asset, thus removing problems of trust and custodianship. The asset used to back the stablecoin is a pool of reserve tokens that collectively represent the system itself; controlling these reserve tokens reflects participation in the Havven system, and are a proxy for its value. Havven generates fees from users who transact in the stablecoin and distributes them among the holders of the reserve token, compensating them for underpinning the system. Havven therefore rewards those who actively participate in maintaining the stability of the system and charges those who benefit from its utility. These rewards are proportionally applied in response to the active management of the supply of the exchange token such that its price mirrors that of the asset it tracks.

Because we have created a system that generates cash flow for participants, we now have an asset which can be used as the collateral to support the stablecoin with a well-defined market value. The key to this is that the value of the system is measured in USD. This allows the system to issue a stablecoin which can be presented and redeemed for a percentage of the collateral tokens valued at 1 USD. Backing a stablecoin in this way is beneficial because such a cryptoeconomic system does not require trust in a centralised party; each participant has full transparency over how many tokens have been issued against the available collateral at all times.

The two linked tokens and the complex of incentives are described below:

Havvens: The collateral token, whose supply is static. The capitalisation of the havvens in the market reflects both the system's aggregate value and the reserve which backs the stablecoin. Thus, users who hold havvens take on the role of maintaining stability. Following bitcoin, the Havven system will appear in upper case and singular; while the havven token will be lower case and may be plural.

Nomins: The exchange token - the stablecoin - whose supply floats. Its price measured in fiat currency should be relatively stable. Other than price stability, the system should also encourage some adequate level of liquidity for nomins to act as a useful medium of exchange.

Each holder of havvens is granted the right to issue a value of nomins in proportion to the USD value of the havvens they hold and are willing to place into escrow. If the user wishes to release their escrowed havvens, they must present the system with nomins in order to free their havvens and trade them again. The holders of this token provide both collateral and liquidity, and in so doing assume some level of risk. To compensate this risk, such nomin-issuers will be rewarded with fees the system levies automatically as part of its normal operation.

1.4 Havven's Design

This issuance mechanism allows nomins to act as a form of representative money, where each nomin represents a share in the havven value held in reserve. Nomins derive value insofar as they provide a superior medium of exchange, and are effectively redeemable for a constant value of the denominating asset. In this paper, we use USD as this asset, but this could be any external and appropriately fungible asset, such as a commodity or a fiat currency.

In this manner, the system incentivises the issuance and destruction of nomins so that the value of the nomin pool expands and contracts in proportion with the total value of havvens backing them. If prices change exogenously, then the system is designed to provide incentives for actors to counteract that change.

The Havven system is relieved of the obligation to respond to major macroeconomic conditions, as it benefits from the stabilisation efforts of large institutions acting in fiat markets. In addition, as Havven has the freedom to significantly overcollateralise its pool of circulating currency, it insulates itself against dramatic corrections in the havven market. Havven therefore acts as a bridge between fiat currency and cryptocurrency as a hybrid of two technologies and possessing the advantages of both.

Finally, the design choice to back the system with a self-referential token was obvious; an asset-backed stablecoin with a cryptocurrency basket as reserve will always be inherently volatile, despite diversification, and will never be able to achieve the bespoke functionality of an asset which derives its value from stability.

Clearly, the introduction of a new cryptocurrency in isolation offers no additional value given the existing and established alternatives such as Bitcoin or Ethereum. Havven thus seeks to derive value from the addition of **stability** to its inherited properties as a modern cryptocurrency. It is designed to substantially improve the technology of money by providing a practical medium of exchange without compromising the benefits that decentralisation offers.

There are many applications which Bitcoin's inherently deflationary monetary policy and volatility presently make impossible. Achieving a cryptocurrency token which demonstrates the best utility characteristics from both fiat-based and cryptography-based money systems will prove to be extremely useful and significantly enhance global uptake of cryptoeconomic technology.

2 System Description

Havven is a dual-token system that, combined with a set of novel incentive mechanisms, stabilises the price of the nomin with respect to an external asset.

The havven token serves two functions:

- To provide the system with collateral.
- To allow actors to participate profitably in stabilising the nomin price.

