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.

Incorporate white paper criticisms.

Contents

1 TODO

Todo list

2 Introduction

2.1 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 goods and services. If the price of money is too variable then it becomes less useful as a denominator of other goods.

2.2 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.

2.3 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 provided 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 for stability are defined 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 stable 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.

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.

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 provide a practical medium of exchange, without compromising the benefits that decentralisation offers in order to substantially improve the technology of money. There are many applications which Bitcoin's inherently deflationary monetary policy and volatility presently make impossible: any token which is able to demonstrate an increment in utility over both fiat and cryptocurrencies in these dimensions will significantly enhance the uptake of cryptoeconomic technology globally.

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.

3 Design Considerations

Havven works by providing a set of market incentives that support the stability of nomin value with respect to an external asset.

Address how to maintain baseline demand.

Address the role of the Havven foundation.

Outline basic verbs for market players.

Move analytical subsections from functional description section to the qualitative analysis and/or rationale sections.

3.1 Investment incentives

We consider the reasons why any rational actor would buy havvens. A potential buyer has at least three avenues for making money in Havven:

Capital gains due to the appreciation of havvens: Due to its constrained supply, and the intrinsic utility of the stablecoin that it backs, it's reasonable to assume that havvens will appreciate in price.

Interest accrued from fees: If the price of havvens stabilises for long periods of time, fees may be the only source of revenue. Ideally fees are set at a level where they are both high enough to be an incentive for rent-seekers to hold havvens in the long term (thus assuming the risk of providing collateral for the system) and low enough not to be a disincentive for ordinary users to transact in nomins. It is desirable, perhaps in a future world dominated by micropayments, for these fees to be negligible for end users, while still being macroeconomically important for the system, and for those who capitalise it.

Arbitrage profit: It is the arbitrageurs who will ultimately bring the price of nomins back into balance by a triangular circuit through nomins, havvens, and the external (crypto or fiat) markets. Arbitrageurs might hold havvens for a short time in order to pursue this strategy.

3.2 Fees

There are several key considerations with respect to fee design:

3.2.1 Fee design considerations

The purpose of fees Fees are intended to be redistributed to actors who support the stability of the system. A fee pool will be distributed periodically for this purpose. If the system determines that the nomin price is too low, then fees could be burned. If the price is too high then the system could sell these back into the system at a discounted rate. The fee collection rate will also be a direct measure of the velocity of money in Havven. It's in the interest of havven holders to maximise liquidity in order to maximise their return.

Fee beneficiaries One possibility would be simply to award fees to any holder of havvens, but in this situation holders can get all the benefit without taking any risk. Although in the aggregate, it would be better for havven-holders if everyone issued nomins, the marginal return for any single player (who cannot issue a large fraction of all circulating nomins) of actually issuing them would not outweigh the risk they take on in doing so. If a user can issue 1% of circulating nomins, then doing so will only increase their fee takings by 1%. Hence rational actors would not be incentivised to issue nomins at all. This is a classic tragedy of the commons.
In order to avoid this situation, we must improve the marginal benefit of issuing nomins into circulation. Hence, fees must be paid to those who *issue* nomins, not just those who hold havvens.

Fee collection The system can charge fees whenever any value is transferred, or any state is updated. Different fee rates have different macroeconomic effects. We might in general like to set higher havven than nomin transfer fees, making the stablecoin itself a lower friction market in order to incentivise its use for exchange. Meanwhile, issuance and redemption fees will change the difficulty of entering and exiting the issuance game.

It is also possible for fees to float. The fee schedule could be altered dynamically in order to stabilise the system. It is even conceivable that the system could set negative fee rates if it needed to and charge punitive fees if a user is above the targeted utilisation ratio. For example, if nomin liquidity is low, meaning the system wants to incentivise issuance, then nomin transfer fees could increase, thus having the combined effect of increasing the interest accrued by issuers (thus incentivising issuance) and at the same time making it more expensive to transact in nomins. This would reduce demand and decrease the liquidity requirements.

Of note, fees are antithetical to arbitrage. The higher the fee, the higher the transaction friction, and the harder it is to make money by arbitrage. For example, if exchange fees amount to 1% per trade, then a full arbitrage cycle between all three markets, (nomins, havvens, and fiat) will cost in excess of 3%. So it would not make sense to undertake arbitrage until such a time as the quoted exchange rate is misvalued by more than 3% relative to the cross exchange rate. Hence, fees compete with arbitrage to stabilise price. Lower fees allow tighter stabilisation, within a window exactly in proportion with the fee rates themselves.

