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 potential 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

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. As payment technology has advanced in recent years, it has become increasingly invisible and it is often lost upon users of money that, like any technology, it can be improved. Specifically, this means improving the performance of those 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 these functions 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.

The interested reader can also find additional discussion of stablecoins, cryptoeconomics, competitors, and other related topics on our blog at `http://blog.havven.io`.

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 able 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 Design Rationale

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 price changes exogenously, then the system is designed to provide incentives for actors to recalibrate to the new price.

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 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, for example prediction markets and insurance contracts. 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. Users of the nomin token pay the owners of the havven token for collateralising and stabilising the system.

The havven token incentivises those who hold it to serve two functions:

- To provide the system with collateral.
- To participate in the stabilisation of 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 automated collateral recovery. Where a significant portion of nomins are being used for hedging, (and hence not generating transaction fees) a charge can be applied to ensure that the cost of utility for hedging is not being solely borne by transactions.

2.1 Equilibrium Nomin Price

We first introduce the core system variables:

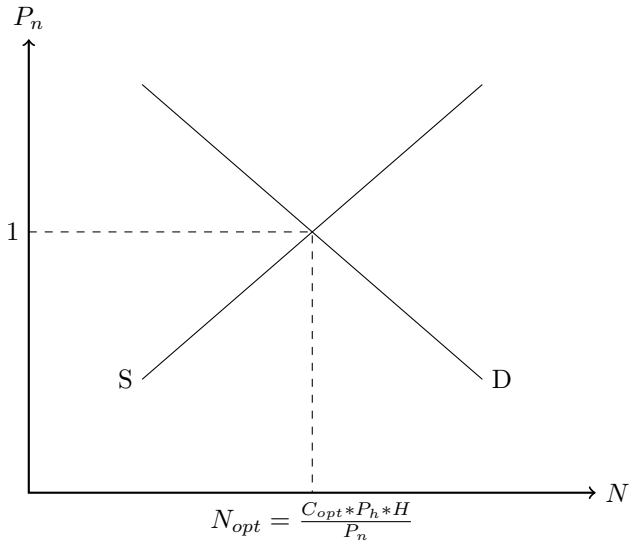
$$H := \text{havven quantity} \qquad N := \text{nomin quantity}$$
$$P_h := \text{havven price} \qquad P_n := \text{nomin price}$$

All havven tokens are created at initialisation, 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. As we proceed, we may subscript variables with t to indicate the value of that variable at a given time.

In Havven, the measure of the value of nomins against the value of havvens is called the collateralisation ratio:

$$C = \frac{P_n * N}{P_h * H} \tag{1}$$

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 equilibrium below with a hypothetical demand curve, D, and a supply curve, S.



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.

2.2 Intrinsic Havven Value

Being freely-tradable ERC20 tokens, havvens will have a market price which, like the nomin price, can be measured by an oracle. In the initial phases, while nomin demand is low, we will use the market price. However, once nomin transaction volume has increased to sufficient levels, we may transition to a different havven-valuation system that attempts to more directly connect the valuation of the havven with demand for nomins.

One problem with using the market price for P_h is that would it exposes the collateralisation ratio computation to speculative price shocks. Instead, the "true" price of a havven is computed as a function of the transaction fees that the system charges. In this way we connect the computed price of the havven directly with nomin velocity. Price increases will allow an expansion in the money supply exactly when demand has expanded, while contractions in the money supply will be incentivised exactly when demand has contracted.

We define the value of a havven as a share in the discounted sum over past fee returns. In this way the price is not vulnerable to instantaneous volume spikes, while taking the most recent transaction volumes to be the most highly-correlated with future volumes.

$$P_{h,t} = \frac{1}{H} \sum_{t'=1}^{t} \frac{F_{t-t'}}{(1+r)^{t'}} \tag{2}$$

where

$P_{h,t}$ is the price of one havven at time t
F_t is the total fees collected in period t
r is a falloff term

This can be computed efficiently, because $P_{h,t+1} = \frac{P_{h,t}+F_t}{r}$. Further, if it is assumed that the average fee take is approximated by F_t, and t is large, then

$$P_{h,t} \approx \frac{1}{H} \sum_{t'=1}^{\infty} \frac{F_t}{(1+r)^{t'}} = \frac{F_t}{H \cdot r} \tag{3}$$

2.3 Issuance and Collateralisation

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

$$0 < C_{opt} < 1 \tag{4}$$

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

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

$$C_i = \frac{P_n \cdot \check{N}_i}{P_h \cdot H_i} \tag{5}$$

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:

$$\check{H}_i = \frac{P_n \cdot \check{N}_i}{P_h \cdot C_{max}} \tag{6}$$

Under equilibrium conditions, there is some $\check{H}_i \leq H_i$ when $C_i = C_{opt}$, which the issuer is incentivised to target. These incentives are provided in the form of transaction fees, discussed in section 2.4. It is important to note that the issuer may voluntarily increase their C_i up to the limit of C_{max}; for example if they anticipate a positive movement in C_{opt}. C_i may never exceed C_{max}, except by price fluctuations, and in such circumstances, issuers are rewarded for bringing C_i back under C_{max}.

