A Credit Risk Free Yield on Stable Coins*.DRAFT

John Fletcher[†], Ying Chan, and Marcin Wójcik

Cambridge Cryptographic Ltd

April 13, 2022

Abstract

In this paper we present *Proof of Deposit.* This blockchain hosted mechanism provides a return on stable coins, at a market rate, *without the need to loan out such stable coins* (i.e. a credit risk free interest rate). Prior to this invention there was no known mechanism to provide a market determined, credit risk free interest rate on a price stable asset. This is significant because a market determined credit risk free rate can avoid the effect of time inconsistency with respect to the level of the rate.

1 Introduction

Consider an asset with stable value relative to some measure of the cost-of-living such as the consumer price index (CPI)—for example—this could be a fiat currency, or an asset that is pegged to the CPI. 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. In this paper we outline a mechanism for providing a credit risk free interest rate on a stable asset, such that the level of the interest rate is market determined. Our solution utilises public blockchain technology. (The first instance of which was Bitcoin [1].) We begin with some informal definitions:

Native token The token which is provides to validating nodes of a public blockchain network in order to incentivise participation. For instance, bitcoin (BTC) is the native token of the Bitcoin network.

Stable asset An asset that is pegged to another asset, or basket of assets. In our case, we add the condition that the asset to which it is pegged should be "external" to the system which hosts the stable asset.[1]

Stable coin A stable asset asset that is pegged to a benchmark such that it could be used as money. A suitable benchmark could be the cost-of-living, or a fiat currency.

Credit risk Risk that a borrower will not repay all or part of a loan, plus agreed interest.

Market determined Established through supply and demand between market participants through local (peer-to-peer) interactions. See for example [2].

Delegation (of stable coin deposit). Delegation of a stable coin deposit to a validator node of the network enables that node to earn additional rewards. The act to delegation does not require the deposit holder to transfer custody of the stable coin.

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

[†] Email: john.fletcher@cambridgecryptographic.com

[1] For example, if the system were the Ethereum blockchain network, a stable asset might be one which is pegged to the value of gold. It may not be one which is pegged the the value of the Ether token.

There is currently no way to obtain a market-determined credit risk free yield on a stable coin. However, with the emergence of public blockchain technologies, which feature the continuous generation of rewards for participating in a consensus protocol, several of the necessary components are available:

(i) *Decentralised synthetic (stable) assets* [3]: For example, a synthetic goods or services, or a synthetic version of a fiat currency (a stable coin), can provide a token which is a *stable* asset, and which does not depend upon a central issuer.

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

(iii) *Delegated Staking* [4]: Delegation of native token balances, to a validator node. The native token holder does not risk loss of principal, since custody of the tokens is retained (only the associated influence/voting power is transferred). Through revenue sharing, this provides a *market determined credit risk free* yield on an *non-stable* asset (the native token).

A market determined credit risk free interest rate on a *stable* asset cannot be realised simply by "staking" the stable asset in place of the (non-stable) native token: This does not work because standard token security models (e.g. proof-of-stake, proof-of-storage, etc), assume the value of staked token to be coupled to the value of the network (which is diminished if the network is disrupted), meaning that nodes risk significant loss of purchasing power if they do not behave correctly. In other words, standard token security models assume the purchasing power of the token to be "at stake". This would no longer be the case if the token were taken to be a stable asset, which should maintain it's peg 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:

xDai side chain. Aspired to replicate something like proof-of-stake using a *stable* asset for staking [5, 6]. 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.

Dai savings rate. Maker DAO [7]. Is not *market determined* but rather voted on by holders of the MKR governance token. Parameters decided by a collective decision making processes such as voting[2] are subject to time inconsistency [9]. For certain types of parameters such as interest rates, time inconsistency means that agents prefer ever lower values [10]. This is the reason why the Dai Savings Rate was voted down to zero, where it has remained for the past two years. A market determined rate can avoid the effect of time inconsistency.

3 A Two Token Mechanism

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[3]:

$$I_i \propto E[R_i]. \tag{1}$$

We weaken this condition, so that (1) need only be the case in equilibrium: See requirement 2, below.

Denote *non-stable* asset, which can vary significantly in 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

$$\hat{a}_i := \frac{a_i}{\sum_{j=1}^{n} a_j}, \quad \hat{b}_i := \frac{b_i}{\sum_{j=1}^{n} b_j} \quad \text{and} \quad R_i = f(\hat{a}_i, \hat{b}_i). \tag{2}$$

[2] Collective decision making also includes the case where the parameter is centrally determined by an entity which reflects popular sentiment to a significant degree [8, 2].

[3] Block rewards typically comprising the transaction fees from the transactions included in the block, plus any subsidy.

Choice of function f

We have the following requirements:

1. Nodes should be incentivised to hold (and/or have delegated to them) *both* stakes of *non-stable* asset and deposits of *stable* asset. In this way, the *non-stable* asset can serve as Sybil-defence, and a credit risk free return is generated on the *stable* asset[4].

   This means that function f should 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 compete for the revenue conferred by delegation of *stable* asset.

2. Nodes should be incentivised to have (delegated to them) roughly equal fractions[5] of *non-stable* asset and *stable* asset—in other words—there should be an equilibrium when nodes' hold/have delegated to them, equal fractions of each asset. If this were not the case, nodes may decide to favour one of the assets over the other (such as if one asset is cheaper to obtain). 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 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 maximum when a node has equal proportions of both assets:

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

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

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 (2). We note that there are many possibilities for f, some of which allow for greater configurability.

4 Discussion

The incentives in Proof of Deposit are as follows:

(i) Nodes generate demand for decentralised *stable* asset, as their revenue is contingent on attracting delegated deposits of stable asset.

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

(iii) Arbitragers satisfy demand for the *stable* asset as per a typical stable coin stability mechanism[6]. This generates demand for the *non-stable* asset, which increases its price.

(iv) Any increase in the price of the *non-stable* asset not only benefits nodes which hold the asset, but also increases security by contributing to Sybil-defence provided by the staked tokens.

A *market determined credit risk free interest rate* on a decentralised *stable* asset offers a compelling reason to use decentralised *stable* assets over their centralised counter-parts, such as the Tether stable coin (USDT). At the time of writing, Tether has a higher daily traded volume than all other 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 [12].

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

[5] As a fraction of the total quantity of that token outstanding. See Definitions (2).

[6] See for example [11].

References

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

[2] James M Buchanan. Individual choice in voting and the market. *Journal of Political Economy*, 62(4):334–343, 1954.

[3] Michael Spain Kain Warwick Samuel Brooks, Anton Jurisevic. 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] Andrew G. xDai sidechain. Technical report, xdaichain.com, 2021.

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

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

[8] Jon Elster. *Ulysses unbound: Studies in rationality, precommitment, and constraints*. Cambridge University Press, 2000.

[9] Finn E Kydland and Edward C Prescott. Rules rather than discretion: The inconsistency of optimal plans. *Journal of political economy*, 85(3):473–491, 1977.

[10] Guillermo A Calvo. On the time consistency of optimal policy in a monetary economy. *Econometrica: Journal of the Econometric Society*, pages 1411–1428, 1978.

[11] Celo. Stability Algorithm (Mento). https://docs.celo.org/celo-codebase/protocol/stability/doto, 2022.

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