3.3 Encouraging liquidity

It's desirable that when actors issue nomins they are actually injected into the liquidity pool for their intended use, rather than being held by the same actor in order to benefit from both the receipt of fees while retaining the option of using those nomins to rapidly release their havvens. In this manner they would accrue fees, but take on none of the risk of spending those nomins, for they always have an instantaneous option to liquidate their position and escape. On the other hand, an actor who had done the economically-desirable thing and issued nomins to the market would be forced to buy them back before redeeming their escrowed havvens.

3.3.1 Non-discretionary Issuance

One possibility is to simply provide an issuer no control over the tokens they issue. That is, when a quantity of nomins is issued, they are generated by the system, which then places a sell order at the current going rate for that quantity on an exchange on the behalf of the issuer. When the order is filled, the proceeds in ether are remitted to the issuer.

Conversely, when a quantity of nomins is burned, they must first be obtained from the open market. In this way, a user would indicate an intention to burn, providing sufficient value to buy the proposed quantity of nomins, and the system would bid for that quantity on their behalf, thereby liquidating the user's havven position once the nomins have been obtained.

So one might consider there to be a formal distinction between wallets that issue tokens and those that do not. In this vein, one might envisage an extra fee to be charged to directly transfer nomins (rather than buying from the market) into a wallet that has an outstanding quantity of nomins it has previously issued, but not burnt. The result of this is that it would be less reasonable for an agent to sit on nomins in order to burn them in future as it is more advantageous in times of relative stability to simply buy them from the market.

3.4 Price discovery

One of the key challenges with denominating a cryptocurrency in a fiat currency is the fundamental link this creates to the centralised world. When the denominating currency exists external to the blockchain ecosystem, some bridge must be built so that the system can act with knowledge of external information. We recognise that a decentralised price-finding mechanism would be our preferred approach. Research into this mechanism is on our horizon, and future versions of this white paper will contain our results. However, in order to reclaim system performance, we can trade some of the trustlessness of the design, for example by a trusted "Oracle" service, which transmits knowledge of the external world into the system, building a causal link.

3.5 Utilisation Ratio

Even though rational actor modelling suggests that the price of nomins and havvens will equilibrilate given that an agent may pay up to some multiple of the market value of a nomin in order to release escrowed havvens, we are aware that there may be some prevailing macroeconomic or psychological influences relating to an undercollateralised position (i.e. if the value of the collateral pool is less than the issued stablecoin). As such, our modelling incorporates the notion of a "utilisation ratio" $0 < U < 1$, such that the system is over-collateralised in an attempt to counteract these potential issues. It may be that resolving an optimised utilisation ratio is beyond the ability of our agent-based modelling to determine, and as such, selecting this may need to be informed by the activity of a live system. Thus it is currently intended for Havven to initially include in its governance model the power to correct the utilisation ratio. This power can be removed over time as the system is proven, perhaps directly linked to some parametric milestones such as nomin velocity and stability.

4 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.

4.1 Definitions

We first introduce the core system variables:

$$H := \text{havven quantity} \qquad N := \text{nomin quantity}$$
$$P_h := \text{havven price} \qquad P_n := \text{nomin price}$$

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:

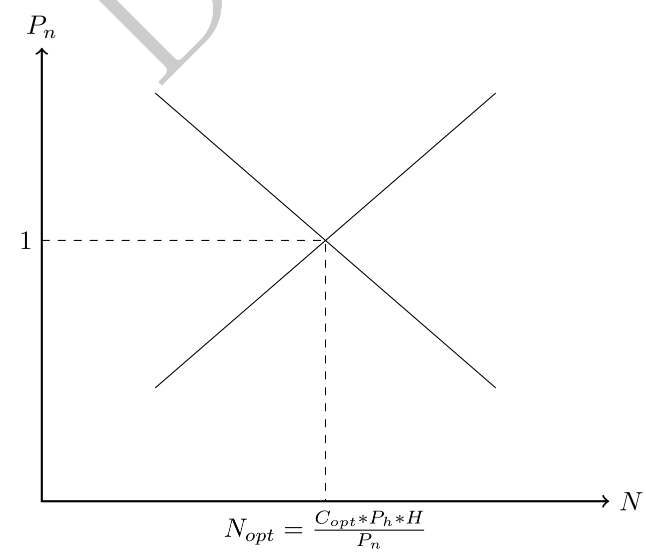
$$C = \frac{P_n * N}{P_h * H}$$

4.2 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.

curved lines

make diagrams pretty



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.

