A Market Determined Risk Free Interest Rate*

John Fletcher†, Ying Chan, and Marcin Wójcik‡

Cambridge Cryptographic Ltd

8 October 2021

Abstract

Decentralised finance has managed to replicate many facets of traditional finance, but a risk free interest rate on a decentralised (non-permissioned) *stable* asset has remained out of reach. Simply replacing 'proof-of-stake' with 'proof-of-deposit'[1] breaks the token security model. In this paper, we present a solution arising from a general framework that utilises not one, but two tokens in order to derive a nodes' influence in a consensus protocol.

1 Introduction

Consider an asset with *stable* value relative to some measure of the cost-of-living such as the consumer price index. Imagine that we wish to earn a return on a deposit of our asset, *without risking loss of principal*, and such that we can retrieve 100% of our assets at any time with certainty. We cannot simply turn to the market: if a borrower cannot take risk in order to generate profit with money we loan to them, why would they offer any interest in return? If the asset were cash, a central bank might offer a positive *risk free* return on demand deposits, but this is not at a *market determined* rate: it is centrally determined.

Nevertheless, a positive[2] *risk free interest rate* (sometimes called the *central bank rate*) on cash deposits is required because otherwise the economy would become unstable[3]. In the literature on non-permissioned digital currency, a lot of attention until now has related to the central banks' discretion over the base money supply, but relatively little to the short term central bank interest rate (risk free rate). This is despite the fact that the risk free interest rate is the most important parameter in an economy, as it fixes a lower bound for commercial lending rates.

In this paper we outline a mechanism for providing a risk free interest rate on a stable asset in a decentralised setting, such that the level of the interest rate is market determined. We begin with some informal definitions:

Stable asset *Stable* relative to the cost of living. Is suitable for use as money.

Risk free return Guaranteed return of the principal plus interest. Risk of loss of principal is considered negligible, and so the rate is deemed "*risk free*" for practical purposes.

Market determined Established through supply and demand.

There is currently no way to obtain a *market-determined risk free rate* on a decentralised *stable* asset. However, with the emergence of Bitcoin and related schemes [2], most notably the continuous generation of rewards for participating in a consensus protocol, several of the components would seem to already be in place:

*This work is the object of the following patent applications: EP20275088.1, GB2016187.3, GB2016186.5

†Email: john.fletcher@cambridgecryptographic.com

‡Signumx Ltd.

[1] We use the term proof-of-deposit for *stable* assets to emphasise that the purchasing power of principal is not "at stake".

[2] Typically substantial [1].

[3] Indeed, instability in recent decades is attributable to the central bank rate being persistently held too low.

(i) *Synthetic assets* [3]: For example, a synthetic basket of goods and services, or a synthetic version of a fiat currency, can provide a token which is a *stable* asset.

(ii) *Staking rewards* [4]: Rewards for participating in a consensus protocol employing proof-of-stake Sybil-defence, can provide a *risk free*[4] return on an *non-stable* asset.

(iii) *Delegated Staking* [4]: Delegation of *influence* (i.e. voting power) by a token holder, to a node. The token holder (the delegator) has zero risk of loss of principal, since control of the tokens is retained (only the associated influence is transferred). Through revenue sharing, this can in effect provide a *market determined risk free 'interest rate'* on an *non-stable* asset[5].

How can these components be combined in order to provide a market determined risk free interest rate on a *stable* asset? The solution is not as straightforward as replacing proof-of-stake with proof-of-deposit: this does not work because standard token security models (e.g. proof-of-stake, proof-of-storage, etc.) assume the token to be an *non-stable* asset. When staked, this *non-stable* asset provides Sybil-defence, creating an economic barrier-to-entry such that nodes can only attain substantial influence in the consensus protocol through substantial investment, and risk significant loss of purchasing power if they do not behave correctly. In other words, standard token security models assume the purchasing power to be "at stake" due to it being coupled to the value of the network (which is diminished if the network is disrupted). This no longer holds true with proof-of-deposit, where the principal is an asset which should maintain stable purchasing power under all but the most adverse of circumstances.