Collateralisation Confidence in stability of the nomin begins with overcollateralisation, so that the value of escrowed havvens is greater than the value of nomins in circulation. The value of havvens is derived internally by the system as a function of the demand for nomins; this decouples the value of the collateral pool from market speculation.

As long as the ratio of total nomin value to total havven value remains favourable, there is sufficient backing in the underlying collateral pool to ensure that nomins can be redeemed for their face value. The redeemability of a nomin for the havvens against which it was issued strongly supports a stable price.

Incentives Havven rewards those that have issued nomins. These rewards are derived from transaction fees and are distributed in proportion with how well each issuer maintains the correct nomin supply. The system monitors the nomin price, and responds by adjusting its targeted global supply, which individual issuers are incentivised to move towards.

Where volatility persists, stronger stabilisation mechanisms may be applied such as interest rates or automated collateral recovery. Where a significant portion of nomins are being used for hedging, (and hence not generating transaction fees) time-based account fees can be added to ensure that the cost of utility for hedging is not being solely borne by transactions.

2.1 Definitions

We first introduce the core system variables:

$H :=$ havven quantity	$N :=$ nomin quantity
$P_h :=$ havven price	$P_n :=$ nomin price

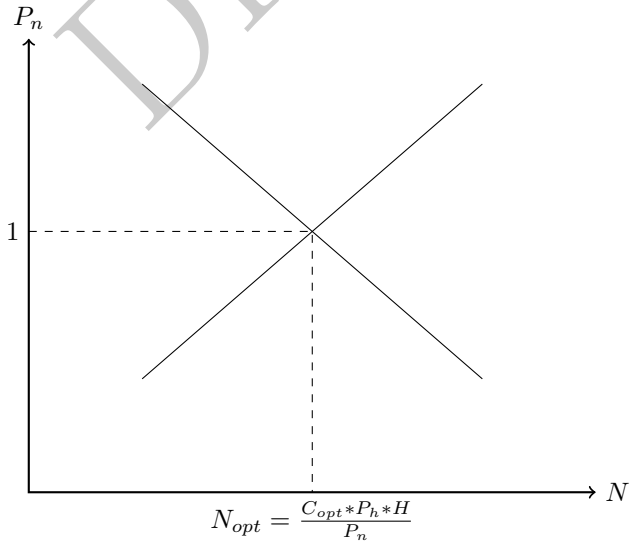
All havven tokens are created in the initial system state, so H is constant. The quantity of nomins, N, floats in response to the actions of havven holders.The Havven system needs to incentivise havven holders to maintain N such that the nomin price, P_n, is stable at \$1.

In Havven, the collateralisation ratio measures the value of nomins against the value of havvens:

$$C = \frac{P_n * N}{P_h * H}$$

2.2 Nomin Equilibrium Price

The law of supply and demand states that there exists some supply of nomins, N_{opt}, where the related level of demand yields an equilibrium price of \$1. This quantity is associated with an optimal collaterisation ratio, C_{opt}. We visualise this situation below.



The system is unable to influence the demand for nomins. We assume that some level of demand exists given the utility of nomins as a stable cryptocurrency. Although demand cannot be manipulated, the supply of nomins is controlled by havven holders, whose issuance incentives are in turn controlled by the system. It follows that as we require a fixed price $P_n = \$1$ and are unable to control either P_h or H, we must manipulate C_{opt} such that $N = N_{opt}$ in order to satisfy our requirement.

2.3 Issuance and Collateralisation

Havven's goal is to remain overcollateralised. In order to do so, the system defines a collaterisation target:

$$0 < C_{opt} < 1$$

It is necessary at this point to distinguish between the nomins in a wallet N_i (equity) and the nomins that have been issued by that wallet $\check{N}_i$ (debt). Note that globally, the $\sum_i N_i = \sum_i \check{N}_i$, as all circulating nomins were issued by some wallet. However, a given wallet may have a balance different from its issuance debt.

Hence we can define the collateralisation ratio for an individual wallet i in terms of its issuance debt:

$$C_i = \frac{P_n \cdot \check{N}_i}{P_h \cdot H_i}$$

The system provides incentives for individual issuers to bring their C_i closer to C_{opt} while maintaining C_{opt} itself at a level that stabilises the price.