4.3 Issuance and Collateralisation

separate wallets from accounts

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.

Make sure this equity/debt language is not too security-like.

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.

4.3.1 Issuance Example (Diagrams to come?)

Finish the example. I don't really know if dealing with nomin price changes here is right, before introducing fees.

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. The number of nomins issued is:
$$5 = \frac{1 \cdot \check{N}_i}{10 \cdot 0.5}$$
$$\check{N}_i = 25$$
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:
$$C_i = \frac{1 \cdot 25}{10 \cdot 10}$$
$$C_i = 0.25$$
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}. (This confuses me because effectively he's getting a higher fee rate ??)
6. 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.
7. Bob now decides he would like to escrow the remainder of his havvens to issue more nomins.
8. He escrows the last 5 and generates 25 more nomins. His C_i is now 0.5.
9. P_h drops again to \$7 and the value of his Havvens decreases to \$70. Now his C_i has increased to 0.71 which is greater than C_{opt}. The system needs to incentivise Bob to lower his C_i such that it is below C_{opt}.

4.4 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.

4.4.1 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.

$$a_c = k.$$

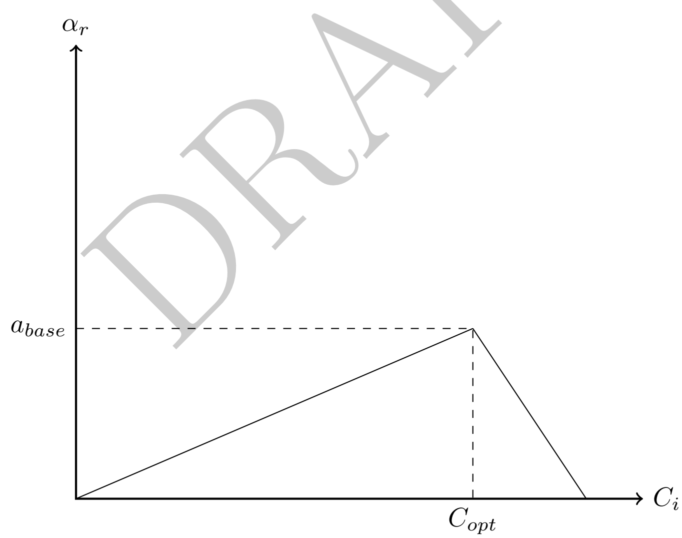
4.4.2 Fees received by Havven Holders

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.

figure out whether t stays

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

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



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

4.4.3 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:

figure out whether t stays

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

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

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

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.

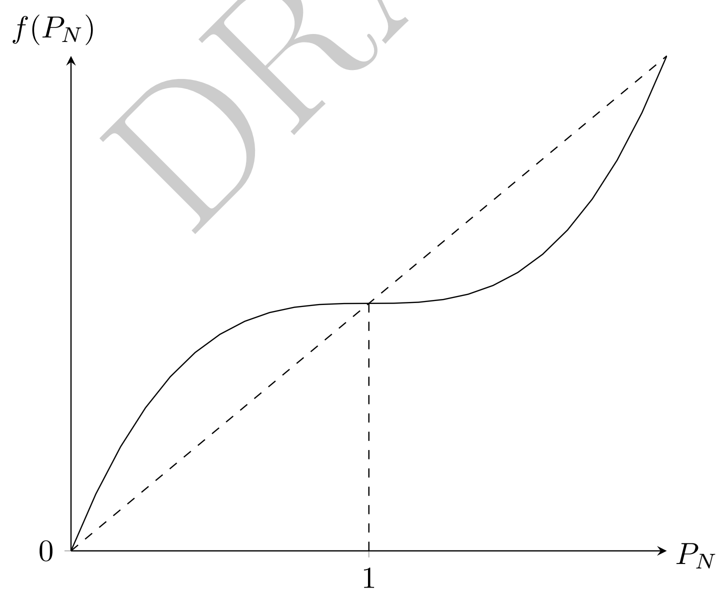
4.5 Collaterilisation Ratio

4.5.1 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}.

