Havven: a stablecoin system
v0.3

Samuel Brooks, Anton Jurisevic, Kain Warwick

October 2017

1 Introduction

1.1 Money and Cryptocurrencies

There are three primary functions of money; 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. Money has become almost invisible over the past few decades as payment technology has advanced. Because of this, 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 as a technological improvement on existing forms of money is impressive because it manages to simultaneously improve durability, portability, and divisibility. Further, it does so without requiring the enforcement of a nation state from which to derive its value. The Bitcoin supply is, therefore, not subject to control by any central authority.

This fixed monetary policy means that increased adoption has tended to drive the price up over time, allowing Bitcoin to outperform other forms of money as a store of value, precisely because it is not subject to debasement and devaluation. Unfortunately this fixed monetary supply creates the potential for volatility in the short term because there is no mechanism within Bitcoin that can monitor or adjust to changing demand for the currency.

Thus it has 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 other goods and services, because money is ultimately a good that other goods are denominated in. If the price of money as a good is too variable then it becomes less useful as a denominator of other goods.

1.2 Stablecoins

A stablecoin is a cryptocurrency designed for price stability, such that it can function as both 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; 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 fact that as decentralised systems, they have had relatively inflexible internal monetary policies which have fostered volatility and deflation. Hence stability continues to be one of the most valuable and yet the most elusive characteristics. The fact that we have yet to achieve stability in cryptocurrencies without resorting to extreme centralisation should by no means be taken as evidence that this problem is insurmountable. The reality is that the technology to create alternative monetary policies within cryptoeconomic systems has only existed for a few years. Clearly, significant research into stable monetary frameworks for cryptocurrencies is required.

1.3 Achieving Stability

A viable, autonomous, and decentralised stablecoin is a *sine qua non* for achieving a decentralised economy. Such a token is a challenge to design. Central banks have near complete discretion over their money supplies; a great deal of effort and wealth are expended in supporting the stability of state-backed fiat currencies. And yet, there are many examples where these efforts have utterly failed. Stability is far harder in cryptoeconomic systems because their behaviour must be almost completely defined at the start, which means that there can be very little consideration for events that are unpredicted. We must likely resign ourselves to the fact that these systems will be only functional under certain conditions. However, if those conditions are well understood, and the cost of destabilising the system is greater than any derived benefit, we might ensure that the utility of the system outweighs the risks of participating in it.

With Havven we have accepted that such an approach to building an *intrinsically* stable currency is likely out of reach in the short term. If economists cannot agree on the optimal approach to monetary policy, it seems unlikely that a system constructed with the current orthodoxies baked in could succeed in the long term. Instead we prefer simply to map the value of a stable token to that of the global reserve currency, the USD. In this way we provide *nominal* stability, by relying on the stability of the underlying fiat currency. This peg, stable as measured with respect to a single external asset, is more achievable, though it has an obvious limitation: it is only as good as that external asset. For example, ff the US dollar is subject to hyperinflation, our stable token will be similarly impacted. However, we do not consider this to be a severe problem, given the historically greater stability of fiat currencies, and that any other asset can be trivially substituted for USD at any time.

1.4 Havven

The mechanism Havven uses for maintaining its peg relies on two linked tokens and a complex of incentives for stability:

Nomin The stablecoin itself, 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.

Curit The collateral token, whose supply is static. The capitalisation of the curits in the market reflects the system's aggregate value, and the reserve which backs the stablecoin. Thus, users who hold curits take on the role of maintaining the peg.

Each holder of curits is granted the right to issue a value of nomins in proportion to the USD value of the curits they hold and are willing to place into escrow. If the user wishes to redeem their escrowed curits, they must present the system with nomins in order to free their curits 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, nomin-issuers will be rewarded with fees the system levies automatically as part of its normal operation.

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 curits backing them. If the curit price changes, then the volume of the token pool changes with it. On the other hand, if the nomin price changes exogenously, then the system is designed to provide incentives for actors to counteract that change.

