HAVVEN

Havven: a stablecoin system
v0.2

Samuel Brooks, Anton Jurisevic, Kain Warwick

October 2017

1 Introduction

1.1 Money and Cryptocurrencies

There are three primary functions of money; to act as a unit of account, a medium of exchange and as a store of value. In addition, money should ideally exhibit durability, portability, divisibility, uniformity, limited supply, and acceptability. Money has become almost invisible over the past few decades as payment technology has advanced. Because of this, it is often lost upon users of money that it is itself a technology that can be improved. Specifically, this means improving the performance of our six desirable properties.

Bitcoin as a technological improvement on existing forms of money is impressive because it manages to simultaneously improve durability, portability, and divisibility. Further, it does so without requiring the enforcement of a nation state from which to derive its value. The Bitcoin supply is, therefore, not subject to control by any central authority.

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

Thus it has tended to be a poor medium of exchange and an even worse unit of account. In order for something to perform well as a medium of exchange or unit of account it must remain relatively stable against other goods and services, because money is ultimately a good that other goods are denominated in. If

the price of money as a good is too varied then it becomes less useful as a denominator of other goods.

1.2 Stablecoins

A stablecoin is a cryptocurrency designed for price stability, such that it can function as both a medium of exchange and unit of account. It should ideally be as effective for making payments as fiat currencies like the US Dollar, but still retain the desirable characteristics of Bitcoin; transaction immutability, censorship resistance and decentralisation.

Cryptocurrencies are in these ways a far better form of money, but have been significantly hindered in their adoption by the fact that as decentralised systems, they have had relatively inflexible internal monetary policies. Hence stability continues to be one of the most valuable and yet the most elusive characteristics. The fact that we have yet to achieve stability in cryptocurrencies without resorting to extreme centralisation should by no means be taken as evidence that this problem is insurmountable. The reality is that the technology to create alternative monetary policies within cryptoeconomic systems has only existed for a few years. Clearly, significant research into stable monetary frameworks for cryptocurrencies is required.

1.3 Achieving Stability

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

With Havven we have accepted that such an approach to building an *intrinsically* stable currency is likely out of reach in the short term. If economists cannot agree on the optimal approach to monetary policy, it seems unlikely that a system constructed with the current orthodoxies baked in could succeed in the long term. Instead we prefer simply to map the value of a stable token to that of the global reserve currency, the USD. In this way we provide *nominal* stability, by relying on the stability of the underlying fiat currency. This peg, stable as

measured with respect to a single external asset, is more achievable, though it has an obvious limitation: it is only as good as that external asset. For example, ff the US dollar is subject to hyperinflation, our stable token will be similarly impacted. However, we do not consider this to be a severe problem, given the historically greater stability of fiat currencies, and that any other asset can be trivially substituted for USD at any time.

1.4 Havven

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

Nomin The stablecoin itself, whose supply floats. Its price measured in fiat currency should be relatively stable. Other than price stability, the system should also encourage some adequate level of liquidity for nomins to act as a useful medium of exchange.

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

Each holder of curits is granted the right to issue a value of nomins in proportion to the USD value of the curits they hold and are willing to place into escrow. If the user wishes to redeem their escrowed curits, they must present the system with nomins in order to free their curits and trade them again. The holders of this token provide both collateral and liquidity, and in so doing assume some level of risk. To compensate this risk, nomin-issuers will be rewarded with fees the system levies automatically as part of its normal operation.

In this manner, the system incentivises the issuance and destruction of nomins so that the value of the nomin pool expands and contracts in proportion with the total value of curits backing them. If the curit price changes, then the volume of the token pool changes with it. On the other hand, if the nomin price changes exogenously, then the system is designed to provide incentives for actors to counteract that change.

1.5 Rationale

It seems clear that the introduction of a new cryptocurrency, in isolation, offers no additional value given the existing and established alternatives such as Bitcoin and Ethereum. Havven thus seeks to derive value from the addition of **stability** to its inherited properties as a modern cryptocurrency.

Havven is designed to provide a practically-useful medium of exchange, without compromising the decentralisation that cryptocurrencies offer. There are

many applications which Bitcoin's inherently-deflationary monetary policy and crypto's volatility make impossible. So any crypto-token which is able to demonstrate an increment in utility on these fronts over both fiat and cryptocurrencies will significantly enhance the uptake of cryptocurrency. For an end user, the means by which this is achieved is somewhat academic, but we hope that if it is achieved, we will have substantially improved the technology of money.

In his discussion of Hayek money[1], Ametrano correctly makes the point that Bitcoin serves the purpose of crypto-gold much better than it does crypto-unit-of-account due to its volatility and constrained supply. By contrast, governments – which mint their own currencies – can and do execute discretionary stabilisation policies to manipulate the circulating supply. This kind of powerful lever is not available to Bitcoin and other supply-constrained currencies of its type, but a similar system whose monetary policy is algorithmically countercyclical rather than deflationary could inherit the desirable characteristics of both monetary paradigms. It should be possible, by automatic means, to incentivise the issuance and destruction of tokens according to demand. In this way, users of such a currency would be allowed to capitalise it while the system automatically seeks to expand and contract the money supply as its backing reserve fluctuates in value. By this mechanism we might produce a more perfect currency where supply floats with necessity, but which is not prone to debasement and other issues commonly associated with either inflationary or deflationary forms of money. Ideally, we also seek to remove some of the distortions created by traditional monetary policy, which, when it is expansionary, shrinks the purchasing power in every account which is not a direct beneficiary of that policy.

