HAVEN

CRYP2NOVA

Archived copy · cryp2nova.com

HAVVEN

A decentralised payment network and stablecoin v0.8

Samuel Brooks, Anton Jurisevic, Michael Spain, Kain Warwick

Abstract

There is currently no decentralised currency useful for everyday economic purposes. We propose a peer-to-peer payment network and price-stable token that does not rely on a central authority to maintain trust. Prior to Bitcoin, attempts to create digital currencies were centralised, making them vulnerable to censorship and seizure. Bitcoin's consensus mechanism protected it from interference, but its fixed monetary policy induced extreme price volatility. Havven solves this by issuing tokens against a distributed collateral pool, which derives its value from fees levied on transactions. Growth in transaction volume thus increases the value of the collateral, allowing the token supply to expand to meet demand. The resulting system retains the best features of Bitcoin, while the introduction of price stability results in a superior form of money.

CRYP2NOVA

11:14, June 11, 2018

Archived copy · cryp2nova.com

Contents

1 Introduction **1**
- 1.1 Payment Networks . . . 1
- 1.2 Cryptocurrency . . . 1
- 1.3 Stablecoins . . . 2
- 1.4 Distributed Collateral . . . 2
- 1.5 Havven . . . 3

2 System Description **4**
- 2.1 Equilibrium Nomin Price . . . 5
- 2.2 Issuance and Collateralisation . . . 6
- 2.3 Collateralisation Ratio . . . 8
  - 2.3.1 Optimal Collateralisation Ratio . . . 8
  - 2.3.2 Maximum Collateralisation Ratio . . . 9
- 2.4 Transaction Fees . . . 10
  - 2.4.1 Fees Received by Havven Holders . . . 10
  - 2.4.2 Nomin Transaction Fees . . . 11
  - 2.4.3 Base Fee Rate . . . 11

3 System Analysis **12**
- 3.1 Nomin Demand and Havven Value . . . 12
- 3.2 Fee Evasion . . . 13
- 3.3 Issuance Case Study . . . 14
  - 3.3.1 Practical Issuance Dynamics . . . 15
  - 3.3.2 Optimality of Targeting C_{opt} . . . 18

Appendices **23**

A Road Map **23**
- A.1 Ether-Backed Nomins (`eUSD`) . . . 23
- A.2 Havven-Backed Nomins (`nUSD`) . . . 24
- A.3 Continuing Development . . . 25

B Modelling **26**
- B.1 Agent-Based Modelling . . . 27
- B.2 Expected Market Players . . . 27

CRYP2NOVA

Archived copy · cryp2nova.com

1 Introduction

1.1 Payment Networks

Payment networks are closed systems within which users can transfer value. Such systems include credit card networks, the SWIFT network, and PayPal. Proprietors of these networks possess absolute control over the value within the network, so any transaction conducted within them may be blocked or reversed at any time. Although this is ostensibly designed to protect users, it introduces systemic risk for all participants. If the network is compromised or its owners cease to behave benevolently, no party can trust that the value in their account is secure or accessible.

In a traditional payment network like American Express, participants trust that the fees charged are sufficient to service the expenses incurred. However, were this trust to disappear, merchants would refuse to participate. Thus, the value of the unit of account within this network is derived solely from a single entity and the trust that participants have in that entity. As a result, the viability of any centralised payment network depends on complete trust in a central authority.

Bitcoin solved these problems by ensuring that users have sole discretion over the money in their account by producing a trustless, permissionless payment network in which anyone could participate at will. Since users could enter and exit the system at any time without being exposed to the aforementioned risks, adoption was accelerated, and network effects were amplified. Programmable blockchains allow the logic of a payment network to be decentralised in a transparent way, enabling anyone to verify whether the network is solvent. This eliminates systemic risk and reduces the costs associated with centralised networks.

1.2 Cryptocurrency

The technology of money has three key functions: to act as a unit of account, a medium of exchange and a store of value. As payment technology has advanced in recent years, money has become increasingly invisible and it is often lost upon its users that, like any technology, it can be improved. Bitcoin and other cryptocurrencies represent an impressive technological advancement on existing forms of money because they deliver improved durability, portability, and divisibility. Further, they do so without requiring centralised control or sovereign enforcement from which to derive their value. Their fixed monetary policies have protected them from debasement and devaluation, allowing them to outperform other forms of money as a store of value. However, this has created the potential for short-run volatility as they lack mechanisms to dynamically adjust supply to changing demand. Bitcoin has thus tended to be a poor medium of exchange and an even worse unit of account. In order for a token to effectively act as money its purchasing power must remain stable against goods and services over the short to medium term.

Archived copy · cryp2nova.com

1.3 Stablecoins

Cryptocurrencies exhibit transaction immutability and censorship resistance, and in these ways are a better form of money; but their adoption has been hindered by the volatility inherent in their static monetary policies. Users cannot engage with such systems as a medium of exchange if the purchasing power fluctuates. Stability continues to be one of the most valuable yet elusive characteristics for the technology.

Stablecoins are cryptocurrencies designed for price stability. They should ideally be as effective at making payments as fiat currencies like the US Dollar, while retaining their other desirable properties. A decentralised payment network built on a stablecoin would be able to capture all the benefits of a permissionless system, while also eliminating volatility. One approach to achieving price stability is to produce a token whose price targets the value of a fiat currency. Targeting stability against fiat currencies obviates the need to respond to macroeconomic conditions, as the token then benefits from the stabilisation efforts of large institutions acting in fiat markets. Furthermore, if a token's price can be maintained at $1, then it can serve as an interface between fiat money and cryptocurrency. If such a stablecoin does not require an account in a traditional bank, then it can be effectively used for settlement and purchasing, without the centralisation and counterparty risk involved in fiat transactions. Thus it can be expected that by using stablecoins, exchanges that trade fiat for crypto will be able to rapidly reduce their transactional costs, reducing the barriers for new users to enter the market.

