Havven - A Stablecoin
v0.2

Anton Jurisevic, Samuel Brooks, Kain Warwick

October 2017

1 Introduction

Introduction.

1.1 What is money?

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 to the three functions money should ideally exhibit these characteristics; durability, portability, divisibility, uniformity, limited supply, and acceptability. Over the last few decades money has become almost invisble as payment technology has advanced, because of this it is often lost upon users of money that it is itself a technology. Money, like all technologies can be improved upon, in this case that means improving the perfomance of the three functions, or improving the six characteristics.

1.2 Bitcoin as money

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 support of a nation state from which to derive its value. The bitcoin supply is, therefore, not subject to control by a centralised entity. This fixed monetary policy means that increased adoption has tended to drive the price up over time allowing bitcoin 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 the Bitcoin system that can monitor or adjust to changing demand for the currency. Thus it has tended to be a poor medium of exchange and and 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 varied then it becomes less useful as a denominator of other goods.

1.3 What is a stablecoin

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 characteristics of bitcoin; transaction immutability, censorship resistance and decentralisation.

1.4 Why stablecoins

Cryptocurrencies, while in some ways a far better form of money, have been significantly hindered in their adoption by the fact that as decentralised systems they have had relatively inelastic internal monetary policies, thus 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. There are numerous structural and cultural reasons why stability has been somewhat ignored in favour of other challenging problems, these will be outlined later in the paper, but suffice to say we believe that significant research into stable monetary frameworks for cryptocurrencies is required.

Outline the current issues around why stablecoin (particularly the centralisation risks that Kain called out) ***I think we move this to a leter section.***

1.5 Intrinsic versus Nominal Stability

Stability is a complex goal, and there are many different approaches to acheiving it, but there is no question that a viable, autonomous and decentralised system that supports the issuance of an intrinsically stable token is a key element in the progression towards a dencentralised economy. Unfortunately while there is no evidence demonstrating this approach is not possible, such a system is still extremely challenging to design. Central banks have almost complete

discretion over their money supplies and vast numbers of man hours are expended in supporting the stability of state based fiat currencies and yet there are many examples where these efforts have failed utterly. Stability is far harder in cryptoeconomioc systems, because a cryptoeconomic system 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 such a sytem will be only functional within certain narrow parameters. This is not in itself neccesarily an issue, provided the paramters within which the system fucntions are well understood and the cost of destablising the system is sufficient such that the utility of the system outweighs the risks of participating in it.

With Havven we have accepted that such an approach is likely to be out of reach in the short term. If economists cannot agree on the optimal approach to monetary policy, it seems unlikely that a system contructed with the current state of knowledge could succeed in the long term. We have therefore, decided to take an alternative approach, to simply provide nominal stability by mapping the value of a stable token to an external currency, initially the USD. This significantly reduces the surface area of the system, since we do not need our stable token to be stable in and of itself, we only need it to be stable with respect to an external measure. So if the USD becomes subject to hyperinflation our stable token will be similarly impacted. The mechanism by which we achieve this is described below, but in short, we find the value for the entire system in USD and use the value of the system to issue a token denominated in USD backed by the collateral of system itself. We thus remove the need for the system to monitor demand for the currency, it must simply be able to determine the price of the entire system and ensure that the total value of circulating currency remains below some pre-defined threshold.

1.6 What Havven is designed to solve

Havven has been designed with two criteria in mind; not compromising decentralisation for stability, and to be stable only with respect to an external proven medium of exchange, not to itself be intrinsically stable. The first tenent should be fairly self evident to anyone who believes in the decentralised nature of blockchain. The second is predicated on the fact that so long as the world is dominated by fiat, a solution that demonstrates incremental utility over both fiat and existing cryptocurrencies as a medium of exchange will significantly improve crypto adoption. For the end user, whether a stablecoin is intrinsically stable or simply mapped to an external value is somewhat irrelevant. Thus we chose a path that represents an incremental technical improvement, but that when achieved will unlock a myriad of use cases currently not possible due to the limitations of the Bitcoin monetary policy.

1.7 Havven, a stablecoin

We intend to design a decentralised stablecoin; a cryptocurrency which can act as a medium of exchange due to it possessing a sufficiently stable price relative to other goods and services, but that does not require a trusted third party to maintain the stability of the system.

In his discussion of Hayek money, 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. [1] By contrast, governments, who 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. It should be possible however, 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 by selfish or misguided actors, or other issues commonly associated with inflationary forms of money. We should also seek to ideally 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.