1.5 Rationale

It is clear that the introduction of a new cryptocurrency, in isolation, offers no additional value given the existing and established alternatives such as Bitcoin and 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. So any token which is able to demonstrate an increment in utility on these fronts over both fiat and cryptocurrencies will significantly enhance the uptake of cryptocurrency.
In his discussion of Hayek money[1], Ametrano correctly makes the point that Bitcoin serves the purpose of crypto-gold much better than it does crypto-unit-of-account due to its volatility and constrained supply. By contrast, governments – which mint their own currencies – can and do execute discretionary stabilisation policies to manipulate the circulating supply. This kind of powerful lever is not available to Bitcoin and other supply-constrained currencies of its type, but a similar system whose monetary policy is algorithmically countercyclical rather than deflationary could inherit the desirable characteristics of both monetary paradigms. It should be possible, by automatic means, to incentivise the issuance and destruction of tokens according to demand. In this way, users of such a currency would be allowed to capitalise it while the system automatically seeks to expand and contract the money supply as its backing reserve fluctuates in value. By this mechanism we might produce a more perfect currency where supply floats with necessity, but which is not prone to debasement and other issues commonly associated with inflationary or deflationary forms of money. Ideally, we also seek to remove some of the distortions created by traditional monetary policy, which, when it is expansionary, shrinks the purchasing power in every account which is not a direct beneficiary of that policy.

The Havven stablecoin system is akin to representative money in the sense that the fungible nomin tokens represent some value held in reserve. We define the curit to be the token of backing value as this is both the start and end point of using the Havven mechanism; curits develop intrinsic value given their ability to maintain stability (through nomins) with an external denomination. Hence, nomins have no intrinsic value because we define curits as carrying the value associated with being able to provide a functioning stable medium of exchange.

Havven however is not representative money as we have traditionally known it. Historical instantiations, such as the gold standard which allowed anyone to claim against the reserve, caused exacerbations in times of economic turmoil. Given that it does not need to act as the primary currency in the market, Havven is relieved of any pressure to respond and correct for macroeconomic market issues. We leave such manipulations of the money supply to the whims of central banks, for good or ill. Thus Havven is at its simplest a bridge between fiat and cryptocurrency, a hybrid of the two technologies and thus for numerous use cases superior to both. But it bears repeating that whatever monetary policy is applied to the external denomination will flow through to the system. For example, if the USD is significantly devalued through inflation, so too will the nomin. In this scenario, the value of curits against the USD will increase and more nomins will be able to be issued against that value, so long as they are denominated in USD.

The Havven system is designed such that the nomin is both denominated in and mapped to an external store of value. Throughout this paper we use USD as the reference, however this could be any external and appropriately fungible asset, such as a commodity or fiat currency. Note that denominations in other cryptocurrencies are not necessary as these already benefit from the features Havven is implementing for the external denominator.

2 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.

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. It's hoped that this can often provide a more effective method of characterising market behaviour and equilibrium prices, when analytic reasoning fails.[3]

Such simulations also provide an immediate means of measuring quantities of interest. We can discover how varying input parameters affects system outputs in an experimental fashion, simply by observing the model. 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.

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

- Does the system stabilise its nomin price?
- Under what conditions can this peg fail?
- What are reasonable initial settings for fees and other parameters?

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

3 Functional description

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

3.1 Stability design considerations

Fundamentally, we wish to configure the system such that it incentivises the desired properties of a stablecoin, namely:

1. Value stabilisation
2. Value transfer

This paper focuses on value stabilisation as the key enabler for a better form of money; once we have this, we assume that we get value-transfer (market share for the currency) for free.

Let us consider the various ways in which one can maintain a stable value relative to a fiat currency. The question we wish to answer is, "How can we **control the value** of the cryptocurrency such that the price of one unit of the stablecoin matches the price of one unit of the denominating currency?" This is a challenging scenario because there are multiple related forces at work on the price of each currency. We consider these as two independent groups: "market forces" and "control forces".

Market forces represent supply and demand. These are necessarily different for each currency, otherwise they would move strictly in unison.

Control forces then are the controls one is able to apply over a currency to affect its value, such as an inflation rate or a buy-back scheme.

Our price mapping then should seek to tune the control forces such that one unit of a control currency equals one unit of the denominating currency. We assume that the forces for one currency are independent of the forces for another.

So what are the mechanisms we can apply to control the value of a currency? We consider:

- Issuing new currency to increase supply (inflation)
- Buying back existing currency to decrease supply (deflation)
- Unilateral balance control (changing account balances to maintain a stable buying power)
- *Others?*

Unilateral balance control, such described by Amentrano (source), is discounted on the basis that an individual's balances being directly modified would be unpalatable to the general population.

This leaves us with simply the forces relating to modifying supply.

We review the key incentive drivers in the design of an economically stable cryptocurrency.