2 Related Work

Some proposals which have sought to provide a *risk free* return on a *stable* asset:

Dai savings rate. MakerDAO [5]. Is not *market determined* but rather voted on by holders of the MKR governance token.

xDai sidechain. Aspired to replicate something like proof-of-stake using a *stable* asset for staking [6, 7]. However, they were unable to do so because standard proof-of-stake security models assume that the price of the staked token is coupled to the value of the network.

Yield farming. Decentralised exchanges such as Uniswap [8] offer a return to anyone willing to provide liquidity. This includes liquidity between pairs of stable assets. However, the return will tend to zero as liquidity increases and a more *stable* peg is achieved.

3 A Two Token Scheme

Consensus protocols are typically designed such that the *influence* I (i.e voting power) of a participating node i is proportional in expectation to the revenue R accrued from block rewards:

$$I_i \propto E[R_i].$$

We denote *non-stable* asset which can lose purchasing power by a, and the *stable* asset (which maintains stable purchasing power) by b. The supply of *non-stable* asset and *stable* asset may fluctuate. This fluctuation may be especially pronounced for the *stable* asset, where the supply is subject to adjustment in order to maintain a stable peg. As such, absolute quantities of each token cannot in general be compared directly, and we therefore define unitless measures $\hat{a}$ and $\hat{b}$, where

$$\hat{a}_i = \frac{a_i}{\sum_{j=1}^{n} a_j}, \quad \hat{b}_i = \frac{b_i}{\sum_{j=1}^{n} b_j} \quad \text{and} \quad I_i = f(\hat{a}_i, \hat{b}_i). \tag{1}$$

The function f should be such that a node i, which attains substantial influence in the consensus protocol, risks significant loss of purchasing power if it does not behave correctly.

[4] We neglect technology risk such as the risk of successful exploitation of a software bug or technical malfunction.
[5] We assume no slashing.

Choice of function f

We have the following requirements:

1. Nodes should be incentivised to hold stakes of *non-stable* asset and deposits of *stable* asset, since the *non-stable* asset can serve as Sybil-defence, and a *risk free* return is generated on the *stable* asset[6].

   This means that function f needs to be monotonically increasing:

   $$\forall\, x, y \in \mathbb{R}, \quad \Delta x > 0, \Delta y > 0, \quad f(x + \Delta x, y) \geq f(x, y) \quad \text{and} \quad f(x, y + \Delta y) \geq f(x, y)$$

   A *market rate* of interest on *stable* asset can be determined by allowing nodes holding *non-stable* asset to bid for the influence conferred by delegation of *stable* asset.

2. Nodes should be incentivised to have a balance of *non-stable* asset and *stable* asset, or else nodes may opt to favour one of the assets over the other (such as if it is cheaper). If, for example, nodes were only to acquire the *stable* asset, then the *non-stable* asset would no longer serve as Sybil-defence. On the other hand, if all nodes choose to only acquire the *non-stable* asset, then a (risk free) return can no longer be generated on the *stable* asset.

   One way to incentivise the optimal balance is for function f to be symmetric, and maximised when a node holds both assets in equal proportions:

   $$\forall x, y \in \mathbb{R}, \quad f(x, y) = f(y, x)$$

   $$\text{For } \; x + y = constant, \;\; f(x, y) \;\text{ is maximised when }\; x = y.$$

A simple choice for f which meets the requirements is $f(\hat{a}_i, \hat{b}_i) = \min(\hat{a}_i, \hat{b}_i)$ where $\hat{a}_i, \hat{b}_i$ are defined by (1). We note that there are many possibilities for f, some of which allow for greater configurability.

4 Discussion

We expect that influential nodes will have significant holdings of *non-stable* asset. This is for the same reason that mining pools are most profitably run by large miners [9]. The incentives in our scheme are as follows:

(i) Nodes generate demand for decentralised *stable* asset as their influence in the consensus protocol (and consequently revenue) is contingent on attracting delegated deposits of stable asset.

(ii) Nodes compete for delegators by offering an interest rate on delegated deposits of *stable* asset.