Whilst we believe that ultimately such a system of intrinsic stability can be constructed, we see such an achievement as relatively far away from being implementable. As discussed above, we also believe that to the end user the distinction is somewhat irrelevant, we therefore take an approach which we believe will be far simpler to implement and model and that will result in practically the same outcome. Hence, we propose a system of two tokens which serve distinct purposes as a part of the Havven stablecoin system:

Curit The collateral token. Users who hold Curits take on the role of maintaining the system. The holders of this token are providing collateral for the stablecoin, and in so doing, assuming some level of risk. To compensate this risk, Curit-holders will be rewarded with fees the system levies automatically as part of its normal operation. The capitalisation of the Curits in the market reflects the system's aggregate value.

Nomin The stablecoin. The system intends the price of each Nomin to be stabilised in terms of some external, relatively-stable currency or commodity basket. Each holder of Curits is granted the right to issue Nomins, in proportion to the 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 freely trade them again. Other than price stability, the system should also encourage some adequate level of liquidity for Nomins to act as a useful medium of exchange.

Clearly, the introduction of a new cryptocurrency, in isolation, offers no additional value given the existing and established alternatives, such as Bitcoin and Ether. Havven then seeks to derive value from the addition of **stability** to its inherited properties as a modern cryptocurrency.

The Havven stablecoin system is akin to representative money in the sense that the fungible "Nomin" tokens of the Havven system 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 as we define Curits as carrying the functional value associated with being able to provide a stable medium of exchange.

However, Havven 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. Havven given that it does not need to act as the primary currency in the market 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 crypto, a hybrid of the two technologies and thus for numerous use cases superior to both. But it bears explicitly stating that whatever monetary policy is applied to the external value that Nomins are mapped to, will flow through to the system, such that if the USD is significantly devalued through inflation 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 stable currency issued (Nomins) is both denominated in and mapped to an external store of value. Throughout this paper we use USD as a the reference, however this could be any external and appropriately fungible asset, such as a commodity or fiat currency, (note, denominations in other cryptocurrencies are not necessary as these already benefit from the features Havven is implementing for the external denominator).

Nomins in the early stages of the system are anticipated to be used as a means to hedge against cryptocurrency volatility and as a settlement layer. For example, centralised cryptocurrency exchanges may use the Havven system to settle between themselves, expressing the value of the settled funds/assets in USD (for Nomins denominated in USD). Later, with greater maturity and scalability of Ethereum, Havven may be extended for more general purpose use.

1.8 Use cases for Stablecoins

USE CASES - Kain to add.

More information can be found on havven.io or by reading the position paper.

2 Functional description

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

2.1 Stability design considerations

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

- 1. Value stablisiation
- 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 both currencies, otherwise the value of both currencies would move 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 as that as described in Amentrano's paper on Hayek Money, is discounted on the basis that 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 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?
- *@anton What is this one?* Utilisation ratio needs to have distinct parts. Number of escrowed Curits is not quite the same as the number of issued nomins.
- 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?

2.2 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.

The 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.

2.3 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.

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.

(SGB: escrowing Curits and selling them for nomins by a Curit holder creates demand for when the holder needs to buy-back the nomins to get his Curits back. If we don't do this and hold the ether in reserve, we can automatically buy-back nomins much more efficiently. This is probably far more stable than having individuals control and possible holding onto the nomin supply, thereby creating large spikes in both demand and supply; a spike in demand could be felt when there's a run on Nomins to release Curits, this could be compensated for if other efficient market actors then escrowed their Curits to sell nomins at the higher price, but in the case that there are no more nomins to issue (all Curits are escrowed), the price of Nomins could skyrocket.)

2.4 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. [**?**].

Havven achieves this causal bridge to USD through market arbitrage; on the Havven decentralised exchange (hosted on Ethereum), both Curits and Nomins are denominated in ETH. Ether, in turn, is assumed to have some instantaneous value in USD on one or more external markets. In this way, we can avoid a trusted bridge and instead reduce our price-finding requirement to the minimum viable assumption that there will always be some external market for ETH in USD (or some other chosen denomination) and that market actors will seek profit through arbitrage.

This method is superior to using an Oracle service pushing the exchange rate

of ETH/USD at a regular cadence into the Havven decentralised exchange as it completely removes any risk associated with centralisation risks of such a process.

2.5 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?

Finally, we arrive at the simplest and most ideal solution, being 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 as we argue that the collateralised value exists in the Curit token.

SGB: Critical issue: fiat works because you cannot copy a country. Havven may not work because you can easily copy the source code and start your own. So there needs to be a great deal of effort expended to gain market traction. This is where the ICO comes in and an open-ended one could work the best.

The basis for Havven is an 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 of the crypto-assets chosen.