- Fees
- Supply control
- Capital growth
- Bonds

We also consider the following significant questions:

- How do we incentivise actors to contribute to system liquidity?
- How should Nomins be created and destroyed?
- Should fees only be given to those who have actually issued Nomins?
- Are transfer fees charged in only Nomins? Would actors not then just try to convert to Curits and exchange there?
- How do we select a utilisation ratio? What is its curve?
- Should we allow the system to maintain a pool of Curits/Nomins that it itself can buy/sell?
- What if the system didn't burn the Nomins that were handed back when Curits were redeemed?
- Should Nomins, or Curits, be serialised?
- Should newly created Nomins go to escrowed Curit accounts, or be sold?

3.2 Description of mechanism

Curit holders have an ongoing option to commit to an escrow of their collateral token in return for an amount of Nomins valued at some fraction of the value of the Curits, denominated in USD. We call this fraction the Utilisation Ratio, (or later more formally, the Issuance Ratio), U.

A Curit holder can then sell their Nomins for ETH for any price (or we can force a sale at the correct ETH price), and retain the ETH.

3.3 Alternative approaches

An autonomous system which mimics the actions of a central bank, wherein reserves of cryptocurrency are held for the purposes of currency buy-back was also considered. This approach involves a complex system of managing bonds and Nomin issuance as coupons to bond-holders (similar to Basecoin), whilst also acting as a buyer of last resort for all Nomins sold under the peg beyond some threshold. This approach was discounted due to the need to anticipate complex market counter-algorithms to support the peg. By contrast, the Havven mechanism is a novel and simpler approach which uses only open market incentives for economically rational participants to bring stability to the exchange token.

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 the outside world. Often, this is done by sacrificing trust; in order to reclaim system performance, we can trade some of the trustlessness of the design, such as through implementing an trusted “Oracle” service in order to gain knowledge of the external world and build a causal link.[?].

3.5 Backing collateral

Central to the design of the Havven money system is how the currency is backed by collateral.

For monetary systems that are backed by an external asset, centralisation risks are frequently encountered and are often without solution. The question arises:

How can one take an external asset and make it distributed such that we can mitigate the centralisation risk?

We contend that the simplest and most elegant solution is to use the system itself as the backing collateral. We can then issue an exchange token against this in a manner similar to fiat in that the exchange token has no intrinsic value, but similar to representative money in that the collateralised value exists in the Curit token.

The basis for Havven is the initial acceptance of the idea that the asset can be the system. The only other alternative is to use a basket of cryptocurrencies to back the exchange token, however this ultimately suffers from the same issues we are trying to prevent, namely volatility that is only mitigated through diversification.

Finally, in backing by a real-world (external) asset, such as gold or a state currency, we encounter centralisation risks once again, including an inability to prove the existence of the backing asset (fraud risk).

Fundamentally, whenever you want to denominate a stablecoin in something from the real world (such as USD), then you will always need a bridge between the real world and the walled garden of the blockchain.

To this end, our design initially assumes an Oracle-based bridge between fiat and Ether. The price of Ether is then taken and injected into the Havven Decentralised Exchange (DEX) where Curits and Nomins can be bought and sold. The DEX can then act with knowledge of the exchange rate between Ether/USD.

In the future, we aim to remove the need for an Oracle; we are currently working on a method to use a purely on-chain mechanism to discover the price of Ether in fiat.

3.6 System pricing

We consider several options in estimating the total value of the Havven stablecoin system (i.e. what is the price of a Curit?):

- Initial Pricing of the value of the system (Curits):

    1. Market-discovered pricing. This is likely to be initially undervalued and grow over time.

    2. Pre-determined, calculated estimate

    3. Hybrid: capped ICO of a portion of the Curits at an estimated value of the ultimate system

- 3. Ongoing pricing of the value of the system (Curits):

    1. Oracle.

    2. Rolling auction.

    3. DEX (experimental)

3.7 Investment incentives

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

Capital gains due to the appreciation of Curits: Presumably the currency will appreciate due to a demand for Curits that is founded in the intrinsic utility of a stablecoin. Speculators will naturally be important players too.

Interest accrued from fees: If and when the price of Curits stabilises, then this may be the only long term positive-expected 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 Curits 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, Curits, and the external (crypto or fiat) markets. They might hold Curits for a short time in order to pursue this strategy.

3.8 Fees

There are a number of questions to be asked, and answered, regarding fee design:

- What are fees for?
- Who is entitled to them?
- When can fees be levied?
- What is the macroeconomic effect of the fee design as a coin travels through the system?

3.8.1 Discussion of 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 Curit holders to maximise liquidity in order to maximise their return.

