Decentralized growth coin: designing a low volatility investment cryptocurrency protocol

Pavel Krolevets[1]

[1]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, China*
pavelkrolevets@sjtu.edu.cn

November 29, 2019

Abstract

Nowadays cryptocurrency becoming widespread and blockchain technology is taken seriously by global banks and community. There are significant variety of cryptocerrency assests have appeared after success of Bitcoin and Ethereum. Stable coins like USDT ans Dai provided so long anticipated fiat money replacements in the cryptocurrency. However, there rapidly changing financial landscape demands for a new type of blockchain transferable means which will play a role of low risk investments, filling the gap between high volatility original cryptocurrency and stablecoins. In this paper we making an attempt to bridge computer science and economics, fostering transfer of expertise. The proposal of this work lies within the uncomfortable middle ground between money definition, cryptographic algorithms, game theory, and unfamiliar paradigm shifts.

As the result, we propose another kind of decentralized cryptocurrency protocol - low volatility growth coin which can be used as a safe investment and a direct competitor for bank deposits or bond investments, accompanied with stablecoin and high volatility asset.

1 Introduction

Blockchain technology is changing the landscape of financial industry by providing new

possibilities of automation, security, and trust. Success of the first cryptocurrency Bitcoin proved that a long term cryptographical dream can materialize and be a mean of decentralized cryptocurrency. A successor, Ethereum paltform went further and provided a new type of decentralized computaton and storage - blockchain based virtual computational machine which can be used to execute the code in the decentralized manner. An impact to financial industry is unarguably significant. Financial industry received new ways of processes automation and decentralization.

We are not going to dig deep into the history of cryptocurrecncy and blockchain as we assume a reader already familiar with it. For those who want to refresh their memory or learn about the history of digital cash protocols and final appear of cryptocurrency can refer to [2, 3].

Any financial system cannot exist without stable low volatility assets. Very high volatility of cryptocurrency is a one of the main problems preventing it of wide use. As a attempt to solve this problem a price stabilized cryptocurrency was introduced which is pegged to the price of a fiat currency, creating a layer on top of the existing monetary system.

Pegging cryptocurrency to fiat currency inherently has problems. First, it affected from the decisions of the Central bank and, therefore, cannot be claimed absolutely decentralized despite of the underlying protocol of the stablecoin. Second, it can affect effectiveness of the Central bank monetary policies if the stablecoin accumulates significant capitalization. In this case it can be subject of the additional regulation.

This paper is organized as follows. In Section II, we review price stabilization mechanisms. In Section III, we describe a design of a non-collateralized low-volatility growth token protocol. In conclusion, we summarize the meaning of this paper and state challenges for the future. This is the first survey ofstablecoins to the best of our knowledge.

2 Preliminary

2.1 Stablecoins

Stablecoin - is a blockchain cryptocurrency with a price stabilization mechanism. Usually its pegged to an exchange rate of a real asset like USD, but there are attempts to peg the price to gold [1]

The first of its kind stable crypto-asset pegged to USD fiat currency (Tether) was introduced in 2012 by J.R. Willett [13]. Its main idea was to create a pool of real assets and issue an equal amount of cryptocurrency tokens with the promise to exchange this tokens to real assets at any time. The demand and anticipation for such an asset was very high and it had a quiet a success despite the fact that it uses collateral as a price stabilization mechanism and, therefore, centralized.

As an attempt to create the first truly decentralized stable criptocurrency in 2014 Maker DAO team introduced Dai (formerly called eDollar) stable coin pegged to USD [12]. This system is built on a set of smart contracts and keeps a soft peg to USD real currency by supply/demand forces coming from Dai creators who is basically margin borrowers and a collateral is their cryptoassets. Maker Team also introduced a decen-

tralized way of creating an oracle to determine current cryptoasset exchange rate to keep overall system margin above set level.

Dai protocol approach suffers from a margin call problem in case of severe asset price depreciation or speculative economic attack. The design of the protocol allows a decline of the underlying collateral (Ethereum cryptocurrency) to the level not lower than 80 percent. In this case a global margin call is initiated and all operations are halt till the decentralized owners of the system make an action. This theoretically minimizes the risk of system shutdown and loss of the collateral, but it has never been tested in real environment and still raises some questions. Another problem which Dai protocol suffers is overcollaterization.