1.4 Distributed Collateral

Today's fiat money is not backed by an asset; its stability is derived from the authority of the governments which issue it. These governments require that tax obligations are denominated in the currencies they control, which are then used to fund active stabilisation efforts. However, with government control comes the risk of tyranny and debasement. Decentralised monetary systems don't have these powers, and so they must use collateral to provide confidence in the value of their tokens. A decentralised system cannot use collateral assets that exist outside the blockchain, as interfacing with these assets necessitates centralisation with the aforementioned failure modes. Meanwhile, cryptoasset prices have been dominated by speculative volatility. So whether a system uses real-world assets or cryptoassets to back a stable token, if the value of the collateral is uncorrelated with the demand for the token, then the system is vulnerable to external price shocks. Large corrections can destroy the value of collateral without any change in the demand for the token issued against it. Clearly then, in designing an asset-backed stablecoin it is important to select the collateral asset carefully, but no existing asset perfectly serves the purpose.

Archived copy · cryp2nova.com

1.5 Havven

Havven is a decentralised payment network where users transact directly in a price-stable cryptocurrency. Those who use the stablecoin pay fees to those who collateralise the network, compensating them for the risks of providing collateral and stability. Collateral providers control the money supply, and fees are distributed in proportion with each individual's stabilisation performance. Thus, Havven rewards suppliers of stability and charges those who demand it.

Havven implements two linked tokens to achieve this structure:

Nomin

The stablecoin, whose supply floats. Its price as measured in fiat currency should be stable. This token is useful insofar as it provides a superior medium of exchange. Thus in addition to price stability, Havven should encourage adequate nomin liquidity.

Havven

This token provides the collateral for the system and has a static supply. Its market capitalisation reflects the system's aggregate value. Ownership of havvens grants the right to issue a value of nomins proportional to the dollar value of havvens placed into escrow. If a user wishes to release their escrowed havvens, they must first present the system with the quantity of nomins previously issued[1].

The havven token is a novel decentralised asset, whose intrinsic value is derived from the fees generated in the network it collateralises. This enables a form of representative money in which there is no requirement for a physical asset, thus removing the problems of trust and custodianship. Issuance of nomins requires a greater value of havvens to be escrowed in the system, providing confidence that nomins can be redeemed for their face value even if the price of havvens falls. The system incentivises the issuance and destruction of nomins in response to changes in demand, but ultimately the intrinsic value of the havvens will reflect the required nomin supply. Backing a stablecoin in this way provides full transparency over how many tokens have been issued against the available collateral. This provides a solid basis for confidence in the solvency of the payment network built upon it.

Denominating the value of the nomin in an external fiat currency means that stability is relative only to that currency. Initially this currency will be the US dollar, and this is the target currency used throughout this paper, but in the future the system will support additional flavours of stablecoin that are denominated in other currencies.

[1] Following Bitcoin, the Havven system will appear in uppercase and singular; while the havven token will be lowercase and may be plural.

Archived copy · cryp2nova.com

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 fulfil two functions:

- To provide the system with collateral.
- To participate in the stabilisation of the nomin price.

Collateralisation

Confidence in the stability of the nomin begins with overcollateralisation, so that the value of escrowed havvens is greater than the value of nomins in circulation. 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.

Stabilisation Incentives

Havven rewards those that have issued nomins. These rewards are derived from transaction fees and are distributed in proportion with how effectively each issuer acts to maintain 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, for example 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.

Archived copy · cryp2nova.com

2.1 Equilibrium Nomin Price

We first introduce the core system variables:

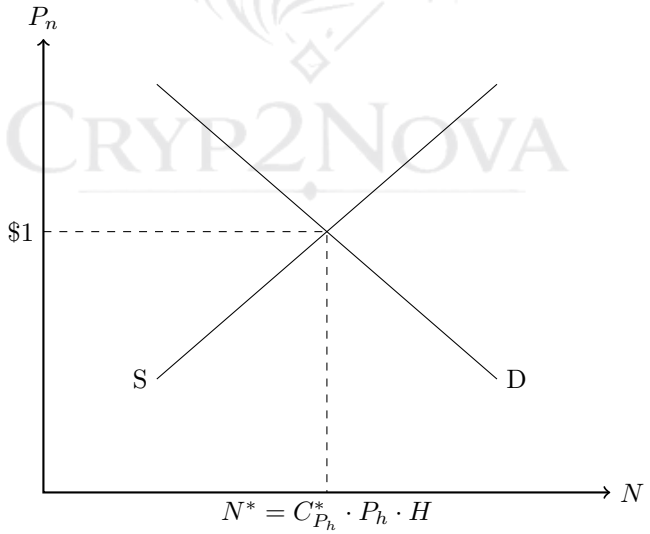
H	havven quantity	N	nomin quantity
P_h	havven price	P_n	nomin price

All havven tokens are created at initialisation, so H is constant. The quantity of nomins floats, responding to the issuance actions of havven holders. The Havven system needs to incentivise issuers 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. Any variable lacking such a subscript indicates the value of the quantity it represents at the current time.

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

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

From the law of supply and demand, at a given level of demand, there exists some supply of nomins N^* which yields an equilibrium price of \$1. This quantity is associated with an ideal collateralisation ratio at a particular havven price $C^*_{P_h}$ which is achieved when $N = N^*$. Therefore, when $C = C^*_{P_h}$, $P_n = \$1$. We visualise this equilibrium below with hypothetical demand and supply curves.



CRYP2NOVA

Archived copy · cryp2nova.com

We assume that some level of demand exists given the utility of nomins as a stable cryptocurrency. Although the organic supply and demand for nomins cannot be easily manipulated, all issuance is controlled by havven holders, whose 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 incentivise havven holders to manipulate N, and therefore C, in order to satisfy our requirement.

2.2 Issuance and Collateralisation

Havven's goal is to stabilise the nomin price while remaining overcollateralised. In order to do so, the system defines a collateralisation target:

$$0 < C_{opt} < 1 \tag{2}$$

C_{opt} is implicitly closer to $C^*_{P_h}$ than C is; when C approaches C_{opt}, it also approaches $C^*_{P_h}$.