Nomin Issuance The nomin issuance mechanism allows Havven to reach its collaterisation target. Issuing nomins escrows some quantity of havvens, which cannot be moved until they are unescrowed. The quantity of havvens $\check{H}_i$ locked in generating $\check{N}_i$ nomins is:

$$\check{H}_i = \frac{P_n \cdot \check{N}_i}{P_h \cdot C_{opt}}$$

Under equilibrium conditions, this implies that $C_i = C_{opt}$ is attained for a wallet exactly when all havvens have been escrowed, at $H_i = \check{H}_i$. As a result, the issuer cannot take actions that would bring C_i above C_{opt} and undercollateralise their position. Instead, C_i can only exceed C_{opt} with price fluctuations.

After generating the nomins, the system places a **limit sell** order with a price of \$1 on a decentralised exchange. This means that the nomins will be sold at the current market price, down to a minimum price of \$1 USD. If we assume implementation on Ethereum, then the nomins are sold for ETH, with the proceeds of the sale remitted to the issuer.

Nomins Destruction In order to access the original havvens that have been escrowed, the issuer must return the same quantity of nomins to the system to be burned. Nomins can be purchased in the open market.

2.3.1 Issuance Example

1. Bob purchases 10 havvens at \$10 each, total value \$100.

2. Bob decides to escrow 5 of his havvens to issue nomins. The optimal collateralisation ratio C_{opt} is 0.5 and P_n is 1. Recall the number of nomins issued is:

$$\check{H}_i = \frac{P_n \cdot \check{N}_i}{P_h \cdot C_{opt}}$$

$$5 = \frac{1 \cdot \check{N}_i}{10 \cdot 0.5}$$

$$\check{N}_i = 25$$

3. The system generates and sells 25 nomins in the market, transferring the funds in Eth to Bob's wallet.

4. Since Bob only escrowed half of his havvens, his individual collaterisation ratio is:

$$C_i = \frac{P_n \cdot \check{N}_i}{P_h \cdot H_i}$$

$$C_i = \frac{1 \cdot 25}{10 \cdot 10}$$

$$C_i = 0.25$$

5. The havven price drops to \$8. The value of his havvens has decreased to \$80 which means his C_i has increased to 0.31 but is still below C_{opt}. The system needs to escrow more of Bob's havvens to maintain the level of collateral.

$$\check{H}_i = \frac{1 \cdot 25}{8 \cdot 0.5}$$

$$6.25 = \frac{1 \cdot 25}{8 \cdot 0.5}$$

6. The system has locked an extra 1.25 of Bob's havvens. Bob now has 6.25 escrowed havvens.

7. The havven price then increases back to \$10. The value of his havvens has increased to \$100 and his C_i has decreased back to 0.25. The system releases 1.25 havvens back to Bob but his original 5 are still escrowed.

2.4 Transaction Fees

Havven needs a direct incentive mechanism that can react to changes in C due to a change in either P_h or P_n.

2.4.1 Nomin transaction fees

Every time a nomin transaction occurs, the Havven system charges a small transaction fee. Transaction fees allow the system to generate revenue, which it can distribute to havven holders as an incentive to maintain nomin supply at C_{opt}.

The fee rate charged on nomin transactions is α_c. It is constant and will be sufficiently small that it provides little to no friction for the user.

