Havven: a stablecoin system
v0.3

Samuel Brooks, Anton Jurisevic, Kain Warwick

October 2017

DRAFT

Abstract

There is currently no effective decentralised unit of account. Previous attempts to create stable tokens have either relied on significant centralisation or have been undermined by their complexity. We present Havven, a representative money system which seeks to achieve price stability with respect to an external asset. Havven is a dual-token solution, composed of a stabilised exchange token and the reserve token which backs it. Users are incentivised to maintain this distributed reserve, and to manage the stable token supply so that it is in proportion with the value of the collateral. Because the collateral is encapsulated entirely within the system and distributed among its users, we remove the need for a trusted central authority. Such a stable cryptocurrency, useful for everyday economic purposes, will accelerate the adoption of distributed ledger technology.

Incorporate white paper criticisms.

Todo list

DRAFT

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 is an impressive technological advancement upon existing forms of money which simultaneously improves 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.

It is precisely its fixed monetary policy which has protected Bitcoin from debasement or devaluation, allowing it to outperform other forms of money as a store of value. Increased adoption has tended to drive the price up over time; unfortunately the fixed money supply has created the potential for short-run volatility, because there is no mechanism within Bitcoin that can 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.

DRAFT

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 volatility caused by the fact that as decentralised systems, they have tended to have relatively inflexible internal monetary policies. Hence stability continues to be one of the most valuable and yet the most elusive characteristics for the technology. Clearly, the ability to create alternative monetary policies within cryptoeconomic systems is still new,

and significant research into stable monetary frameworks for cryptocurrencies is required.

1.3 Havven

The Havven system is a novel form of representative money where there is no requirement for a physical asset, thus the problem of trust and custodianship is removed. The asset we use to back our stablecoin is the pool of reserve tokens, contained within the system itself. These tokens reflect participation in the system, and are a proxy for its value. Havven generates fees from users who transact in the stablecoin; and distributes them among the holders of the reserve token, compensating them for underpinning the system. Thus Havven rewards those who actively participate in maintaining it and charges those who passively utilise it. To maintain stability, Havven includes market incentives that manage the supply of the exchange token such that its price mirrors that of the asset it tracks.
Because we have created a system that generates cash flow for participants we now have an asset which has a defined market value and can be used as the collateral to support the stablecoin. The key to this is that the value of the system is measured in USD. This allows us to issue a stablecoin which can be presented and redeemed for a percentage of the collateral tokens valued at 1 USD. Backing a stablecoin in this way is beneficial because such a cryptoeconomic system does not require trust in a centralised party; each participant has full transparency over how many tokens have been issued against the available collateral at all times.

DRAFT

The two linked tokens and the complex of incentives for stability are defined below:

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. The nomin has value because it can be redeemed directly from the system for a fraction of curits worth 1 USD.

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 stability.

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, such nomin-issuers will be rewarded with fees the system levies automatically as part of its normal operation.

This issuance mechanism allows nomins to act as a form of representative money, where each nomin represents a share in the curit value held in reserve. Nomins derive value insofar as they provide a superior medium of exchange, and are effectively redeemable for a constant value of the denominating asset. In this paper, we use USD as this asset, but this could be any external and appropriately fungible asset, such as a commodity or a fiat currency.

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 prices change exogenously, then the system is designed to provide incentives for actors to counteract that change.

The Havven system is relieved of the obligation to respond to major macroeconomic conditions, as it benefits from the stabilisation efforts of large institutions acting in fiat markets. As Havven has the freedom to significantly overcollateralise its pool of circulating currency, it insulates itself against dramatic corrections in the curit market. Thus Havven acts as a bridge between fiat currency and cryptocurrency - a hybrid of the two technologies which possesses the advantages of both.

DRAFT

1.4 Rationale

In his discussion of Hayek money[1], Ametrano correctly makes the point that, due to its volatility and constrained supply, Bitcoin serves the purpose of crypto-gold much better than it does crypto-unit-of-account. By contrast, governments – which mint their own fiat currencies – can and do execute discretionary stabilisation policies to manipulate the circulating supply. This powerful lever is not available to Bitcoin and other supply-constrained currencies of its type, but a cryptocurrency whose monetary policy is algorithmically countercyclical rather than deflationary could inherit the desirable characteristics of both monetary paradigms. It should be possible to automatically provide incentives for the issuance and destruction of tokens according to demand. Users of such a currency would be allowed to back it while the system automatically seeks to expand and contract the money supply as its backing reserve fluctuates in value.

Clearly, 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: 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 cryptoeconomic technology.

DRAFT

2 Functional description

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

Address how to maintain baseline demand.

Address the role of the Havven foundation.

Outline basic verbs for market players.

Move analytical subsections from functional description section to the qualitative analysis and/or rationale sections.

2.1 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: Due to its constrained supply, and the intrinsic utility of the stablecoin that it backs, it's reasonable to assume that curits will appreciate in price.

Interest accrued from fees: If the price of curits stabilises for long periods of time, fees may be the only 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. Arbitrageurs might hold curits for a short time in order to pursue this strategy.

DRAFT

2.2 Fees

There are several key considerations with respect to fee design:

2.2.1 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 possibility would be simply to award fees to any holder of curits, but in this situation holders can get all the benefit without taking any risk. Although in the aggregate, it would be better for curit-holders 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 would not be incentivised to issue nomins at all. This is a classic tragedy of the commons.
In order to avoid this situation, we must improve the marginal benefit of issuing nomins into circulation. Hence, fees must be paid to those who *issue* nomins, not just those who hold curits.