It is necessary at this point to distinguish for an account i the nomins it contains N_i (equity) from the nomins it has issued $\check{N}_i$ (debt). Note that globally, $\sum_i N_i = \sum_i \check{N}_i$, as all 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:

$$C_i \;=\; \frac{P_n \cdot \check{N}_i}{P_h \cdot H_i} \tag{3}$$

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. As each C_i targets C_{opt}, the overall collateralisation ratio does also.

Nomin Issuance

The nomin issuance mechanism allows Havven to reach its collateralisation 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:

$$\check{H}_i \;=\; \frac{P_n \cdot \check{N}_i}{P_h \cdot C_{max}} \tag{4}$$

Under equilibrium conditions, there is some $\check{H}_i \leq H_i$ when C_i coincides with 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}.

Archived copy · cryp2nova.com

On the other hand, no one may issue a quantity of nomins that would lock more than H_i havvens. Consequently, 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. If we assume implementation on Ethereum, then the nomins are sold for an equivalent value in ether, with the proceeds of the sale remitted to the issuer.

Nomin Destruction

In order to access the havvens that have been escrowed, the system must destroy the same number of nomins that were originally issued. When the issuer indicates the intention to retrieve their havvens, the system places a **limit buy** order on a decentralised exchange, up to a maximum price of $1. The system places this order on behalf of the issuer and upon completion, the nomins are immediately destroyed.

CRYP2NOVA

Archived copy · cryp2nova.com

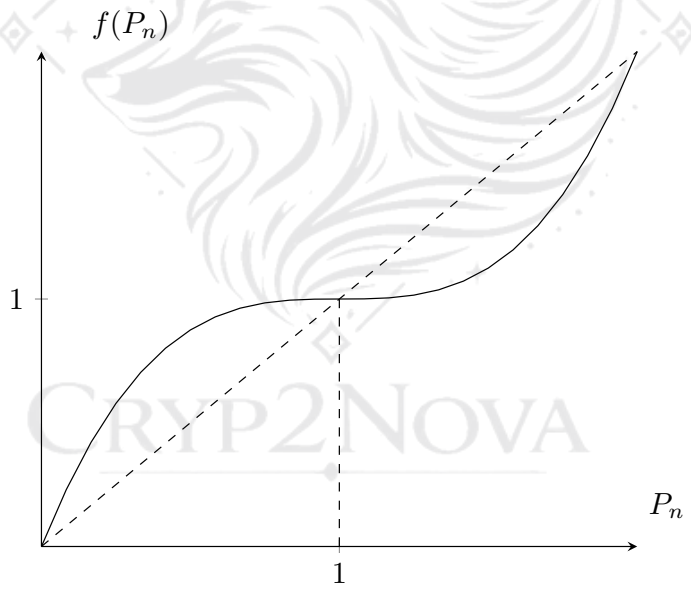
2.3 Collateralisation Ratio

2.3.1 Optimal Collateralisation Ratio

The optimal collateralisation ratio C_{opt} is a target for havven holders to reach which brings the global C closer to $C^*_{P_h}$. If havven holders target C_{opt} effectively, the amount of fees they receive is maximised.
C_{opt} is defined as a positive function of P_n, such that its value directly tracks changes in the nomin price; a havven holder wishing to maximise their fees will target C_{opt} by issuing or destroying nomins to manipulate their individual C_i.

The function for C_{opt} given below provides our dynamic target for havven holders based on the price of nomins:

$$\begin{aligned} C_{opt} &= f(P_n) \cdot C \\ f(P_n) &= \max(\sigma \cdot (P_n - 1)^{\psi} + 1, 0) \\ \sigma &\quad \text{price sensitivity parameter } (\sigma > 0) \\ \psi &\quad \text{flattening parameter } (\psi \in \mathbb{N},\ \psi \nmid 2) \end{aligned} \tag{5}$$



When P_n is at \$1, no signal is available to suggest that the global nomin supply is incorrect. In this case $C_{opt} = C$ and no incentive exists to move away from current collateralisation levels. However, if $P_n < \$1$, nomin supply outstrips demand; then $C_{opt} < C$, which encourages issuers to burn nomins, thereby raising the price. This movement of C_{opt} reflects the fact that $C^*_{P_h} < C$ under these circumstances. The $P_n > \$1$ case is symmetric.

Archived copy · cryp2nova.com

Notice that when the P_n is close to \$1, $f'(P_n)$ is small, so that Havven does not overshoot the correct nomin supply. However, the further it diverges from \$1, the larger the slope becomes, providing a stronger fee incentive for a havven holder to move toward C_{opt}.

2.3.2 Maximum Collateralisation Ratio

Havven seeks to maintain $C \leq C_{opt} < C_{max} < 1$, in order to retain sufficient havven collateral. It might seem intuitive that C_{max} should be a static value. However, since C_{opt} varies linearly with P_n and inversely with P_h, there are situations where C_{max} may need to change. We allow that a user may wish to set their $C_i > C_{max}$, but constrain by how much they may do so.
Below we define C_{max} in terms of C_{opt}.

$$\begin{aligned} C_{max} &= a \cdot C_{opt} \\ a &\geq 1 \end{aligned} \tag{6}$$

The value of C_{max} determines how much collateral each nomin is issued against. The higher it is, the more nomins can be generated for the same value of havvens. By contrast, if C_{max} is low, the system has a greater capacity to absorb negative shocks in the havven price before it becomes undercollateralised. The value of C_{max} therefore represents a tradeoff between *efficiency* and *resilience*. By defining C_{max} as a function of C_{opt}, Havven finds the optimal balance in this dilemma. This ensures that like C_{opt}, C_{max} only changes as a consequence of instability in the nomin price.

It should be noted that $C_{max} > 1$ corresponds to a fractional reserve monetary system, where a greater value of nomins can be issued against each havven. In Havven, this situation is unsustainable because it would cause simultaneous appreciation of havvens (up to at least the value of nomins issuable against a havven) and depreciation of nomins, immediately diminishing C, C_{opt} and C_{max}, bringing them back under 1.