Fee beneficiaries One fee design starting point is to simply award fees to any holder of Curits, however in this situation holders can get all the benefit without taking any risk. Although in the aggregate, it would be better for holders of Curits 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 may not be incentivised to issue Nomins at all.

We must improve the marginal benefit of issuing Nomins into circulation in order to avoid this tragedy of the commons situation. Hence, fees must be paid to those who issue Nomins, not just those who hold Curits.

Fee collection The system can potentially charge fees whenever any value is transferred, or any state is updated.

There are only a few circumstances that these things happen:

- Nomin transfers
- Curit transfers
- Nomin issuance
- Curit redemption

The question to consider is at what levels should these fees be placed? We might in general like to set higher Curit 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's also possible for fees to float. The fee schedule could be altered dynamically in order to stabilise the system. It's even conceivable that the system could set negative fee rates if it needed to. We might charge punitive fees if a user is above the targeted utilisation ratio.

One 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, reducing demand and decreasing the liquidity requirements.

It should be pointed out that fees are antithetical to arbitrage. The higher the fee, the higher the 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, Curits, 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.

3.9 Encouraging liquidity

It's desirable that when actors issue Nomins they are actually injected into the liquidity pool for their intended use, rather than be held by the same actor in order to benefit from both the receipt of fees but also the option of using those Nomins to release their Curits. In this manner they would accrue fees, but take on none of the risk of spending those Nomins, for they always have an instant option to liquidate their position and escape. An actor who had done the economically-desirable thing, on the other hand, who issued Nomins and then spent them, would be forced to buy Nomins in the open market in order to redeem their escrowed Curits.

The use of someone escrowing their Curits is that they provide backing for the currency flowing through the system, and so they should be rewarded for assuming this risk. In the fractional reserve system, this incentive is provided by the interest accrued upon the loans which generate money. It may be possible to adapt this system to Havven, by allowing issuers to escrow their Curits for a fixed time period, allowing the system to issue currency against that collateral, to be paid back a greater value of Nomins at a later time.

If an issuer should not just be able to hold Nomins and accrue fees, that must also include letting them sit in another wallet they control. They should also not be able to sell their Nomins into the open market and with the proceeds buy the same value and let *that* sit, only transferring it back to their main wallet once they want to flee.
But how to encourage a user to actually increase liquidity by buying goods with the Nomins they hold?

3.9.1 Non-discretionary Issuance

One possibility is to simply provide an issuer no control over the tokens they issue. That is, when a quantity 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 ETH are remitted to the issuer.

Conversely, when a quantity of Nomins is burned, they must first be obtained from the open market. So 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, only liquidating the user's Curit position once they 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. This means 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.

3.9.2 Motility

But let us assume that we cannot force a user to issue and burn from the open market. We might like to encourage an issuer to spend their Nomins by other means. One method is to provide every account with a motility score and pay fees in proportion with the product of this score and the number of tokens that account has issued.

This should be subject to common-sense obligations. The system should not be easily gamed. A user should not be able to cycle Nomins through accounts they control and collect fees. An issuer should not be able to just manipulate an account they control to have a high motility with small values and then dump a large value they want to hold into it. Ideally transferring value around repeatedly to manipulate the fee system would be expensive enough that the value lost to fees charged would outweigh the diminution of risk.

We would like to incentivise long transaction paths out of an account, and high out-degree nodes along those paths (so money is actually liquid/fungible). Hence, we don't like short cycles or isolated subgraphs. Ideally, money would travel into the main connected component of the transaction graph as quickly as possible, then circulate in there with high velocity.

Definitions

$$\begin{aligned}
A &: \text{ The set of all accounts} \\
T &: \text{ The multiset of all transactions; a subset of } A \times A \times \mathbb{N}. \\
T_{a \to b} \subseteq T &: \text{ The set of transactions from } a \text{ to } b \text{ with } a,\ b\ \in A. \\
v_t &: \text{ the value of a transaction } t \in T. \\
V_{a \to b} &:= \sum_{t \in T_{a \to b}} v_t \quad \text{(the total value transferred from } a \text{ to } b\text{)} \\
V_a^{in} &:= \sum_{p \in A} V_{p \to a} \\
V_a^{out} &:= \sum_{p \in A} V_{a \to p}
\end{aligned}$$

We might interpret (A, T) as a weighted multigraph of transactions, with each transaction $t \in T_{a \to b}$ corresponding to a weighted edge in that graph between nodes a and b. Note that $T_{a \to a} := \varnothing$, and hence $V_{a \to a} = 0$ (accounts can't transfer to themselves).