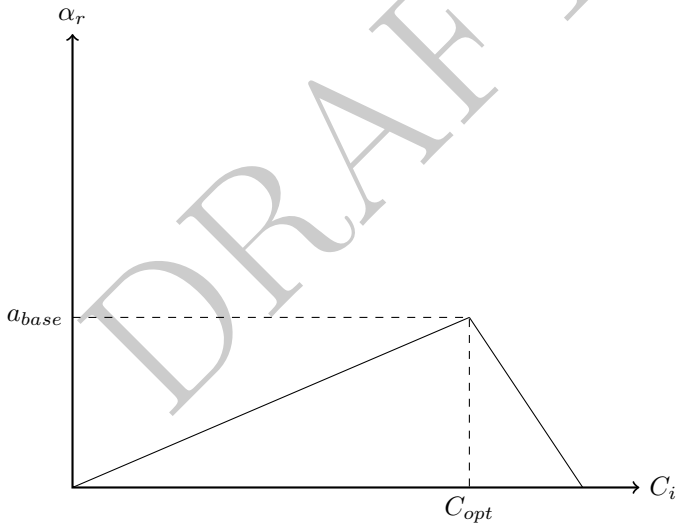
$$a_c = k.$$

2.4.2 Fees received by Havven Holders

The fee rate paid to a havven holder that has escrowed is α_r. This rate changes with respect the individual's unique collaterilisation ratio, C_i. It increases linearly to a maximum at the optimal collaterilisation ratio C_{opt}, before quickly diminishing as C_i approaches C_{max}. Beyond the maximum collaterilisation ratio α_r is 0. Note, α_r is applied to the pool of collected fees which is determined by α_c.

$$\alpha_{R,t,i} = \alpha_{base,t} * f_{i,t}(C_{i,t}, C_{opt}, C_{max,t}),$$

$$f_{i,t}(C_{i,t}, C_{opt}, C_{max,t}) = \begin{cases} \frac{C_{i,t}}{C_{opt,t}} & \text{when } C_i \leq C_{opt}, \\ \frac{C_{max,t} - C_{i,t}}{C_{max,t} - C_{opt,t}} & \text{when } C_{opt} \leq C_i \leq C_{max}, \\ 0 & \text{otherwise.} \end{cases}$$



This fee distribution curve encourages havven holders who have escrowed to maintain their U_i at U_{opt}.

2.4.3 Deriving the base fee rate

The total amount of fees collected from users has to be equal to the total amount of fees paid to the havven holders. We define the total amount of fees collected, $A_{c,t}$ below:

$$A_{c,t} = \alpha_{c,t} * v_{n,t} * \sum_{I} N_{I,t},$$

$v_{n,t}$ the velocity of nomins at t,

$\sum_{I} N_{I,t}$ the total issued nomins.

Next we define the total fees paid to havven holders $A_{R,t}$:

$$A_{R,t} = \sum_{I} \alpha_{R,t,I}.$$

Havven requires that:

$$A_{R,T} = A_{c,t}.$$

Substituting our earlier definition of $\alpha_{R,t,I}$:

$$\alpha_{base,t} * \sum_{I} f_{i,t}(C_{i,t}, C_{opt}, C_{max,t}) = \alpha_{c,t} * v_{n,t} * \sum_{I} N_{I,t}.$$

Solving for $\alpha_{base,t}$:

$$\alpha_{base,t} = \frac{\alpha_{c,t} * v_{n,t} * \sum_{I} N_{I,t}}{\sum_{I} f_{i,t}(C_{i,t}, C_{opt}, C_{max,t})}.$$

We have now defined the maximum fee rate, α_{base}, in terms of the fees collected, $A_{c,t}$. This rate should be achieved when an individuals U_i is at U_{opt}.

The definition of C_{opt} must therefore provide the following incentive. If $P_n > 1$ then the system must encourage more nomin to be issued. If $P_n < 1$, the system must encourage nomin to be burned.

2.5 Collaterilisation Ratio

2.5.1 Optimal collaterilisation Ratio

The optimal collaterilisation ratio C_{opt} is a target for havven holders to reach in order to maximise the amount of fees they receive. C_{opt} is defined in terms of P_n such that havven holders can influence the price of nomin through directly controlling the supply of nomin (a havven holder can change their individual collaterilisation ratio by buying or issuing more nomins).