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.

Nomin 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. This is a main way an issuer can reduce their collateralisation ratio. If an issuer does not possess the required nomins, they can be purchased on the open market.

2.3.1 Issuance Example

1. Bob purchases 100 havvens at \$1 each, total value \$100. The maximum collateralisation ratio C_{max} is 0.5, the optimum collateralisation ratio C_{opt} is 0.4 and the nomin price P_n is \$1.

2. Bob decides to issue nomins up to C_{opt}. By equation (6), the system generates 40 nomins and escrows 80 of his havvens, locking \$80 worth of value in the system ($\check{N}_i \cdot C_{max}$).

3. The system sells the nomins on the market for \$40 worth of ether, transferring it to his account.

4. The havven price drops to \$0.90. The value of his havvens has decreased to \$90 which means his C_i has increased to 0.44, greater than C_{opt}. The system escrows more of Bob's havvens to maintain the value of the locked collateral.

5. By (6) the system escrows an extra 8.9 of his havvens. He now has 88.9 havvens escrowed. The value locked in the system remains unchanged at \$80.

6. The havven price then increases back to \$1. The value of his havvens has increased to \$100 and his C_i has decreased back to 0.4. The system releases the 8.9 havvens back to Bob and he has 80 escrowed.

The above example has illustrated how the system maintains the value of the underlying collateral by adjusting the quantity of a user's escrowed havvens as the havven price changes.

2.4 Transaction Fees

Havven needs a direct incentive mechanism that can correct changes in the global collaterisation ratio, C, when the price of havvens or nomins changes.

Some of the equations below are defined in the discrete time domain and are referenced with a subscript t. These will be specifically used in our game theoretic modelling.

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.

$$\alpha_c = k \tag{7}$$

We may then express the total fees collected in period t, F_t, as a function of the velocity of nomins v_t and the total nomin supply N_t:

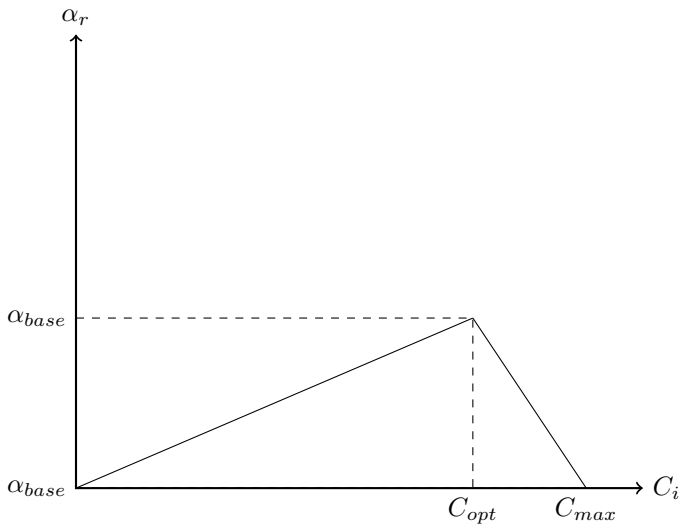
$$F_t = v_t \cdot \alpha_c \cdot N_t \tag{8}$$

2.4.2 Fees Received by Havven Holders

The fee rate paid to a havven holder that has escrowed is α_r. The actual fee they receive is $\check{H}_i \cdot \alpha_r$, being proportional with the value they stake. The received fee rate changes with respect their unique collaterilisation ratio, C_i. It increases linearly to a maximum α_{base} at the optimal collaterilisation ratio C_{opt}, before quickly diminishing as C_i approaches the maximum collaterisation ratio C_{max}. This function is designed to encourage havven holders to constantly target the optimal collateralisation ratio, by rewarding them with greater fees if they do so.