We would like to know how likely a Nomin is to be spent soon from a given account. The motility of the account should measure this. Considering an account a, we will take $\mathcal{M}(a)$ to be the motility of a:

$$\begin{aligned}\mathcal{M}(a) &:= \sum_{p \in A} P(a \text{ transfers to } p) \cdot \mathcal{M}(p) \\ &= \sum_{p \in A} \frac{V_{a \to p}}{V_a^{in}} \cdot \mathcal{M}(p) \\ &= \frac{1}{V_a^{in}} \sum_{p \in A} V_{a \to p} \cdot \mathcal{M}(p)\end{aligned}$$

Intuitively, if you transfer a lot of money to high-motility accounts, then your own motility is taken to be high.

Calculating Motility This will need to be calculated iteratively, and locally. Note that $V_{a \to p} = 0$ for p that a has never transferred to, so those accounts can be neglected. It's probably too costly to store the value of $V_{a \to b}$ explicitly. So we will have to eliminate this quantity in our expressions. We will update motility scores whenever a new transaction t from a to b of value v_t is made.

Value into b increases, so $\mathcal{M}(b)$ can be easily recalculated.

$$\begin{aligned}V_b^{in\prime} &\leftarrow V_b^{in} + v_t \\ \mathcal{M}'(b) &\leftarrow \frac{1}{V_b^{in\prime}} \sum_{p \in A} V_{b \to p} \cdot \mathcal{M}'(p)\end{aligned}$$

Meanwhile, the value transferred from a to b also increases.

$$\begin{aligned}V'_{a \to b} &\leftarrow V_{a \to b} + v_t \\ \mathcal{M}'(a) &\leftarrow \frac{1}{V_a^{in}} \Big(V'_{a \to b} \cdot \mathcal{M}'(b) \; + \sum_{p \in A \setminus \{b\}} V_{a \to p} \cdot \mathcal{M}'(p) \Big)\end{aligned}$$

Although these updates should also influence accounts which have (transitively) transferred into a and b, we want to reward people for increasing liquidity today, rather than at some future time, and we take the motility of an account to be relatively stable after some time. As a result we will take $\mathcal{M}'(p) \approx \mathcal{M}(p)$ for $p \notin \{a, b\}$. Then:

$$
\begin{aligned}
\mathcal{M}'(a) &\approx \frac{1}{V_a^{in}}\Big((V_{a\to b} + v_t) \cdot \mathcal{M}'(b) \; + \sum_{p \in A\setminus\{b\}} V_{a\to p} \cdot \mathcal{M}(p)\Big) \\
&\approx \frac{v_t}{V_a^{in}}\mathcal{M}'(b) \; + \frac{1}{V_a^{in}} \sum_{p\in A} V_{a\to p} \cdot \mathcal{M}(p)
\end{aligned}
$$

So we will take our update step for a transaction t from a to b to be the following:

$$
\begin{aligned}
V_b^{in\prime} &\leftarrow V_b^{in} + v_t \\
\mathcal{M}'(b) &\leftarrow \frac{V_b^{in}}{V_b^{in} + v_t}\mathcal{M}(b) \\
\mathcal{M}'(a) &\leftarrow \frac{v_t}{V_a^{in}}\mathcal{M}'(b) \; + \mathcal{M}(a)
\end{aligned}
$$

It may also be desirable to add a decay term so that accounts that have not moved any money in a long time are taken to have a lower motility.

3.10 System-actuated arbitrage

It is agreed that the system relies upon arbitrage to bring the prices of its various components into equilibrium. However, arbitrage is in some sense a form of economic friction.

One possibility is to allow Havven itself to perform this arbitrage. This serves the dual purposes of improving the efficiency of the markets, and contributing to Havven's own capital pools. Ini this way, arbitrage opportunities could be spotted early, capitalised upon in a fee-free manner, arbitrage profit within the Havven ecosystem could be retained for productive price-stabilisation purposes, mining rewards, and any other uses that are found for this excess capital.

3.11 Utilisation ratio

It's not clear to me exactly what purpose U_{max} serves. It certainly keeps the value of the pool of Curits below the value of the pool of Nomins, assuming there is no devaluation of a ratio more severe than U_{max} itself. However, if the system has adequate mechanisms enforce $U \leq U_{max}$, then why not simply allow users to issue Nomins up to the maximum value of Curits they have escrowed?