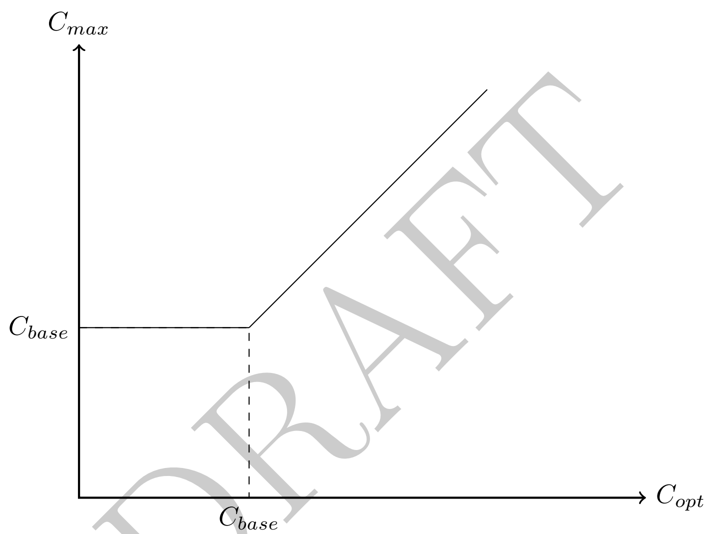
$$C_{opt} = f(P_n) * C,$$
$$f(P_N) = max(\sigma * (x-1)^{\phi} + 1, 0),$$
$$\text{where } 0 \leq \sigma, \text{ the price sensitivity parameter},$$
$$\phi \geq 1, \text{ the flattening parameter}.$$



4.5.2 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}.

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



4.6 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.

5 Quantitative System Analysis

We take the view that falsification is an important aspect of validating the Havven system. In our quantitative analysis we seek to identify failure modes of the system, and also to characterise not just *whether* Havven stabilises nomin prices, but *how much* it does.

5.1 Game-theoretic modelling

Discuss the structure of the game Havven represents, incorporating information the economists produce.

Discuss game theoretic modelling.

5.1.1 Actor Definitions

Havven Holder *An investor who owns* HAV *tokens.*

In order to purchase HAV the expected return has to be greater than that of alternative investments (opportunity cost). The expected return of HAV comes from:

1. The fees received on escrowed HAV.
2. An increase in P_h.
3. Seigniorage (i.e., an increment in P_h implies that the investor can issue more NOM, which may eventually have a larger value than his original investment.

At any moment in time, the investor must decide:

1. Whether or not to issue new NOM (assuming $U_i < U_{max}$), or to burn some of them. All NOM are issued/burnt at the prevailing market exchange rate, denominated in ETH.
2. Whether to sell some quantity of HAV in the market at price $P^M_{h,t}$. Only HAV which haven't been escrowed can be sold. Otherwise they must burn NOM to release them.

Nomin User *A person who uses the* NOM *token.*

In order to purchase NOM, it must provide the user more utility than USD, since both have the same consumption value in the market. This utility may come from the properties of crypto.

At any time, they must decide:

1. Whether to buy or to sell NOM at P_n.

Agent-based modelling It has been observed that analytic methods are often difficult to apply in the complex and dynamic setting of a market. One suggested solution to this problem is *agent-based modelling*. Under this paradigm, we proceed by first defining rational agent behaviour and then simulating the interplay of those strategies over time. We seek to develop a more effective method of characterising market behaviour and equilibrium prices than pure analytic reasoning.[?]

Such simulations also provide an immediate means of measuring quantities of interest. Simply by observing the model, we can discover how varying input parameters affect system outputs in an experimental fashion. One important corollary is that this is a way of extracting reasonable settings for system parameters (such as fee levels) that might be difficult to reason about *a priori*. These systems, reactive as they are, also provide a method for testing proposed remedies for any identified failure modes.