$$\alpha_{r,t,i} = \alpha_{base,t} \cdot \mathcal{F}_{i,t}(C_{i,t}, C_{opt}, C_{max,t}) \tag{9}$$

$$\mathcal{F}_{i,t}(C_{i,t}, C_{opt,t}, C_{max,t}) = \begin{cases} \frac{C_{i,t}}{C_{opt,t}} & \text{when } C_{i,t} \leq C_{opt,t} \\ \frac{C_{max,t} - C_{i,t}}{C_{max,t} - C_{opt,t}} & \text{when } C_{opt,t} \leq C_{i,t} \leq C_{max,t} \\ 0 & \text{otherwise} \end{cases} \tag{10}$$



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

2.4.3 Base Fee Rate

Let us define the total fees paid to havven holders $F_{r,t}$:

$$F_{r,t} = \sum_i \check{H}_i \cdot \alpha_{r,t,i} \tag{11}$$

Havven requires that the total fees collected from users has to be equal to the total amount of fees paid to the havven holders, so that $F_{r,t} = F_t$. Substituting our earlier definition (9) for $\alpha_{r,t,i}$ and solving for $\alpha_{base,t}$:

$$\alpha_{base,t} = \frac{F_t}{\sum_i \check{H}_i \cdot \mathcal{F}_{i,t}(C_{i,t}, C_{opt,t}, C_{max,t})} \tag{12}$$

We have now defined the maximum fee rate, α_{base}, in terms of the fees collected, F_t. This rate should be achieved when an individual's C_i is at C_{opt}.

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

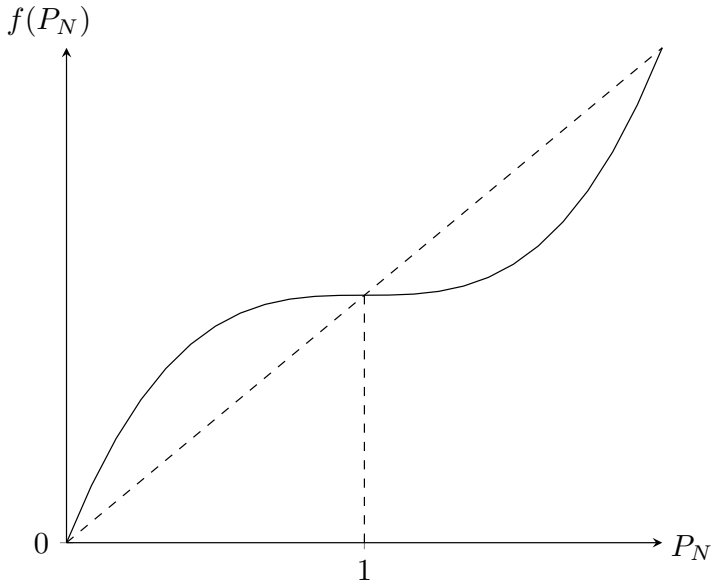
2.5 Collateralisation Ratio

2.5.1 Optimal Collateralisation 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}.

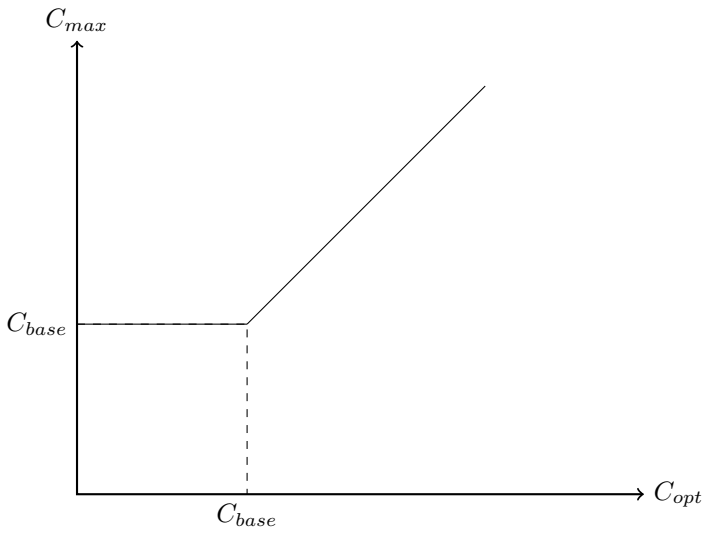
$$\begin{aligned} C_{opt,t} &= f(P_{n,t}) * C_t \\ f(P_{N,t}) &= max(\sigma * (P_{N,t} - 1)^{\phi} + 1, 0) \\ 0 &\leq \sigma, \text{ the price sensitivity parameter} \\ \phi &\geq 1, \text{ the flattening parameter} \end{aligned} \tag{13}$$