A low U_{max} seems like it would place upward pressure on the price of Nomins. Consider a situation where $U_{max} = 0.2$, and I have an impecunious friend, Jake, who owns a wallet which has issued \$20 worth of Nomins on the back of \$100 of escrowed Curits. At the moment, he has no money, but his wallet is worth \$80, since he can burn \$20 worth of Nomins to get at those curits. So Jake should be willing to pay anywhere up to \$80 to buy enough Nomins to free up the Curits. This situation will still motivate Jake until the price of the Nomins he's issued is equal to the price of the Curits he's escrowed. That is, until the price of a Nomin is worth five times the price of a Curit.

Finally, let's consider the impact of the utilisation ratio on a Curit investor's value proposition. Examine the aggregate fees collected from Nomin transfers Ag_{nx}, and expand out its definition:

$$Ag_{nx} = \frac{F_{nx} \cdot S_n \cdot C \cdot P_c \cdot U}{P_n}$$

This quantity is proportional with the actual utilisation ratio U. The more Nomins that have been issued, the more fees are returned. So if $U = 0.2$, then if the system would like to return a fee rate of 5% per annum to Curit-holders, then fees to the tune of 25% per year will have to be levied on Nomin transfers, assuming no other fees exist. This may be a little high.

3.12 Failure modes

We must try to identify ways Havven can produce undesirable results ahead of time so that they can be simulated and, if they turn out to be real issues, patched. In what follows we try to identify ways the system can fail, and explain why they are, or are not, likely or reasonable.

3.12.1 Nomin inflation cycle

Although it's true that the system limits the total value of Nomins relative to the total value of Curits, if the price of each individual Nomin falls, then more of them may be printed. If they are, then supply increases, further decreasing the price.
Is this a vector for hyperinflation? Is it rational for individual agents to engage in behaviour which would encourage this? We would like to avoid a Weimar-style devaluation of the currency, so we must ensure that is not the case.

Note that this is may be counterposed by the previous discussion of Nomin deflation due to the utilisation ratio limiting supply, although the higher the utilisation ratio ceiling, the weaker the effect. It remains to be seen through our modelling if that pressure is strong enough to overcome this inflationary scenario even at low utilisation ratios.

Consider an agent which wants only to issue as many Nomins as possible in order to accrue fees on them. The most obvious way of doing this is to buy Curits, and then perform the following steps repeatedly:

1. escrow all available Curits;
2. issue as many Nomins as possible against escrowed Curits;
3. sell the Nomins to buy more Curits;
4. goto 1.

Static price What quantity of escrowed Curits can be accumulated in this fashion? Let's say an agent starts with $\$c$ worth of Curits, and the max utilisation ratio is U_{max}.
Further assume that this agent is acting in isolation, with access to infinitely deep currency markets, and so can't change market prices by its actions. Then, on the first iteration, the agent obtains $U_{max} \cdot \$c$ additional value of Curits, against which a further $U_{max}^2 \cdot \$c$ worth of Nomins can be issued on the second iteration, and so on. In a frictionless market, this cycle is also perfectly reversible.

This geometric sum implies that after iterating as long as possible, the agent's wallet contains approximately $\sum_{k=0}^{\infty} U_{max}^k \cdot \$c \;\; = \frac{\$c}{1-U_{max}}$ worth of escrowed

Curits and $\frac{\$c \cdot U_{max}}{1-U_{max}}$ issued Nomins.

So, for example, if $U_{max} = 0.2$, then the agent can cycle until their wallet contains $\$1.25c$ worth of escrowed Curits and $\$0.25c$ worth of issued Nomins. That is, they have been able to issue 25% more Nomins than they naively should have been able to, and so will also collect 25% more fees. Note the agent assumes no extra risk if the market is sufficiently liquid, as they can still recover their original $\$c$ of Curits by unrolling the cycle.

These effects become more pronounced as U_{max} grows; at $U_{max} = 0.5$, an agent can issue twice the face value of its initial Curit supply. If $U_{max} = 1$, then the sum diverges, and agents can issue an infinite quantity of Nomins. Given transaction fees, this is never actually the case, but it is still extreme enough if a multiplier of tens or hundreds is in play.

Elastic price Of course, the reader may easily object that these situations are impossible both because the market is frictionless, and because as more agents try to exploit these cycles, Curits will become progressively more expensive, and Nomins progressively cheaper, so the cycles will become less advantageous. However this implies that agents with escrowed Curits will now immediately be able to issue more Nomins and continue the cycle.

