Preliminary Havven System Analysis

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.

- Fees should only be given to those who have actually issued nomins?
- How do we incentivise people to even transfer stuff.
- 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 nomins when curits were redeemed?

1.1 Restatement of Purpose

We want to make a stablecoin in order to provide a currency which is a viable medium of exchange. Evidently, such a coin must have a relatively stable price. We will do this by allowing users to back it, automatically expanding and contracting the money supply as the well of capital fluctuates in value. To this end, we will provide two intertwined tokens.

Curits The reserve tokens, 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, assume some level of risk, but will be rewarded with fees the system levies automatically as part of its usual operation. The capitalisation of the reserve market reflects the value of the entire system.

Nomins The exchange tokens. 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. 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 beneficiaries

When fees can be collected 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 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 also charge punitive fees if a user is above the targeted utilisation ratio.

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. However, 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 behaving 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 issues nomins and then spends them, would be forced to buy nomins in the open market in order to redeem their escrowed curits.

But how to encourage a user to actually increase liquidity by buying goods with the nomins they hold?

1.5 Motility

We would like to encourage a user to spend their nomins. So we can give them a motility score and they are paid fees in proportion with the product of this score, and the number of escrowed curits they hold.

A user should not just be able to hold nomins and accrue fees. A user 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.

A user should not be able to cycle nomins through accounts they control and collect fees.

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

$$\begin{aligned} A &:= \text{The set of all accounts} \\ V_{a\to b} &:= \text{total value transferred from } a \text{ to } b \\ V_{a\to a} &:= 0 \text{ (accounts can't transfer to themselves)} \\ V_a^{in} &:= \sum_{p\in A} V_{p\to a} \\ V_a^{out} &:= \sum_{p\in A} V_{a\to p} \end{aligned}$$

We might interpret $V_{a\to b}$ to be the sum of the weights on the edges in the transaction multigraph corresponding to transactions between a and b.

We would like to know how likely a nomin is to be spent from a given account. Its motility should measure this.

We might try to measure the probability that a coin will be spent soon, if it resides in an account a. We will take $\mathcal{M}(a)$ to be the motility of a, which should estimate that probability:

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

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 from a to b of value $v_{a\to b}$ is made.

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

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

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

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

Although these updates should also influence accounts which have (transitively) transferred into a and p, 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:

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

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

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

1.6 Utilisation Ratio

1.7 Failure Modes

1.7.1 Liquidity Trap

1.7.2 Trapped Currency

2 System Variables

Money Supply

C	(curits)	: Quantity of curits, should be constant
$C_e = C \cdot U$	(curits)	: Quantity of reserved curits, i.e. the value of tokens have been issued against
$N = \frac{U_a \cdot C \cdot P_c}{P_n}$	(nomins)	: Quantity of nomins. This can float.

Utilisation Ratios We should work out a good level for U_{max}.

$U = \frac{P_n \cdot N}{C_e \cdot P_c}$	(dimensionless)	: Empirical issuance ratio.
U_{max}	(dimensionless)	: Targeted issuance ratio ceiling. Ideally, $0 \leq U \leq U_{max} \leq 1$

Prices These values are important, with the goal of stabilising the nomin price.

P_c	$(\frac{\$}{\text{curits}})$	: curit price
P_n	$(\frac{\$}{\text{nomins}})$	: nomin price
$P_c' = \alpha \cdot f(V_n, V_v) \cdot R$	$(\frac{\$}{\text{nomins} \cdot \text{seconds}})$	: R a risk term incorporating volatility? #buyers - #sellers?)

Fees

F_x, F_i, F_r (dimensionless) : transfer, issuance, redemption fees; these should be ratios, e.g. 0.1%

Money Movement

$V_n = S_n \cdot N$	$(\frac{nomins}{seconds})$	: nomin transfer rate
$V_v = V_i + V_r$	$(\frac{curits}{seconds})$	: nomin $\leftrightarrow$ curit conversion rate.
$V_i = (C - C_e) \cdot S_i$	$(\frac{curits}{seconds})$	: nomin issuance rate. Assumed to grow as there are more free curits in th
$V_r = C_e \cdot S_r$	$(\frac{curits}{seconds})$	: rate at which curits are redeemed in return for nomins (which are burned

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

S_n	$(\frac{1}{\text{seconds}})$	: average nomin spend rate
S_i	$(\frac{1}{\text{seconds}})$	: average issuance rate
S_r	$(\frac{1}{\text{seconds}})$	: average redemption rate