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 incorporates a special exchange (bridge) between fiat and Ether. This exchange is run as a not-for-profit by the Havven benevolent dictatorship. The price of Ether is then taken from this exchange and injected into the DEX (again, assuming scalability issues aside). The DEX then has an

authoritive Ether/USD value

=¿ what happens when this exchange is shutdown by the feds? The whole system collapses. You will always need some kind of trusted source of information for the exchange rate if the denominating asset is outside the system.

SGB: Volume of reserves is also problematic if one is just using the backing system as collateral - this collateral pool (i.e. value of the functionality of maintaining stability plus the value of the generated fees?) is small relative to the value of Nomins on issue (i.e. what happens if the price of nomins goes up but the value of Curits stays the same?)

Raised funds What happens with accumulated ICO funds beyond what is required to build and market the platform? Currently these do not "back" the platform; if the value of the fund moves, the value of Curits is insulated from this. Assuming that the value of funds raised far exceeds the funds required to build.

SGB: Perhaps these raised funds can be used to help stabilise the system in the same way that Basecoin does it. I.e. issue a small buyer of last resort function that perhaps takes a very small fee clip that adds to the collateral in reserve so that the system becomes more stable over time given the increasing reserves.

2.6 Approach

- Functionality of Curits and Nomins
- Initial Pricing of the value of the system:
    1. market-found (likely to be undervalued and grow into your value)
    2. pre-determined ($5b)
    3. Hybrid (capped ICO of a portion of the Curits at a value Haven specifies)
- 3. Ongoing pricing:
    1. Dex - current proposal.
    2. Rolling auction is still on the table.
    3. Oracle

This section will provide an informal treatment of the proposed market's structure and dynamics, while section 2 will scaffold out its structure with a little more formality, including the definitions of all the important system variables. If you see an unfamiliar symbol in section 1, look up its definition in section 2.

2.7 Investment incentives

Why would anyone buy Curits in the first place? A potential buyer of Curits 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.

2.8 Fees

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

- What are fees for?
- Who gets those fees?
- When can fees be levied?
- What macroeconomic effect does this levy have as a coin travels through the system?

The purpose of fees Fees will be redistributed to those who back the system, in order to incentivise people to capitalise it. The fee pool will be distributed periodically, for this purpose. However, if the system determines that the Nomin price is too low, then fees could be burned. If the price is too high then perhaps the system could sell these back into the system at a discounted rate.

Fee collection rate will also be a direct measure of the velocity of money in Havven. So it's in the interest of Curit holders to maximise liquidity in order to maximise their return.

Fee beneficiaries The previous assumption was that fees would simply be awarded to any holder of Curits. But then they get all the benefit with none of the 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 it it makes no sense to actually issue Nomins for any single player; so nobody will do it.

We must improve the marginal benefit of issuing Nomins into circulation in order to avoid this tragedy of the commons situation. So 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 is what levels to place these fees at. 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 place a clear limit on the ability of arbitrage to stabilise price. Lower fees allow tighter stabilisation, within a window exactly in proportion with the fee rates themselves.

2.9 Encouraging liquidity

It's desirable, when actors issue Nomins, that 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. 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.

However, considering Havven as it stands today, there is an important question hanging over the mission of increasing the money supply. What's to stop someone issuing their Nomins, and then just holding onto them? 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.

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?
Some level of Nomin liquidity above zero, where liquidity = flux = (average value).(average frequency). Consider also some optimum liquidity value above zero up to which diminishing returns are a factor.

The system may only ever be able to provide some level of stability within a set of thresholds (without actually backing the value of the token against the thing you're comparing it to, rocks, bottlecaps, USD.) This needs to be explicit.

2.9.1 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 Curits, fiat, crypto, otherwise?) 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.

2.9.2 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. So we will give every account 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). We don't like short cycles. We don't like isolated subgraphs. Would be cool if the money could go into the main connected component of the transaction graph as quickly as possible, then circulate in there with high velocity.

Definitions

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

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 nice 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.

2.10 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.

2.11 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.

2.11.1 Hyper-inflation

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 hope that is not the case.

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 some 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.

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 sufficienly 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 as 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.

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. Well, 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 runaway feedback loop? If it is, 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, but we will hand wave a little to try to get some feeling for how it *might* behave.

Let's assume the pool of agents following our strategy initially holds a fraction θ of the total supply of curits, value $\$C$. We will fudge a bit, and also assume linear demand, supply, 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.