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

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

will be able to be issued against that value, so long as they are denominated in USD.

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

1.6 Use cases for Stablecoins

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.

2 Quantitative System Analysis

We take the view that falsification is an important aspect of validating the Havven system. In our quantitative analysis we seek to identify failure modes of the system, and also to characterise not just *whether* Havven stabilises nomin prices, but *how much* it does.

It has been observed that analytic methods are often difficult to apply in the complex and dynamic setting of a market. One suggested solution to this problem is *agent-based modelling*. Under this paradigm, we proceed by first defining rational agent behaviour and then simulating the interplay of those strategies over time. It's hoped that this can often provide a more effective method of characterising market behaviour and equilibrium prices, when analytic reasoning fails.[3]

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

In sum, then, the modelling seeks to answer the following:

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

2.1 Modelling Havven

Environment

Agents

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

3 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 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.

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

4 Alternative approaches

4.1 Basecoin

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

The whitepaper at the time of writing is still in draft, with much of it actually dedicated to explaining why a stable cryptocurrency would be useful. Only a high level description exists of how the stablisation mechanism operates. Basecoin is described as operating similarly to Havven in that there is separation between a backing token and a transactional token, however Basecoin also separates out a specific "bond" token. The peg to an arbitrary external asset is maintained by using an oracle service to discover the price on an external market, before regulating the supply of "basecoins" through actively increasing (issuing new basecoin), and decreasing (auctioning of bonds) the supply, effectively acting as an autonomous central bank.

4.1.1 Key issues

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

Basecoin is intended to operate "as a decentralized, protocol-enforced algorithm, without the need for direct human judgment (sic). For this reason, Basecoin can be understood as implementing an algorithmic central bank." Whilst not without merit, this approach was discarded by Havven due to the high degree of design complexity required to be anticipated in order to ensure the stabilisation mechanism is effective. The paper claims that Monte Carlo simulations have been run which indicate stability under a range of scenarios, however details are yet to be released by the team. Havven's model by contrast employs agent-based computational simulations to demonstrate the viability of the cryptoeconomic system. It is also far simpler in that the system is designed with only open market arbitrage incentives to encourage a stable peg. In this way, a set of rational participating actors can stabilise the price of the stablecoin rather than a single set of smart contracts that attempt to develop complex algorithms for processes that are today managed by a combination humans and markets.

Another element not explored in the Basecoin whitepaper is the incentives for participants to engage with the cryptoeconomic system itself. While there is no

argument against the utility of stablecoins, there must be incentives inherent in all such systems to ensure the appropriate participation of all actors. In this case, there are consumers of the stablecoin and active participants in the monetary policy. It is critical to be able to demonstrate that the incentives within the system will ensure profitable participation strategies for actors. Without this being clarified it is unclear as to whether there will be uptake by enough users to generate sufficient currency in circulation to support the demand for a stablecoin. Critically, the removal of Basecoin from the system to ensure the stable peg is predicated on the significant assumption that participants will take positions in the ongoing bond auctions. This assumption remains untested.

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

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

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

peg-supporting incentives.

A final point needs to be made with respect to the overarching monetary approach espoused in the whitepaper. In the section "Averting Macroeconomic Depressions" the authors appear to support money printing and inflationary policies and the subsequent devaluation of currency. Bitcoin and blockchain generally are often seen as anathema to centralised monetary systems, and we find it somewhat strange that the interventionist policies of quantitative easing (read vast money printing exercises) are praised in the paper. It seems there is a fundamental misapprehension of why fiat currency is still used at all given its long term tendency towards devaluation; it is solely due to legal tender laws enforced through the threat of violence. Hayek, quoting Nussbaum, "As one legal treatise on the law of money sums up the history of punishment for merely refusing to accept the legal money: 'From Marco Polo we learn that, in the 13th century, Chinese law made the rejection of imperial paper money punishable by death, and twenty years in chains or, in some cases death, was the penalty provided for the refusal to accept French assignats. Early English law punished repudiation as lese-majesty. At the time of the American revolution, non-acceptance of Continental notes was treated as an enemy act and sometimes worked a forfeiture of the debt.' "[2] The idea that people would accept a decentralised monetary system that could arbitrarily impose a tax on savings in the form of inflation is hard to imagine. Even were it possible to demonstrate that inflation of the money supply via such a system would be effective in combating a deflationary spiral, a far better argument could be made that simply by implementing a stable store of value and unit of account that such a system would not be required. Generally, the apparent assumption that such a system would be achievable and still able to handle monetary crises in a far future time without centralised intervention stretches credulity. It's not entirely unclear why Basecoin has intended to merely replicate the function of a central bank, rather than aim for pure stability or a relative-stable approach such as Havven.

It is worth explicitly clarifying that we are skeptical of any group that would advocate for monetary approaches that are diametrically opposed to cryptoeconomic efforts to democratise money. Clearly, Bitcoin is not a perfect solution, but the proposal to intentionally create a systematically inflationary monetary system is not the answer. Instead, we should at this point in time be aiming to construct a system that provides a stable store of value relative to an arbitrary fiat currency. The macroeconomic benefits of such a system are clear, and for as long as we live in a fiat-dominated world this will continue to be the case.

4.1.2 Current state

Key issues

Current state

4.2 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.

4.3 MakerDAO

Description of system

Key issues

Current state

4.4 Nubits

Description of system

Key issues

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

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