The question now to answer is: is this a positive feedback loop? If so, then Havven might be vulnerable to hyperinflationary events. It's a little difficult to characterise the situation from here, since it depends upon the elasticities in the market, which we do not know a priori.

Let's assume the pool of agents following our strategy initially holds a fraction θ of the total supply of Curits, value $\$C$. We approximate with a assuming linear demand, supply, and elasticity curves. Then, by selling $\$U_{max}\theta C$ worth of Nomins and buying the same value of Curits, the price of Nomins will drop by a factor of around θ, while the price of Curits will increase by about $U_{max}\theta$. Hence, our pool's issuance rights will increase to $\frac{1+Umax\theta}{1-\theta}$ of its previous value.

In effect, they can issue $\frac{\$(1+Umax\theta)U_{max}\theta C}{1-\theta}$ after the first iteration.

3.12.2 Liquidity Trap

Details to be announced.

3.12.3 Trapped Currency

Details to be announced.

3.13 Assumptions

1. Ethereum will appropriately scale.
2. Unit of account will continue to be fiat for many use cases for the foreseeable future.

4 System variables

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, CUR and NOM will be used as abbreviations for Curits and Nomins considered as units of measurement.

Prices

$$P_c \qquad (\frac{\$}{\text{CUR}}) \qquad : \text{curit price.}$$

$$P_n \qquad (\frac{\$}{\text{NOM}}) \qquad : \text{nomin price.}$$

$$\pi := \frac{P_c}{P_n} \qquad (\frac{\text{NOM}}{\text{CUR}}) \qquad : \text{curit to nomin conversion factor.}$$

$$P_c' = f(V_n, V_v) \cdot R \qquad (\frac{\$}{\text{NOM} \cdot \text{sec}}) \qquad : \text{curit price rate of change.}$$

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

Money Supply

$$C \qquad (\text{CUR}) \qquad : \text{Quantity of curits, which is constant.}$$

$$C_e \qquad (\text{CUR}) \qquad : \text{Quantity of escrowed curits.}$$

$$N = C_N \cdot \pi \qquad (\text{NOM}) \qquad : \text{Quantity of nomins. This can float.}$$

$$C_N = \frac{N}{\pi} \qquad (\text{CUR}) \qquad : \text{Curit value of issued nomins.}$$

Ideally, $C_N \leq C_e$.

Utilisation Ratios

$$U = \frac{C_N}{C} \qquad \text{(dimensionless)} \qquad \text{: Empirical issuance ratio.}$$

$$U_{max} \qquad \text{(dimensionless)} \qquad \text{: Targeted issuance ratio ceiling.}$$

Ideally, $0 \leq U \leq U_{max} \leq 1$, but we need to work out a good level for U_{max}.

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

$$S_n \qquad (\frac{1}{\text{sec}}) \qquad \text{: average nomin spend rate}$$

$$S_i \qquad (\frac{1}{\text{sec}}) \qquad \text{: average issuance rate}$$

$$S_r \qquad (\frac{1}{\text{sec}}) \qquad \text{: average redemption rate}$$

Money Movement

$$V_n = S_n \cdot N \qquad (\frac{\text{NOM}}{\text{sec}}) \qquad \text{: nomin transfer rate.}$$

$$V_v = V_i + V_r \qquad (\frac{\text{CUR}}{\text{sec}}) \qquad \text{: nomin} \leftrightarrow \text{curit conversion rate.}$$

$$V_i = (C - C_N) \cdot S_i \qquad (\frac{\text{CUR}}{\text{sec}}) \qquad \text{: nomin issuance rate.}$$

$$V_r = C_N \cdot S_r \qquad (\frac{\text{CUR}}{\text{sec}}) \qquad \text{: curit redemption rate.}$$

V_i is assumed to grow as there are more free curits in the system. Actually perhaps it should grow with the number of escrowed Curits with no Nomins issued against them.

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

Fees

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

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

5 Alternative approaches

5.1 Basecoin

Description of system The Basecoin team appear to have mounted a somewhat a credible attempt to design a stablecoin, however we consider there to be a number of fatal issues that are discussed below.

The whitepaper at the time of writing is still in draft, with much of it actually dedicated to explaining why a stable cryptocurrency would be useful. Only a high level description exists of how the stablisation mechanism operates. 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.