Discuss that the game theory conclusions can be simulated

In sum, then, the modelling seeks to answer the following, among other questions:

- Does the system stabilise its nomin price?
- Under what conditions can stability fail?
- What are reasonable initial settings for fees and other parameters?
- What effect does the utilisation ratio have on havven/nomin price ratio?
- What is an effective utilisation ratio?
- What is the effect of a direct redemption regime?
- What are the expected returns for havven-holders?

Fuller description of the technicals of the modelling.

Please visit `research.havven.io` for a pre-alpha version of our model.

5.2 Fee/velocity/return computations

Fee/velocity/return computations

6 Qualitative System Analysis

This section provides a qualitative treatment of the reaction of the Havven system in response to various scenarios listed below:

Scenario analysis.

6.1 Incentives

Why would anyone use nomins?

- Versus havvens?
- Versus alternatives?

Why would anyone issue nomins?

- Fees
- Because they thought the peg would break in the positive direction.

6.2 Scenarios

6.2.1 Havvens appreciate against nomins.

- Havven-holders can issue more nomins.

  This might be scary because we either want the nomin supply to fall, or nomin demand to increase. This is fine if the nomin price fell, because then nomin demand should increase. However, if it was simply that the havven price increased, then this might encourage oversupply of nomins as issuers compete for shares of the fee pool.

- Cheaper exit

  Anyone who has previously issued havvens but who wants to exit can buy nomins for cheaper than they issued them at, so egress with a profit. Alternatively, if the havven price doubles, then only half of their stake is required to back the nomins they have issued. They can use these proceeds to completely liquidate their position.

- Each nomin locks fewer havvens.

6.2.2 Havvens depreciate against nomins.

- Havven-holders can issue fewer nomins.

  Perhaps they may even be under-staked.

- Each nomin locks more havvens.

- A player can issue a quantity of nomins and sell them for havvens.

  They would do this on the assumption that, once the nomin price decreases as a result of the increased supply, they will be able to buy back the same quantity of nomins to free up their havvens more cheaply.

6.2.3 Nomin/havven liquidity dries up

- Low nomin supply

  Nomins should appreciate against the havven. See §6.2.2. Fee takings will decrease, hurting havven-holders in the long run, which should incentivise them to inject nomins into the ecosystem.

- Low havven supply

  If system backers are sitting on a pile of havvens, then the havven should appreciate. See sections 6.2.1 and 6.2.4.

6.2.4 Long-run havven price appreciation

Long-run havven appreciation scenario.

In this instance, over the long run, the price of havvens could appreciate quite substantially, which will lead to an increase in nomin issuance rights (and so probably actual nomins in circulation). There are at least two reasons that havvens could appreciate:

- Increased nomin velocity/demand, leading to greater fees; This is fine: in this case, nomin issuance rights increase in proportion with demand for the currency.

- Speculation This is not so fine: in this case, the nomin supply can be expanded without any accompanying expansion in its demand, which will depress the nomin price.

  Resolve disconnect between speculation-driven value of havvens and nomin supply.

6.2.5 Long-run havven price depreciation

Long-run havven depreciation scenario.

6.2.6 Radical shifts in usage

Usage-shift scenario.

6.3 Expected Market Players

List expected players in the market.

Outline incentives and actions for different players.

- Havven Holders

  A havven-holder provides collateral and liquidity. It's assumed havven-holders seek fee revenues, escrowing as many havvens as they can. This incentive only really makes sense if havvens are not significantly volatile over the long run. But in an unstable regime we also provide incentives for stabilising the nomin price.

- Nomin Users

  Merchants, consumers, service providers, and so on: people who use the stable coin as a medium of exchange. They provide a base demand for nomins, which is necessary for fees to exist. These users may be disincentivised from using the system by excessive volatility in the price of nomins, or by high fees.

- Arbitrageurs, Market Makers

  The arbitrage force allows us to assume that the cur/nom, cur/fiat, nom/fiat prices are properly in alignment or will soon become aligned. Market making activities allow us to neglect the bid/ask spread, and situations where there is insufficient liquidity for players to transact.

- Speculators

  May tend to magnify price corrections, and are a significant vector by which to introduce exogenous shocks to the system modelling, e.g. large capital flows in response to breaking news.

- Malicious Attackers

  We should examine what happens if a George Soros (or otherwise) attacks Havven.

  List the various possible attacks against the system.