Archived copy · cryp2nova.com

2.4 Transaction Fees

Havven needs a direct incentive mechanism that can correct the global collateralisation ratio, C, in response to changes in the price of havvens or nomins. In order to target the correct price, the system adjusts the fees it pays to havven holders according to their effectiveness in stabilising the nomin price.

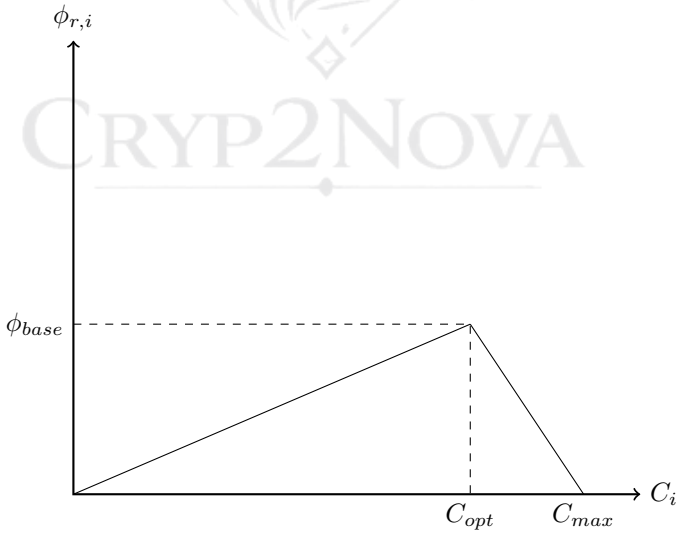
2.4.1 Fees Received by Havven Holders

The fee rate received by a havven holder that has escrowed havvens is $\phi_{r,i}$. The actual fee they receive is $H_i \cdot \phi_{r,i}$, being proportional with their havven balance. This rate changes with respect to their unique collateralisation ratio, C_i. It increases linearly to a maximum ϕ_{base} at the optimal collateralisation ratio C_{opt}, before quickly diminishing as C_i approaches the maximum collateralisation 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 bring their C_i into alignment with C_{opt}.

$$\phi_{r,i} = \phi_{base} \cdot \Gamma_i \tag{7}$$

$$\Gamma_i = \begin{cases} \frac{C_i}{C_{opt}} & \text{when } C_i \leq C_{opt} \\ \frac{C_{max} - C_i}{C_{max} - C_{opt}} & \text{when } C_{opt} < C_i \leq C_{max} \\ 0 & \text{otherwise} \end{cases} \tag{8}$$



Cryp2Nova

Archived copy · cryp2nova.com

2.4.2 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 move the circulating nomin supply towards N^*.

The fee rate charged on nomin transactions is ϕ_c. It is constant and will be sufficiently small that it provides little to no friction for the user. We may then express the total fees collected in a period, F, as a function of the velocity of nomins v and the total nomin supply N:

$$F = v \cdot \phi_c \cdot N \tag{9}$$

2.4.3 Base Fee Rate

Let us define the total fees received by havven holders F_r:

$$F_r = \sum_i H_i \cdot \phi_{r,i} \tag{10}$$

Havven requires that the total fees collected from users has to be equal to the total amount of fees paid to the havven holders in the following period, so that $F_{r,t} = F_{t-1}$. Substituting our earlier definition (7) for $\phi_{r,i}$ and solving for ϕ_{base}:

$$\phi_{base,t} = \frac{F_{t-1}}{\sum_i H_{i,t} \cdot \Gamma_{i,t}} \tag{11}$$

We have now defined the maximum fee rate, ϕ_{base}, in terms of the fees collected, F. This rate should be achieved when an individual's C_i was at C_{opt} in the previous period.

The definition of C_{opt} therefore provides the following incentive. If $P_n > \$1$ then the system encourages more nomins to be issued. However, if $P_n < \$1$, the system encourages nomins to be burned.

Archived copy · cryp2nova.com

3 System Analysis

3.1 Nomin Demand and Havven Value

Being freely-tradable tokens, havvens will have a market price which, like the nomin price, can be measured with an oracle. Initially, while nomin demand is low, a seven day rolling average of the market price will be used for both havvens and nomins. This rolling average is designed to smooth out fluctuations in the market price and increase the cost of attacking the system.

However, once nomin transaction volume is sufficiently high, we may instead estimate the value of a havven by the fees it is likely to accrue. This value, which implicitly measures nomin volume, would allow issuance incentives to directly reflect changes in nomin demand. By using this value instead of the havven market price, the system can avoid the influence of speculation, since the permitted nomin supply would expand and contract in line with actual usage.

While the system cannot perfectly determine future fee returns and hence nomin demand, it is possible to estimate as a function of the transaction fees that the system has recently generated. This computation is designed not to be vulnerable to instantaneous volume spikes, while taking the most recent transaction volumes to be the most highly-correlated with future volumes:

$$V_t \;=\; \sum_{t'=1}^{t} \frac{F_{t-t'} \cdot P_{n,t-t'}}{(1+r)^{t'}} \tag{12}$$

with

V_t	the system's valuation of a havven at period t
F_t	the total fees collected in period t
$P_{n,t}$	the nomin price at period t
r	a falloff term

This can be computed efficiently, because $V_{t+1} = \frac{V_t \;+\; F_t \cdot P_{n,t}}{1+r}$. Further, for large enough t, if it is assumed that $P_n \approx \$1$ and that current fees are close to future ones, so that $F_t \approx F_{t'},\ t < t'$, then:

$$V_t \;\approx\; \sum_{t'=1}^{\infty} \frac{F_t}{(1+r)^{t'}} \;=\; \frac{F_t}{H \cdot r} \tag{13}$$

Consequently, $\frac{1}{r}$ approximates the number of periods for a havven to yield a fee return of V_t. A judicious choice of r can then yield a V_t which underestimates the market price of havvens (which also incorporates, for example, capital gains), while not unduly constraining nomin supply.

Archived copy · cryp2nova.com

3.2 Fee Evasion

Being a set of smart contracts, Havven is potentially vulnerable to the wrapping of its tokens being by another smart contract. Such a smart contract would take deposits of nomins, and replicate all nomin functionality on redeemable IOU tokens it issues. These wrapped tokens could then be exchanged without incurring fees. We consider this situation unlikely for a number of reasons.