(iii) Arbitragers satisfy demand for the *stable* asset. This generates demand for the *non-stable* asset.

(iv) Any price increase of the *non-stable* asset not only benefits nodes which hold the asset, but also enhances the effectiveness of staking the *non-stable* asset as Sybil-defence for the consensus protocol.

A *market determined risk free interest rate* on a decentralised *stable* asset offers a compelling reason to use decentralised *stable* assets over their centralised counter-parts. At the time of writing, Tether, a single centralised *stable* asset, has greater daily traded volume than all decentralised tokens (*stable* and *non-stable*) combined. Despite opacity around its reserves (or lack thereof), Tether even serves as collateral to a number of “decentralised” *stable* assets such as Dai [10]. On this basis, some have suggested that that “decentralisation” adds no significant utility to *stable* assets.

Our argument in favour of a decentralised stable coin is closely related to the reason why central banks offer a risk free interest rate in the first place: as a monetary policy tool which provides the means of controlling the level of debt (wide money) in a fractional reserve system by varying the level of the risk free rate [11]. We would like to reassure the reader that our scheme addresses concerns that provision of a risk

[6]The stable asset does make some contribution to Sybil-defence since it is in finite supply. However, the contribution is weak compared to that of the non-stable asset.

free rate of interest will *not* lead to mass capital outflows from commercial banks (a key justification for why central banks do not offer deposit accounts more widely). We defer discussion of this topic to our a later paper, as it relates to the role of sovereign currency and our proposed mechanism for allowing the market to discover the "price" of money [12, 13].

In summary, we have explained how a risk free interest rate can be provided on a stable asset in a decentralised (non-permissioned) setting. To our knowledge, this is an entirely new discovery. In a subsequent paper we consider the question of the *level* of the risk free interest rate under various market conditions. The question of the level of the risk free rate is important because it must be conducive to economic stability. For example, if the market dynamics were such that the risk free rate would tend to *fall* as a result of an unsustainable economic growth rate, this would *not* be conducive to stability. In fact, in such a scenario, we find that our proposed mechanism results in an increase in the risk free rate, and is consistent with a 'counter-cyclical' monetary policy.

References

[1] Paul Schmelzing. Eight centuries of the risk-free rate: bond market reversals from the Venetians to the 'VaR shock'. *Bank of England Working Paper*, 2017.

[2] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[3] Samuel Brooks, Anton Jurisevic, Michael Spain, and Kain Warwick. Synthetix white paper. https://www.synthetix.io/uploads/synthetix_whitepaper.pdf, (2018).

[4] Fahad Saleh. Blockchain without waste: Proof-of-stake. *The Review of financial studies*, 34(3):1156–1190, 2021.

[5] Maker DAO. Maker DAO white paper. https://makerdao.com/en/whitepaper, (2015).

[6] Andrew G. xDai sidechain. Technical report, xdaichain.com, 2021.

[7] Igor Barinov, Vadim Arasev, Andreas Fackler, Vladimir Komendantskiy, Andrew Gross, Alexander Kolotov, and Daria Isakova. Proof of stake decentralized autonomous organization. 2019.

[8] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core. Technical report, Tech. rep., Uniswap, 2021.

[9] Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolinsky, Aviv Zohar, and Jeffrey S Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, pages 919–927, 2015.

[10] MakerDao. Multi-collateral dai launches and introduces the dai savings rate. *https://www.prnewswire.com/news-releases/multi-collateral-dai-launches-and-introduces-the-dai-savings-rate*, 2019.

[11] Ray Dalio. *Principles for Navigating Big Debt Crises: German Debt Crisis and Hyperinflation (1918-1924); US Debt Crisis and Adjustment (1928-1937); US Debt Crisis and Adjustment (2007-2011). Detailed Case Studies.* Bridgewater, 2018.

[12] Friedrich August Hayek. The use of knowledge in society. *The American economic review*, 35(4):519–530, 1945.

[13] Adam Mann. Market forecasts. *Nature*, 538(7625):308–310, 2016.