- Central Banker

  The Havven foundation will have significant capital reserves with which it could intervene in the market if necessary to stabilise nomin prices. The system should work without such actions, but in extreme situations it might be necessary to undertake them. The advantage of such a market participant is, given that a very large market entity is willing to underwrite the stability of the coin, profit strategies predicated upon the stability of the token become less risky, so more feasible. So the Havven foundation in this capacity takes on the role of providing confidence.

Appendices

A Alternative approaches

Establish a summary of arguments against each competitor

A.1 Basecoin

Description of system Basecoin is described as operating similarly to Havven in that there is separation between a backing token and a transactional token, however Basecoin also separates out a specific "bond" token. The peg to an arbitrary external asset is maintained by using an oracle service to discover the price on an external market, before regulating the supply of "basecoins" through actively increasing (issuing new basecoin), and decreasing (auctioning of bonds) the supply, effectively acting as an autonomous central bank.

A.1.1 Key issues

Basecoin is intended to operate "as a decentralized, protocol-enforced algorithm, without the need for direct human judgment (sic). For this reason, Basecoin can be understood as implementing an algorithmic central bank." Whilst not without merit, this approach was discarded by Havven due to the high degree of design complexity required to be anticipated in order to ensure the stabilisation mechanism is effective. The paper states that Monte Carlo simulations have been run which indicate stability under a range of scenarios, however details are yet to be released by the team.

Another element not explored in the Basecoin whitepaper is the incentives for participants to engage with the cryptoeconomic system itself. While there is no argument against the utility of stablecoins, there must be incentives inherent in all such systems to ensure the appropriate participation of all actors. In this case, there are consumers of the stablecoin and active participants in the monetary policy. It is critical to be able to demonstrate that the incentives within the system will ensure profitable participation strategies for actors. Without this being clarified it is unclear as to whether there will be uptake by enough users to generate sufficient currency in circulation to support the demand for a stablecoin. Critically, the removal of Basecoin from the system to ensure the stable peg is predicated on the significant assumption that participants will take positions in the ongoing bond auctions. This assumption remains untested.

A final point needs to be made with respect to the overarching monetary approach espoused in the whitepaper. In the section "Averting Macroeconomic Depressions" the authors appear to support money printing and inflationary policies and the subsequent devaluation of currency. Even were it possible to demonstrate that inflation of the money supply via such a system would be effective in combating a deflationary spiral, a far better argument could be made that simply by implementing a stable store of value and unit of account that such a system would not be required. Generally, the apparent assumption that such a system would be achievable and still able to handle monetary crises in a far future time without centralised intervention stretches credulity. It's not entirely clear why Basecoin has intended to merely replicate the function of a central bank, rather than aim for pure stability or a relative-stable approach such as Havven. We are skeptical of any group that would advocate for monetary approaches that are diametrically opposed to cryptoeconomic efforts to democratise money, and we feel that the proposal to intentionally create a systematically inflationary monetary system is not the answer. Instead, we should at this point in time be aiming to construct a system that provides a stable store of value relative to an arbitrary fiat currency. The macroeconomic benefits of such a system are clear, and for as long as we live in a fiat-dominated world this will continue to be the case.

A.2 Tether

Description of system Tether accepts fiat deposits into the Hong Kong-based Tether Limited bank account and issues "USDT" (USD Tether) over Bitcoin via the Omni Layer protocol. Tethers are an asset-backed digital token, representing a claim on the cash held in reserve.

The stability of the USDT 'coin' effectively relies on the force of external market arbitrage to ensure the peg holds over time.

Key issues Despite the whitepaper claiming that the "goal of any successful cryptocurrency is to completely eliminate the requirement for trust," and that each Tether is "fully redeemable/exchangeable any time for the underlying fiat currency," the company's terms of service quite clearly state that "there is no contractual right or other right or legal claim against us to redeem or exchange your Tethers for money."

Tether clearly relies on a manual, centralised proof of existence for the backing asset, and so suffers from the very issue that the Tether whitepaper decries. Indeed the same issue is encountered with tokenised gold, or similarly any other real-world asset where some Oracle bridge is required to interface into a distributed ledger.

Current state Recently, Tether announced support for issuing ERC-20 compatible tokens on Ethereum as opposed to releasing "tethers" on the Bitcoin blockchain using the Omni Layer protocol.