First, the fees are designed to be low enough that most users shouldn't notice them, so they will not in general be strongly motivated to switch to a marginal and less trustworthy alternative. Additionally, transfer fees will still be charged upon deposit into and withdrawal from token-wrapping contracts, which partly constrains the utility of the wrapper.
Second, network effects are tremendously important for currencies; in order to have utility a token must be accepted for exchange in the marketplace. This is challenging enough in itself, but a wrapped token must do this to the extent that it displaces its own perfect substitute: the token it wraps. In Havven's case, this would undermine its built-in stabilisation mechanisms, which become more powerful with increased transaction volume. Consequently, as a wrapped nomin parasitises more of the nomin market, it destroys the basis of its own utility, which is that nomins themselves are stable.
Finally, it is unlikely that a token wrapper will be credible, not having been publicly and expensively audited, while its primary function undermines the trustworthiness of its authors.

Even as token wrapping may appear unlikely to the authors, there are at least two remedies which can be instituted to resolve this.

It would be a simple matter to implement a democratic remedy, weighted by havven balance, by which havven holders can freeze or confiscate the balance 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 token wrappers from being used, even if they are written, since any user who does so risks losing their entire wrapped balance.

An alternative solution is to institute a hedging fee, charged on static nomin balances. Such a fee could be discounted against transfer fees so that it encourages general token velocity, and imposes a cost on those who buy nomins simply in order to hedge, and are thus a risk for the network. Under this model, a token wrapper would not dodge this fee: the full balance that was wrapped will not be available at the time of unwrapping.

Archived copy · cryp2nova.com

3.3 Issuance Case Study

In this section we illustrate how Havven's incentives encourage havven holders to maintain stability.
In 3.3.1, we first present a simplified example the practical issuance dynamics for a havven holder, Bob, if he targets C_{opt}. In the second part, 3.3.2, we examine the optimality of following this strategy with a more sophisticated model of the mechanism as a two-player game.

It should be noted that these are simply illustrative examples to give the reader a feel for the nature of the system's issuance dynamics. This section is partly an adaptation of the calibrated analysis results presented in much greater depth in as part of the economic analysis of Havven performed by cryptecon, which can be found in its entirety here.

The cryptecon investigation concluded that the Havven system generally stabilises the nomin price at $1, but most of the supporting apparatus has been omitted in this white paper. Therefore, an interested reader should consult that reference for further details and an explanation of the assumptions which underly its results.

Throughout this section we will assume implementation upon Ethereuem, therefore in this example, the system will buy and sell nomins in exchange for ether, but this could be substituted with any asset tradeable in a decentralised way.

CRYP2NOVA

Archived copy · cryp2nova.com

3.3.1 Practical Issuance Dynamics

Initial Conditions

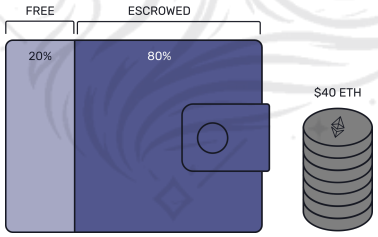
Bob decides to purchase 100 havvens at $1 each. The system is in price equilibrium, with the global collateralisation ratio C equal to the optimal collateralisation ratio C_{opt}. We will denote Bob's personal H and C_i with H_{bob} and C_{bob}. The initial conditions are then as follows:

$$C_{max} = 0.5 \qquad C_{opt} = 0.4 \qquad C = 0.4$$
$$P_n = 1 \qquad P_h = 1 \qquad H_{bob} = 100$$

The internal parameters of C_{opt} and C_{max}, as described in section 2.3, will remain constant throughout the example:

$$\sigma = 50 \qquad \psi = 3 \qquad a = 1.25$$

Initially, Bob's wallet contains only free havvens, but he wants to earn the maximum possible fees, so he issues nomins up to C_{opt}. The system generates 40 nomins and escrows 80 of his havvens, locking $80 worth of value in the system. The nomins are sold for $40 worth of ether and the proceeds are transferred to Bob's account.



We now proceed to examine the respective consequences for Bob of nomin and havven price shocks.

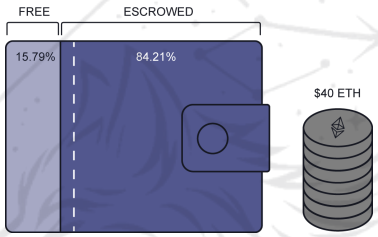
Archived copy · cryp2nova.com

Nomin Price Shock

This example shows how the system incentivises havven holders to correct instability in the nomin price.

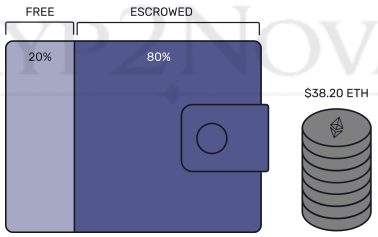
1. As a consequence of reduced demand in decentralised trading markets, the nomin price P_n drops to \$0.90. The system needs to incentivise havven holders to reduce the supply of nomins so that the price returns to \$1.00.

2. First, consider that both C and C_{bob} have decreased to 0.36. Since the nomin price has changed, C_{opt} is recalculated to 0.342, which is smaller than both C_{bob} and C. Consequently, C_{max} also changes to 0.4275. This increases the percentage of Bob's havvens that are locked.



3. Bob now has a higher dollar value of locked havvens and $C_{bob} > C_{opt}$. This means that he is no longer receiving the maximum fee rate ϕ_{base}. In order to return to ϕ_{base} he must lower C_{bob} back to C_{opt} by burning some nomins. He needs to work out how many to burn.

4. He should burn 2 nomins so that he has 38 total issued, which will cost \$1.80. When the system completes this process, his locked havvens will reduce back to 80. In addition, C_{bob} is equal to C_{opt} at 0.342, which means he is once again receiving the maximum fee rate.