2.5.2 Maximum Collateralisation 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}.

$$C_{max,t} = \begin{cases} C_{base,t} & \text{when } C_{opt,t} \leq C_{base,t} \\ a * C_{opt,t} & \text{otherwise.} \end{cases} \tag{14}$$



2.6 Fee Evasion

Being based on Ethereum, Havven is potentially vulnerable to its tokens being wrapped in another smart contract. These wrapped tokens could then be exchanged without incurring fees. We consider this unlikely for a number of reasons. First, the fees are designed to be low enough that most users will not notice them. Second, network effect is tremendously important for currencies; in order to become useful, these tokens must first be accepted as a legitimate currency by vendors. To this end, we do not believe that token wrappers of this kind will be credible, not having been tested or audited, while its authors may also lack credibility.

Nevertheless, it is simple to implement a democratic method, weighted by havven balance, by which havven holders could freeze the assets of any contract that wraps assets. Those havven holders are incentivised not to abuse this system for the same reason that bitcoin mining pools do not form cartels to double-spend: because abuse of this power would undermine the value of the system, and thus devalue their own holdings.

The credible threat of such a system existing is enough to discourage wrapper tokens from being used, even if they are written, since any user who does so risks the balance in the wrapper being confiscated or frozen, so that they could not then unwrap those tokens to retrieve the nomins they wrapped.

3 System Analysis

While the Havven mechanism feels intuitively viable and we have strong confidence in it, we take the view that falsification is vital in validating our proposal. The more stands up to attack, the more we can trust to its ultimate validity.

Ultimately this must done empirically, but it is also important to model Havven extensively before launching it. Therefore in our quantitative analysis we seek above all to identify its failure modes, and also to characterise its stability under a range of conditions.

In our quantitative analysis, we take three distinct approaches in modelling the system:

Analytical

By expressing our system in the language of game theory and microeconomics, we seek to gain insight into Havven's incentive structure and the resulting price equilibria. Examining the problem from this direction can lead us to concise and mathematically robust conclusions.

Simulationist

We implement a broad range of strategies as AI agents, and examine how the market responds under different initial conditions, with different constituent populations, and in response to external shocks. This approach allows us to examine situations which are analytically intractable.

Empirical

Initial releases of Havven will be invaluable in checking our assumptions. Observation of real market behaviour will allow us to better understand how the it responds in different situations, and therefore how to choose appropriate values for system variables.

The results of these investigations will be published as they are completed.

3.1 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, and are a platform to simulate the conclusions of any antecedent game-theoretic reasoning.

3.2 Expected Market Players

Here we outline some of the players anticipated in the market. These represent only some of the agents that our modelling and simulations are predicated upon.

Havven Holders

A havven-holder provides the collateral and liquidity for the system. It is assumed that havven holders primarily seek fee revenues, and escrow most of their havvens, adjusting their issuance to track Havven's moving fee incentives. While these incentives make sense if havvens are relatively stable in the long term, Havven will also provide incentives for correcting the nomin price in in the short term. Returns for these actors are primarily realised in fees, seignorage, and the appreciation of havvens resulting from their constrained supply.

Nomin Users

These are the market participants who will make up the base demand for any stablecoin, chasing its superior utility as a medium of exchange or as as means of hedging against other forms of value. The users of nomins may include merchants, consumers, service providers, cryptocurrency market actors such as exchanges.

The transaction volume these users provide is necessary for fees to exist. They may be disincentivised from using the system in low liquidity situations or with excessive volatility in the price of nomins.

Speculators

Speculators may tend to magnify price corrections, and are a significant vector by which to introduce exogenous shocks to the system. In our modelling we induce volatility by simulating modes of interest such as large capital flows in response to breaking news and the like.

Speculators also produce an important stabilisation force. When the market believes that the price is being stabilised, upward price shifts induce sell pressure, and downward price shifts induce buy pressure. This strategy is profitable on the assumption that the price will return to the equilibrium point. This neutral stabilisation force is a self-sustaining negative feedback loop which operates independently of other incentives; preliminary simulations and observations of other systems have verified the efficacy of this corrective pressure.

Buyer of Last Resort

While the system is designed to work without intervention, the Havven foundation will have capital reserves with which to intervene in the market to stabilise nomin prices in extreme situations.

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 and so more feasible. The Havven foundation in this capacity takes on the role of providing confidence.

Arbitrageurs and Market Makers

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

Please visit `http://research.havven.io` for an alpha version of our model, and `http://blog.havven.io` for further discussion of stablecoins and cryptoeconomics.