Preliminary Havven System Analysis

Anton Jurisevic

1 Discussion

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.

Significant questions

- Should fees only be given to those who have actually issued nomins?
- How do we incentivise people to even transfer stuff.
- Are transfer fees charged only nomins? Would people not then just try to convert to curits and exchange there?
- Utilisation ratio needs to have distinct parts. Number of escrowed curits is not quite the same as the number of issued nomins.
- Why not 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?

1.1 Restatement of Purpose

We would like to design a stablecoin; for any currency which is a viable medium of exchange must have a relatively stable price.

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, which mint their own currencies, very sensibly execute discretionary stabilisation policies that manipulate the circulating supply. This powerful and necessary lever is not available to Bitcoin and other supply-constrained currencies of its type; instead we propose a system whose monetary policy is algorithmically countercyclical rather than deflationary.

It should be possible by automatic means to incentivise issuance of tokens when they are demanded, and destruction when they are not. So, users of this prospective currency will be allowed to capitalise it, while the system automatically expands and contracts the money supply as its well of backing fluctuates in value. By this mechanism we might produce a more perfect currency whose supply floats with necessity, but which is not liable to debasement by selfish or misguided actors. Ideally we also remove some of the distortions of traditional monetary policy which, when it is expansionary, shrinks the purchasing power in every account which is not a direct beneficiary of that policy. In this fashion, we will provide two intertwined currencies which serve very different purposes.

Curit The reserve token, which users buy to obtain a part share in the entire system. The holders of this token are providing collateral for the system, 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 usual operation. The capitalisation of the reserve market reflects the system's aggregate value.

Nomin The exchange token. Philosophically, we would like the nomin to be a utilon, a constant unit of utility, and so the system should stabilise its price in terms of some external, relatively-stable currency or commodity basket, in order to insulate the nomin price from the volatility of its underpinning reserve. Each holder of curits is granted the right to issue their own nomins, in proportion with the value of the curits they hold and are willing to 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 just price stability, the system should also encourage liquidity, if nomins are to be actually-useful as a medium of exchange.

1.2 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.

1.3 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 upside 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.

1.4 Encouraging Liquidity

It's desirable, when actors issue nomins, that they are actually injected into Havven. 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?

1.4.1 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.

1.4.2 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 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

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

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 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.

1.5 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.

1.6 Failure Modes

1.6.1 Liquidity Trap

1.6.2 Trapped Currency

2 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.

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

References

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