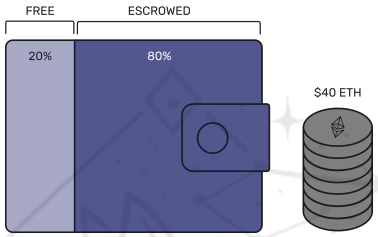
5. Bob has taken the correct actions to raise the low nomin price. By electing to burn nomins, the system performed a limit buy order on his behalf, putting upward pressure on the nomin price. As compensation for doing so, he is rewarded with the optimal fee rate ϕ_{base}.

Archived copy · cryp2nova.com

Havven Price Shock (Market Price)

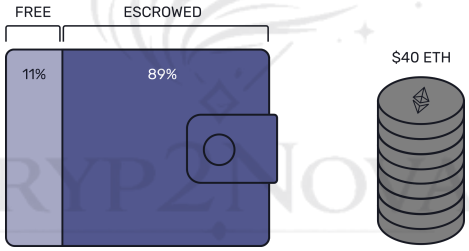
This example illustrates how the system maintains the dollar value of the underlying collateral by adjusting the quantity of a user's escrowed havvens when the havven price changes. We will use the same initial conditions as in the previous example.

1. As before, Bob elects to issue up to C_{opt} in order to maximise fees.



2. The havven price P_h drops to \$0.90, which means the value of Bob's wallet has decreased to \$90. Both C and C_{bob} have increased to 0.44. Since the nomin price has not changed, the system does not need to incentivise issuance or burning. This is reflected in the new value of C_{opt}, which changes to 0.44, matching C and C_{bob}.

3. However, the system needs to escrow more of Bob's havvens to maintain the dollar value of the locked collateral. The system has now locked around 89% of Bob's havvens, to maintain \$80 of locked collateral.



Archived copy · cryp2nova.com

3.3.2 Optimality of Targeting C_{opt}

We will now examine the correct action for players to respond to changes in the nomin price. The game begins in an equilibrium condition, with all players holding issuance levels matching the optimal level.

For simplicity, we consider a system which has only two havven holders. We lose no generality here, as a collection of actors behaving together can be considered as one agent. The sets of agents we consider are those those havven holders who do and do not respond to nomin price shocks by matching their aggregated C_i to C_{opt} as it changes, which is motivated by the monotonicity of the fee function (7) on either side of its maximum.
One player is assumed to own fewer havvens than the other. If this is not the case, then in reality it soon will be if one strategy player's strategy is more profitable than the other's.

We will examine each of the four cases describing how each player can act, and show that the correct action is for each player to target C_{opt}.

Initial Conditions and Definitions

We denote the fraction of e-commerce transactions using nomins with $\varepsilon \cdot GDP$ and assume the following inverse demand function for the nomin price:

$$P_{n,t} = \frac{\varepsilon \cdot GDP_t}{v_t \cdot N_t}$$

The expected profit of a havven holder i at period t, with respect to fees and their issuance actions can be expressed as follows:

$$\pi_{i,t} = \phi_{r,i,t} \cdot \frac{H_{i,t}}{r} \; + \; (N_{i,t} - N_{i,t-1}) \cdot P_{n,t}$$

The first havven holder owns 100 havvens and has issued 50 nomins. The second owns 200 havvens and has issued 100 nomins. Neither havven holder buys or sells havvens:

$$\begin{array}{lll} H = 300 & H_1 = 100 & H_2 = 200 \\ N_{-1} = 150 & N_{1,-1} = 50 & N_{2,-1} = 100 \end{array}$$

The transaction fee rate (ϕ_c), interest rate (r) and velocity (v) are fixed throughout:

$$\phi_c = 0.2\% \qquad r = 0.6\% \qquad v = 6$$

Archived copy · cryp2nova.com

The values of the price sensitivity parameter (σ), the flattening parameter (ψ) and the C_{max} multiplier (a) are:

$$\sigma = 50 \qquad \psi = 3 \qquad a = 1.25$$

To evaluate $P_{n,-1}$ we assume that $\varepsilon \cdot GDP_{-1} = 900$. We can now also evaluate $P_{h,-1}$ and the initial issuance ratios:

$P_{n,-1}$	$P_{h,-1}$	C_{-1}	$C_{1,-1}$	$C_{2,-1}$	$f(P_{n,-1})$	$C_{opt,-1}$	$C_{max,-1}$
1	1	0.5	0.5	0.5	1	0.5	0.625

Table 1: Prices and collateralisation; $t = -1$

The number of escrowed havvens for each havven holder is given by equation (4). We can also evaluate their expected profits:

$$\check{H}_{1,-1} = 80 \qquad \pi_{1,-1} = 100$$
$$\check{H}_{2,-1} = 160 \qquad \pi_{2,-1} = 200$$

At the beginning of period $t = 0$, there is a 10% decrease in $\varepsilon \cdot GDP$ causing the nomin price P_n to decrease from \$1 to \$0.90, but neither player has yet reacted to the situation:

$P_{n,0}$	$P_{h,0}$	C_0	$C_{1,0}$	$C_{2,0}$	$f(P_{n,0})$	$C_{opt,0}$	$C_{max,0}$
0.9	0.9	0.5	0.5	0.5	0.905	0.4525	0.5656

Table 2: Negative shock; no reaction; $t = 0$

We now consider all possible combinations of actions in turn. Either one, neither, or each player will react to bring their own issuance levels into line with C_{opt}. We examine the resulting expected profit for each player in each situation and show that the correct action for both players is to do so.