TODO: Characterise the result of these assumptions w.r.t the value of held curits, issued nomins, and work out a formula for, given these price updates, how many curits, nomins and their value after n iterations of traversing the cycle

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

2.11.2 Liquidity Trap

2.11.3 Trapped Currency

2.12 Assumptions

1. Ethereum will appropriately scale.
2. Stability of existing cryptocurrencies will improve over time (declining utility of the stablecoin?).
3. Unit of account will continue to be fiat for most use cases for the foreseeable future.
4. The value of the platform is equal to the value of money raised in the ICO at that time. - the cost of developing the platform will be less than or equal to the amount raised.
5. Price discovery - internal exchange, mirrors external exchanges (prices Curits in nomins, based on the value of nomins in USD).
6. DEX follows external exchanges (arbitrage).

3 Qualitative Scenario Analysis

1. Ratio moves favourably 2. Ratio moves unfavourably 1. accumulate curits 1. few curits available: what happens? 2. no curits available: what happens? 2. accumulate nomis 1. few nomins available: what happens? 2. no nomins available: what happens? 3. Creation of new curits with new funds (not currently an option as the number of curits is fixed.)

4 Quantitative System Analysis

1. System Dynamics Modelling (sensitivity analysis, etc) 1. method 2. results

4.1 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	$(\frac{\$}{\text{CUR}})$	: curit price.
P_n	$(\frac{\$}{\text{NOM}})$	: nomin price.
$\pi := \frac{P_c}{P_n}$	$(\frac{\text{NOM}}{\text{CUR}})$	: curit to nomin conversion factor.
$P_c' = f(V_n, V_v) \cdot R$	$(\frac{\$}{\text{NOM} \cdot \text{sec}})$	: curit price rate of change.

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

Money Supply

C	(CUR)	: Quantity of curits, which is constant.
C_e	(CUR)	: Quantity of escrowed curits.
$N = C_N \cdot \pi$	(NOM)	: Quantity of nomins. This can float.
$C_N = \frac{N}{\pi}$	(CUR)	: Curit value of issued nomins.

Ideally, $C_N \leq C_e$.

Utilisation Ratios

$U = \frac{C_N}{C}$	(dimensionless)	: Empirical issuance ratio.
U_{max}	(dimensionless)	: 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	$(\frac{1}{\text{sec}})$	: average nomin spend rate
S_i	$(\frac{1}{\text{sec}})$	: average issuance rate
S_r	$(\frac{1}{\text{sec}})$	: average redemption rate

Money Movement

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

These quantities are the aggregated fees accrued by the system per unit time.

$Ag_{nx} \quad := V_n \cdot F_{nx}$	$(\frac{\text{NOM}}{\text{sec}})$	: fees taken from nomin transfers.

5 Alternative approaches

Outline the research to date done by Kain and why certain approaches were discarded.

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 supply (issuing new basecoin), and decreasing supply (auctioning of bonds), effectively acting like an autonomous central bank.

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 it might run on a decentralised computing architecture, it is inherently centralised due to the use of an oracle price-finding mechanism. We feel that this is a key weakness in the approach. This weakness is also implicitly recognised by the team in their discussion on how to implement an Oracle system in a decentralised fashion; whilst some discussion exists around various options for creating a pseudo-decentralised oracle, none are selected due to the fact that Oracles by nature are fundamentally centralised information bridges.

Basecoin is intended to operate "as a decentralized, protocol-enforced algorithm, without the need for direct human judgment. 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 amount of complexity required to be anticipated up-front 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 is far simpler in that the system is designed with open market arbitrage incentives to encourage the peg. In this way, a set of rational participating actors can discover 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.

Some of the criticisms levelled at alternatives seem to be unneccesarily hypocritical. 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 reexamine 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. 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 just in order to maintain a peg is not just neccessary, but actuallly desirable. The problem with using an appreciating asset to back a currency is that it acts to damp economic activity in times of economic stress, causing exaccerbations of economic problems. This is precisely why the gold standard was abandoned in favour of fiat last century.

Critically, the removal of Basecoin from the system to ensure the stable peg is predicated on the significant assumption that participants will take positions the ongoing bond auctions in order to remove basecoin from the system and support the peg. This assumption remains untested.

Of note, the whitepaper also does not provide any implementation or performance considerations, including whether the system is intended to run on Ethereum or on a custom blockchain platform. Further, this precipitates the question regarding how the 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.

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.

5.3 MakerDAO

Description of system MakerDao has been around for a relatively long time in the pursuit of a stablecoin.

Complex system.

Key issues

Current state Recently abandoned the Auction price-finding mechanism and are pursuing a

5.4 Nubits

Description of system

Key issues

Current state

References

[1] Ferdinando M Ametrano. Hayek money: The cryptocurrency price stability solution. 2016.