At the time of writing, the market capitalisation for USDT was approximately $440m, and the discrepancy regarding their terms of service remains unresolved.

A.3 MakerDAO

Description of system MakerDAO allows users to escrow collateral to generate a stablecoin, known as the Dai, similar to Havvens escrow system. However, in Havven the collateral is derived from the system itself, whereas in MakerDAO any ERC20 token can be used to generate Dai. The tokens are locked into a smart contract known as a collateralised debt position (CDP). CDPs have multiple risk parameters which are set by the holders of the MKR token. In this way, governance is not directly linked to the capital that backs the Dai.

A.3.1 Key issues

Allowing the system to be collateralised by a range of ERC20 tokens introduces significant complexity because the system must react to changes in many types of collateral. MKR token holders vote to set the risk parameters of each type of collateral. This raises the question, how can the market be confident that the Maker holders are capable of deciding these values correctly? The system incentivises the holders to vote responsibly, but this does not provide confidence that the MKR holders possess the required knowledge.

The collateral in a CDP is always some form of ERC20 token, initially only Eth. This means MakerDAO can never eliminate the systematic risk of the price of Eth and the other ERC20 tokens are used in CDPs. We acknowledge that this approach makes the system less susceptible to price shocks initially.

Current state

A.4 Nubits

Description of system

Key issues

Current state

Makerdao critique.

B System variables

More complete system variable section.

What follows are the main variables of the system. Under each heading, each row will correspond to a single quantity of interest. Each row will have three columns. Leftmost, a mathematical definition of the variable; in the middle, the dimension of the quantity (which units it is measured in); and on the rightmost, a short English summary of the variable.

Certain abbreviations will be used. For example, HAV and NOM will be used as abbreviations for havvens and nomins considered as units of measurement.

Prices

P_h	$(\frac{\$}{\text{HAV}})$	: havven price.
P_n	$(\frac{\$}{\text{NOM}})$	: nomin price.
$\pi := \frac{P_h}{P_n}$	$(\frac{\text{NOM}}{\text{HAV}})$	: havven to nomin conversion factor.
$P_h' = f(V_n, V_h) \cdot R$	$(\frac{\$}{\text{NOM} \cdot \text{sec}})$	: havven price rate of change.

Here R is a risk term incorporating, for example, volatility, number of buyers versus sellers, and so on.

Money Supply

H	(HAV)	: Quantity of havvens, which is constant.
H_e	(HAV)	: Quantity of escrowed havvens.
$N = H_N \cdot \pi$	(NOM)	: Quantity of nomins. This can float.
$H_N = \frac{N}{\pi}$	(HAV)	: Havven value of issued nomins.

Ideally, $H_N \leq H_e$.

Utilisation Ratios

$U = \frac{H_N}{H}$	(dimensionless)	: Empirical issuance ratio.
U_{max}	(dimensionless)	: Targeted issuance ratio ceiling.

$0 \leq U \leq U_{max} \leq 1$

Microeconomic Variables These should be defined as functions of $P_n,\ P_v,$ fees, etc.

S_n	$(\frac{1}{\text{sec}})$	: average nomin spend rate
S_i	$(\frac{1}{\text{sec}})$	: average issuance rate
S_r	$(\frac{1}{\text{sec}})$	: average redemption rate

Money Movement

$V_n = S_n \cdot N$	$(\frac{\text{NOM}}{\text{sec}})$	: nomin transfer rate.
$V_v = V_i + V_r$	$(\frac{\text{HAV}}{\text{sec}})$	: nomin $\leftrightarrow$ havven conversion rate.
$V_i = (C - C_N) \cdot S_i$	$(\frac{\text{HAV}}{\text{sec}})$	: nomin issuance rate.
$V_r = C_N \cdot S_r$	$(\frac{\text{HAV}}{\text{sec}})$	: havven redemption rate.

V_i is assumed to grow as there are more free havvens in the system.

V_r, by contrast, is taken to grow proportionally with the number of escrowed havvens.

Fees

The following fees are ratios, for example 0.1%, levied on each transaction.

F_{nx}	(dimensionless)	: nomin transfer fee
F_{cx}	(dimensionless)	: havven transfer fee
F_i	(dimensionless)	: nomin issuance fee
F_r	(dimensionless)	: havven redemption fee