Archived copy · cryp2nova.com

Neither Havven Holder Reacts

If neither havven holder changes N_i then P_n will remain at \$0.90. Altough for both havven holders $\phi_{r,i,1} < \phi_{base,1}$, their expected profits remain the same. This is because they have the same fee rate, all fees must be distributed and collectively they own all havvens. However, their number of locked havvens has increased:

$$N_{1,1} = 50 \qquad \check{H}_{1,1} = 88.4 \qquad \pi_{1,1} = 100$$
$$N_{2,1} = 100 \qquad \check{H}_{2,1} = 176.8 \qquad \pi_{2,1} = 200$$

Both Havven Holders React

Instead of remaining idle, each havven holder has an opportunity to increase $\phi_{r,i,1}$ by changing $N_{i,1}$ to align with $C_{opt,0}$:

$$N_{i,1} = \frac{C_{opt,0} \cdot P_{h,0} \cdot H_i}{P_{n,0}}$$

If both havven holders target C_{opt}, their new nomin balances, locked havvens and expected profits are:

$$N_{1,1} = 45.25 \qquad \check{H}_{1,1} = 80 \qquad \pi_{1,1} = 86.22$$
$$N_{2,1} = 90.5 \qquad \check{H}_{2,1} = 160 \qquad \pi_{2,1} = 172.45$$

Due to their actions, the nomin price, $P_{n,1} \approx 1$, $f(P_{n,1}) \approx 1$ and $C_{opt,1} \approx C_1$. There is no further incentive for either havven holder to change N_i. They also have reduced $\check{H}_i$ to the level it was originally:

$P_{n,1}$	$P_{h,1}$	C_1	$C_{1,1}$	$C_{2,1}$	$f(P_{n,1})$	$C_{opt,1}$	$C_{max,1}$
0.9945	0.9	0.500	0.500	0.500	0.999	0.499	0.625

Table 3: Negative shock; both react; $t = 1$

Havven Holder 1 Reacts

We now consider the scenario in which only the first havven holder changes N_1. We show the payoffs for each havven holder after 6 iterations. Havven holder 1 improves his profit at the expense of havven holder 2:

$$N_{1,6} = 46.57 \qquad \check{H}_{1,6} = 80 \qquad \pi_{1,6} = 118.53$$
$$N_{2,6} = 100 \qquad \check{H}_{2,6} = 171.77 \qquad \pi_{2,6} = 171.58$$

Archived copy · cryp2nova.com

P_n stabilises around \$0.92 instead of \$1. The reason being that, although $P_n \neq 1$, $C_{1,6} = C_{opt,6}$. This means that havven holder 1 has no further incentive to change N_1:

$P_{n,6}$	$P_{h,6}$	C_6	$C_{1,6}$	$C_{2,6}$	$f(P_{n,6})$	$C_{opt,6}$	$C_{max,6}$
0.921	0.9	0.500	0.477	0.512	0.953	0.477	0.596

Table 4: Negative shock; havven holder 1 reacts; $t = 6$

Havven Holder 2 Reacts

Finally, we consider the case in which only havven holder 2 changes N_2:

$$N_{1,6} = 50 \qquad \check{H}_{1,6} = 85.31 \qquad \pi_{1,6} = 77.25$$
$$N_{2,6} = 93.78 \qquad \check{H}_{2,6} = 160 \qquad \pi_{2,6} = 204.90$$

In this case, havven holder 2 improves his profit at the expense of havven holder 1. Again, P_n does not stabilise at \$1 but does stabilise closer to \$1 than in the previous scenario, since havven holder 2 has a larger fraction of N:

$P_{n,6}$	$P_{h,6}$	C_6	$C_{1,6}$	$C_{2,6}$	$f(P_{n,6})$	$C_{opt,6}$	$C_{max,6}$
0.939	0.9	0.500	0.522	0.489	0.978	0.489	0.612

Table 5: Negative shock; havven holder 2 reacts; $t = 6$

Nash Equilibrium

Both havven holders are best off by changing N_i to align with C_{opt}. Although for each of them the best scenario would be if the other does not do anything, this scenario cannot be an equilibrium. This can be seen from the following strategic game representation of the previous analysis (for this representation, we assume that all iterations are made instantaneously and simultaneously by both havven holders).

	$N_{2,0}$	N_2^*
$N_{1,0}$	(100, 200)	(77.25, 204.9)
N_1^*	(118.53, 171.58)	(86.21, 172.43)

Table 6: Negative shock; strategic game representation

$N_{i,0}$ is the action of maintaining the same number of nomins taken by holder i, whereas N_i^* is the action of changing their nomin issuance. Each box has the

Archived copy · cryp2nova.com

payoff that both holders get by choosing some particular action. For example, if havven holder 1 chooses $N_{1,0}$ and holder 2 chooses $N_{2,0}$, the former gets a payoff of 100 and the latter 200. It can be seen that havven holder 1 will choose N_1^* no matter what action is chosen by havven holder 2 (1 gets larger payoffs following N_1^* for any action that 2 can take). Similarly, 2 will choose N_2^* no matter what the action of havven holder 1 is. In other words, action N_i^* strictly dominates remaining idle with $N_{i,0}$. Therefore, $\{N_1^*, N_2^*\}$ is the unique Nash equilibrium.

Other Conditions

Note that the expected profit for each player decreases in the case of a negative price adjustment. This is due to the fact that the players must buy back nomins from the market. Yet this analysis does not take into account the profit obtained by later selling those nomins in the case of a positive price adjustment.

The analysis for an isolated positive correction is similar to that for a negative one, but since nomins are being issued rather than burnt, the nash equilibrium profits strictly increase versus the "do nothing" scenario. A table similar to the one above can be constructed for the case of a positive price shock:

	$N_{2,0}$	N_2^*
$N_{1,0}$	(100, 200)	(100, 218.5)
N_1^*	(110.2, 200)	(114.7, 229.5)

Table 7: Positive shock; strategic game representation

In both cases the expected profit is positive; note that a balanced sequence of positive and negative price shocks yields a positive expected profit. Thus in a steady state havven holders should be able to profitably stabilise the system, and absorb modest decreases in aggregate nomin demand.

CRYP2NOVA

Archived copy · cryp2nova.com

Appendices

A Road Map

The Havven system will be released in phases, described in the following sections. This phased rollout accelerates market penetration while allowing features to be introduced and monitored incrementally. The intended approach is to decentralise Havven as it is built, which will be accompanied by a gradual increase in the issuance ratio while the system develops. This provides a balance of safety and functionality until Havven is fully mature.