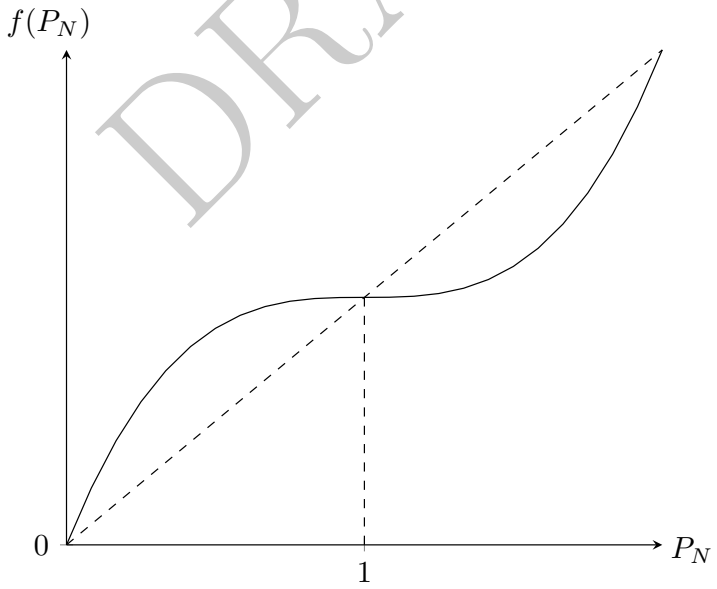
The function for C_{opt} given below provides our dynamic target for havven holders based on the price of nomin. The curve shows that the when P_n is close to \$1, $f'(P_n)$ is small. However, the further P_n diverges from \$1, the larger the derivative becomes, providing an increasing incentive (via fees) for a havven holder to move toward C_{opt}.

$$C_{opt} = f(P_n) * C,$$

$$f(P_N) = max(\sigma * (x-1)^{\phi} + 1, 0),$$

$$\text{where } 0 \leq \sigma, \text{ the price sensitivity parameter,}$$

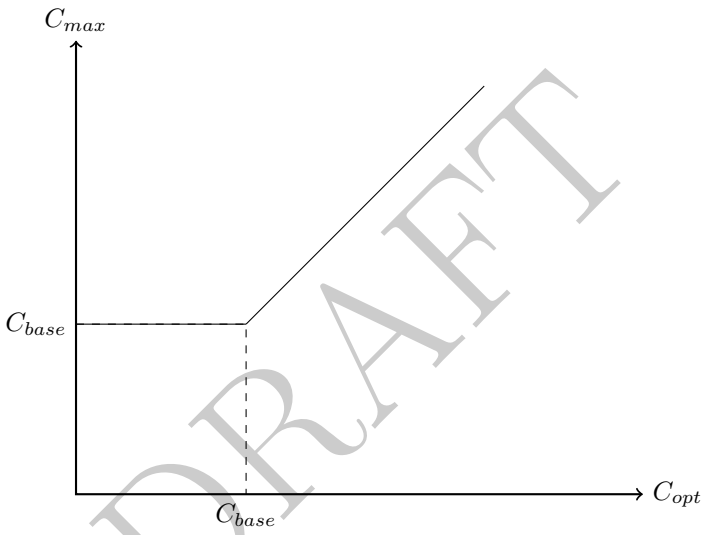
$$\phi \geq 1, \text{ the flattening parameter.}$$



2.5.2 Maximum collaterilisation Ratio

Havven seeks to maintain $C \leq C_{opt} < C_{max} < 1$, in order to remain sufficiently overcollateralised. It might seem intuitive that C_{max} should be a static value. However, since C_{opt} changes linearly with P_n and inversely with P_h, there are several situations where C_{max} may need to change. Below we define C_{max}.

$$U_{max} = \begin{cases} C_{base} & \text{when } C_{opt} \leq C_{base}, \\ a * C_{opt} & \text{otherwise.} \end{cases}$$



2.6 Intrinsic Havven Price

With the havven token being ERC20 compliant, it will have a market price on both decentralised and centralised exchanges.

While the Havven system will access the current market price via a price oracle, it is beneficial to define a P_h that can be determined internally to avoiding the influence of speculation. Ignoring speculative demand, P_h can be expressed as a function of the transaction fees that the system charges. Below we define an initial iteration of the intrinsic P_h.

$$P_{h,t} = \frac{1}{H} * \sum_{t=1}^{\infty} \frac{d_{n,t} * v_{n,t} * \alpha_{R,t}}{(1+R)^t} \approx \frac{d_{n,t} * v_{n,t} * \alpha_{R,t}}{R * H},$$

$P_{h,t}$ is the price of one havven at time t,
H is the number of havvens,
$d_{n,t}$ is the demand for nomins at t,
$v_{n,t}$ is the velocity of nomins at t,
$\alpha_{R,t}$ is the fee from trade with nomins,
R is the interest rate / rate of return of havvens.