5.1.1 Key issues

In the abstract, the paper indicates that Basecoin is “a cryptocurrency whose tokens can be robustly pegged to arbitrary assets or baskets of goods while remaining completely decentralized.” While the system might run on a decentralised computing architecture, it is inherently centralised due to the use of the oracle price-finding mechanism. The implementation and governance is also important for evaluating decentralisation, however no details are provided.

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 claims 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. Havven’s model by contrast employs agent-based computational simulations to demonstrate the viability of the cryptoeconomic system. It is also far simpler in that the system is designed with only open market arbitrage incentives to encourage a stable peg. In this way, a set of rational participating actors can stabilise the price of the stablecoin rather than a single set of smart contracts that attempt to develop complex algorithms for processes that are today managed by a combination humans and markets.

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.

Some of the criticisms levelled at alternative stablecoins seem hyper-critical; for example, "The only reason BitShares are worth 1 USD is because everyone believes it'll be worth 1 USD." We would like to see the Basecoin team re-examine their understanding and/or clarify their description here relating to the fundamental nature of money, as this is the very thing that makes all money work: everyone believes it has value and will continue to do so. Without this critical element, all monetary systems fail. This can be due to poorly applied monetary policies in the failure of fiat currencies, or it can be inherent flaws in the monetary system itself; for example gold was replaced by paper backed by gold due to the improvements in transportability and security this new system provided.

Further, while a significant devaluation of Bitcoin (relative to say, USD) is a possibility, we feel that comparisons that imply that Bitcoin may experience structural and cyclical devaluation are unhelpful. The USD is inherently inflationary, and so some level of inflation of the stablecoin in order to maintain a peg is necessary. The problem with using an appreciating asset as money is that it acts to damp economic activity in times of economic stress and cause exacerbations of macroeconomic turmoil. This is precisely why the gold standard was abandoned in favour of fiat last century. Even though the Havven system is backed by an appreciating asset, it doesn't suffer from the same critical flaw as traditional representative money (or intrinsically-valuable money), because the two-currency system is designed to follow any external price, and in the case of following USD, we have a currency that is inherently inflationary (follows the USD inflation rate), and so Nomins denominated in USD would also be inflationary by the same rate. In this way, Havven can achieve its goal of operating as a interoperability technology between fiat and cryptocurrencies and achieve its goal of accelerated adoption of this technology in a centrally-controlled and fiat-dominated world.

Of note, the whitepaper does not provide any implementation or performance considerations, including whether the system is intended to run on Ethereum or on a custom blockchain platform. This precipitates the obvious question regarding how such a decentralised system is paid for, as no mention is made within the whitepaper regarding levying fees or making use of fees to provide peg-supporting incentives.

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. Bitcoin and blockchain generally are often seen as anathema to centralised monetary systems, and we find it somewhat strange that the interventionist policies of quantitative easing (read vast money printing exercises) are praised in the paper. It seems there is a fundamental misapprehension of why fiat currency is still used at all given its long term tendency towards devaluation; it is solely due to legal tender laws enforced through the threat of violence. Hayek, quoting Nussbaum, "As one legal treatise on the law of money sums up the history of punishment for merely refusing to accept the legal money: 'From Marco Polo we learn that, in the 13th century, Chinese law made the rejection of imperial paper money punishable by death, and twenty years in chains or, in some cases death, was the penalty provided for the refusal to accept French assignats. Early English law punished repudiation as lese-majesty. At the time of the American revolution, non-acceptance of Continental notes was treated as an enemy act and sometimes worked a forfeiture of the debt.' "[2] The idea that people would accept a decentralised monetary system that could arbitrarily impose a tax on savings in the form of inflation is hard to imagine. 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 unclear 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.

It is worth explicitly clarifying that we are skeptical of any group that would advocate for monetary approaches that are diametrically opposed to cryptoeconomic efforts to democratise money. Clearly, Bitcoin is not a perfect solution, but 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.

5.1.2 Current state

Key issues

Current state

5.2 Tether

Description of system Tethers 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.

References

[1] Ferdinando M Ametrano. Hayek money: The cryptocurrency price stability solution. *Available at SSRN: https://ssrn.com/abstract=2425270 or http://dx.doi.org/10.2139/ssrn.2425270*, August 2016.

[2] Friedrich A Hayek. Denationalisation of money. *London: Institute of economic affairs*, pages 20–35, 1976.

[3] Tomaso Poggio, Andrew W Lo, Blake LeBaron, and Nicholas T Chan. Agent-based models of financial markets: A comparison with experimental markets. 2001.