Release Schedule

Type	Iteration	Release (2018)
eUSD	Ether-Backed Nomins	Q1
nUSD	System A: Static Foundation Issuance	Q2
	System B: Dynamic Market Issuance	Q3
	System C: Multi-Currency Nomins	Q4

A.1 Ether-Backed Nomins (`eUSD`)

The ether-backed nomin system implements `eUSD`, an interim stablecoin which is designed to enable data collection to determine the parameters necessary for the havven-backed nUSD system. Price stability is maintained by a pool of ether which backs the circulating stablecoin supply. In this system, `eUSD` can be purchased from and sold into a pool for $1 worth of ether. The Havven foundation provides at least $2 of ether collateral for each issued `eUSD`, which ensures that the entire supply is redeemable for its face value even in the face of the ether price falling by up to two thirds. Fees are collected on transactions, and these fees are collected by havven owners.

The `eUSD` system, being based on ether collateral, has a constrained maximum supply. Therefore, in order to scale, the system must move towards its ultimate issuance mechanism, where nomins are backed with havvens.

Archived copy · cryp2nova.com

A.2 Havven-Backed Nomins (nUSD)

System A Static Foundation Issuance

The System A version of nUSD allows issuance of nomins against the value of havvens up to a static ratio, which is set by the Havven foundation. nUSD will be created directly in the issuer's wallet, and fees paid proportionally with the number of issued nomins per user. Given that it's necessary to encourage liquidity, but not all the mechanisms outlined in this paper will be operating yet, issuance will be by the foundation itself, and potentially other white-listed addresses it trusts. In this way, the stability of the token is maintained by direct market intervention by the foundation.

As System A fundamentally changes the issuance mechanics, nUSD is a distinct token from eUSD, even though both target a price of $1. At the time of the nUSD launch, the eUSD contract will enter a liquidation period, when eUSD can be sold back to the contract. At the conclusion of this period, the contract will be destroyed. Future updates to the Havven system will not entail the destruction of any nomin tokens; thus both havvens and nUSD will persist without further interruption.

System A limits issuance so that only those havvens the foundation controls can be used to back nomins, which means the full value of the havven network cannot be deployed for issuance. At this stage the market will be monitored closely by the Havven foundation, and the issuance ratio maintained at a low level or gradually increased to allow for expansion of the nUSD supply. This version of the system is constrained while the remaining system parameters described in this paper are finalised. Since nomins are created directly in the issuer's wallet, liquidity may be limited if issuers choose not to sell those nomins, which would be counterproductive to the general goal of stability. Systems B aims to combat such limitations.

System B Dynamic Market Issuance

System B composes the complete mechanism as described in the main body of this paper. The incentives will be activated so that users earn fees in accordance with how effectively they stabilise the nomin price. System B will enforce that issuance occurs through an issuance controller or decentralised exchange to ensure that new liquidity is injected directly into the market at $1 per nomin. The Havven system must manage open issue/burn orders while also continually updating the price at which they are offered.
These elements being in place, market players are encouraged to behave correctly. Thus, this phase opens up the opportunity for anyone to engaging in the issuance process. With the intended mechanisms operational, any cap on the ultimate scale of the Havven system is effectively removed, and the most

Archived copy · cryp2nova.com

important remaining task is stimulating demand for nomins.

System C Multi-Currency Nomins

One means of increasing usage of nomins is offering it denominated against a variety of different currencies. In principle, the Havven mechanism can target the price of any asset. With this in mind, the foundation intends to allow issuance of different flavours of nomins. For example, in addition to nUSD, the system could also allow nKRW to be issued, tracking the price of the Korean won. In such a system, issuers would be rewarded with fees only for currencies they have issued. This extension would replicate the Havven mechanism for each currency. If such issuance occurs against the same collateral pool, it is straightforward to see that in the absence of other incentives, the issued supply of each nomin flavour should be proportional with the each flavour's share of total transaction volume.

A multicurrency nomin system clearly has the advantage of providing the benefits of stablecoins to many markets, and thus of deepening the fee-generating volume for havvens. But that these nomin flavours are interrelated by the common pool of capital provides extra utility in the form of relatively cheap foreign exchange in nomins, using havven issuance to settle between them. The introduction of new nomin flavours will become straightforward, requiring only the creation of a new oracle for the intended asset, which does not have to be a currency.

Once this version of the system is operational, additional extensions to its capabilities are anticipated for future work.

A.3 Continuing Development

The Havven protocol is not tied to any particular distributed ledger, only requiring general smart contract capabilities and a modicum of speed. However, its ultimate success is tied to the solution of a number of fundamental problems in the blockchain space, and to the quality of its own mechanisms. To this end, research and development efforts will continue in a number of relevant areas, which may include:

- Fast decentralised oracles.
- Alternative (scalable) blockchains and cross-chain functionality.
- Improved fee structures, including dynamic fees and hedging charges.
- Refined stabilisation mechanisms.
- System parameter optimisation.

Archived copy · cryp2nova.com

- Stablecoin econometrics and modelling.

In addition to these fundamental questions, the Havven foundation will continue to pursue integrations with projects which would benefit from a stable unit of account. This encompasses any platform needing a settlement token which integrates with decentralised systems. All such efforts aim to increase nomin transaction volume, increasing the resources available for havven holders to stabilise the token.

B Modelling

We take the view that falsification is vital in validating a proposed cryptoeconomic system. The more resilient a given system is to hypothetical attacks, the more trust can be put in its viability.

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

In our quantitative analysis, we have taken 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 leads 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

The earlier releases of the Havven system are invaluable in testing our assumptions about later ones. Observation of real market behaviour allows us to better understand how it responds in different situations, and therefore how to choose appropriate values for system variables.

Some of the results of our analytical investigations can be found here, while a simulation may be found here, and its code here.

Archived copy · cryp2nova.com

B.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.

B.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.

Archived copy · cryp2nova.com

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.

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. The interested reader can find additional discussion of payment networks, stablecoins, and cryptoeconomics at `http://blog.havven.io`.

CRYP2NOVA

Archived copy · cryp2nova.com