Fee collection The system can charge fees whenever any value is transferred, or any state is updated. Different fee rates have different macroeconomic effects. 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 is also possible for fees to float. The fee schedule could be altered dynamically in order to stabilise the system. It is even conceivable that the system could set negative fee rates if it needed to and charge punitive fees if a user is above the targeted utilisation ratio. For 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. This would reduce demand and decrease the liquidity requirements.

Of note, fees are antithetical to arbitrage. The higher the fee, the higher the transaction friction, and the harder it is to make money by arbitrage. For example,

DRAFT

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.

2.3 Encouraging liquidity

It's desirable that when actors issue nomins they are actually injected into the liquidity pool for their intended use, rather than being held by the same actor in order to benefit from both the receipt of fees while retaining the option of using those nomins to rapidly 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 instantaneous option to liquidate their position and escape. On the other hand, an actor who had done the economically-desirable thing and issued nomins to the market would be forced to buy them back before redeeming their escrowed curits.

2.3.1 Non-discretionary Issuance

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

Conversely, when a quantity of nomins is burned, they must first be obtained from the open market. In this way, 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, thereby liquidating the user's curit position once the nomins 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. The result of this is 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.

DRAFT

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 external information. We recognise that a decentralised price-finding mechanism would be our preferred approach. Research into this mechanism is on our horizon, and future versions of this white paper will contain our results. However, in order to reclaim system performance, we can trade some of the trustlessness of the design, for example by a trusted "Oracle" service, which transmits knowledge of the external world into the system, building a causal link.

2.5 Utilisation Ratio

Even though rational actor modelling suggests that the price of nomins and curits will equilibrilate given that an agent may pay up to some multiple of the market value of a nomin in order to release escrowed curits, we are aware that there may be some prevailing macroeconomic or psychological influences relating to an undercollateralised position (i.e. if the value of the collateral pool is less than the issued stablecoin). As such, our modelling incorporates the notion of a "utilisation ratio" $0 < U < 1$, such that the system is over-collateralised in an attempt to counteract these potential issues. It may be that resolving an optimised utilisation ratio is beyond the ability of our agent-based modelling to determine, and as such, selecting this may need to be informed by the activity of a live system. Thus it is currently intended for Havven to initially include in its governance model the power to correct the utilisation ratio. This power can be removed over time as the system is proven, perhaps directly linked to some parametric milestones such as nomin velocity and stability.

DRAFT

3 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.

Game-theoretic modelling Discuss the structure of the game Havven represents, incorporating information the economists produce.

Discuss game theoretic modelling.

Agent-based modelling It has been observed that analytic methods are often difficult to apply in the complex and dynamic setting of a market. One suggested solution to this problem is *agent-based modelling*. Under this paradigm, we proceed by first defining rational agent behaviour and then simulating the interplay of those strategies over time. We seek to develop a more effective method of characterising market behaviour and equilibrium prices than pure analytic reasoning.[2]

Such simulations also provide an immediate means of measuring quantities of interest. Simply by observing the model, we can discover how varying input parameters affect system outputs in an experimental fashion. One important corollary is that this is a way of extracting reasonable settings for system parameters (such as fee levels) that might be difficult to reason about *a priori*. These systems, reactive as they are, also provide a method for testing proposed remedies for any identified failure modes.

Discuss that the game theory conclusions can be simulated

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

- Does the system stabilise its nomin price?
- Under what conditions can stability fail?
- What are reasonable initial settings for fees and other parameters?
- What effect does the utilisation ratio have on curit/nomin price ratio?
- What is an effective utilisation ratio?
- What is the effect of a direct redemption regime?
- What are the expected returns for curit-holders?

Fuller description of the technicals of the modelling.

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

DRAFT

4 Qualitative Scenario Analysis

This section provides a qualitative treatment of the reaction of the Havven system in response to various scenarios listed below:

Scenario analysis.

1. Ratio moves favourably
2. Ratio moves unfavourably
   - Accumulate Curits
     - Few Curits available.
     - No Curits available.
   - Accumulate Nomis
     - Few Nomins available.
     - No Nomins available.
3. Creation of new Curits with new funds (not currently explored).

List expected players in the market.

Outline incentives and actions for different players.

Address possible attacks against the system.

DRAFT

5 System variables

More complete system variable section.

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.

DRAFT

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 incorporating, 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.

$0 \leq U \leq U_{max} \leq 1$

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.

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

DRAFT

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

DRAFT

6 Alternative approaches

Establish a summary of arguments against each competitor

6.1 Basecoin

Description of system 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.

6.1.1 Key issues

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 states 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.

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.

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. 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

DRAFT

would be achievable and still able to handle monetary crises in a far future time without centralised intervention stretches credulity. It's not entirely clear 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. We are skeptical of any group that would advocate for monetary approaches that are diametrically opposed to cryptoeconomic efforts to democratise money, and we feel that 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.

6.2 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.

DRAFT

6.3 MakerDAO

Makerdao critique.

Description of system

Key issues

Current state

6.4 Nubits

Description of system

Key issues

DRAFT

Current state

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

DRAFT