2.2 Price stabilization mechanisms

At the top level we can classify price stabilization mechanisms to collateralized and non-collaterized. In the former there is no real asset exists to link to value of the token. Also its possible to classify non-collaterized price stabilization mechanism to protocol layer and application layer [6].

2.2.1 Tokenization of collateral (application layer)

A. Direct collateriziation mechanism is, probably, one of easier to understand. It is well studied and often used in real world applications. The main idea is to provide a frictionless means to exchange of some reprezenation of an asset (token) to the asset itself. A collateral can be any real asset, like currency, gold, oil, etc. This is used by some degree of success by Tether stablecoin [13].

However, this approach has a significant amount of detriments:

- require some degree of centralization, a trusted third party is needed to manage the funds
- frictionless market transactions is impossible to achieve
- high degree of counterparty risk
- low protection against economic speculative attack

B. Proxy collateriziation is a type of collaterized mechanism, but instead tokens are linked to the price of another cryptocurrency or a backet of assets. This can help mitigate some of the detriments of direct collaterization and allow more decentralization as counterparty risk can be eliminated, but it suffers from different types of risks:

- oracle problem. The trusted mechains needed to determine the price of a proxy asset. This is difficult to implement because of limitations on blockchain interaction with the real world.
- difficult to maintain a peg to a proxy with high volatility like Bitcoin
- risk of undercollaterization

C. Self-collateriziation. This is a form of proxy collaterization, but the stabilized token is backed by the underlying cryptocurrency. Exhibits mostly similar problems as proxy collaterization.

D. Interest rate mechanism. In this approach interest rate on loans and deposits is used to control the price of a token. Demand for tokens comes from loans which is created from proxy cryptocurrency. Users lock proxy cryptocurrency to mint new stabilized tokens. They are free to use these tokens while not loosing the ownership of original proxy token. Basically they create a collaterized loan. The interest they pay for this loan is *stability fee*, which is controlled by the governance of the system. The higher a stability fee the less loans are created, decreasing the supply of stabilized tokens. When there is a need to decrease the supply, interest rates on loans increased and less tokens are supplied. When users want to take their collateral back, they return stabilized coin and pay the stability fee. An oracle is used to determine equality of amount of stabilized tokens in the system to the value of the collateral. Margin call is used to *Maker Dai* is the first successful project which uses this stabilization mechanism [12]. Its worth to mention, that in decentralized settings its difficult to implement undercollaterized loans when future income can be taken as a collateral. In [9] authors argue that its impossible to implement in permisionless cryptocurrency because of general anonymity of identities and vulnerability for Sybil attacks.

Problems which this approach suffers from:

- oracle problem. To determine the value of the collateral an oracle is required, which makes it susceptible to an attack on oracle or data providers.
- margin call as mechanism to control the risk of undercollaterization.
- generally a need in overcollaterization for stability of the system.

2.2.2 Open market interventions (application layer)

In this technique a direct market interventions are used to adjust the price of a token. When demand increases new tokens are provided in exchange for the pegged asset and the reserve is created. On the other hand, tokens are bought back from the market using a reserve to affect token price. This approach is naturally centralized to some degree as there should be a central authority to stabilize the price of the token. This approach is mimicking the Central bank operations when it sells or buy treasuries on the market to increase/decrease of the money supply and based on . Seigniorage shares [11] approach falls to this section, because it when supply expands, shareholders of the system receive new stablecoins, otherwise there are new shares issued, which are paid back when there is an expansion. Basecoin [7] project is an example of this type of the protocol.

2.2.3 Block rewards and transaction fees (protocol layer)

It is also worth mentioning that economical principles of asset price appreciation are embedded to Bitcoin [8] and Ethereum [4] protocols through increase in computational complexity in Proof-of-Work consensus algorithm and consequent decrease in supply. For example, PoW consensus algorithm adjusts difficulty of a block creation based on the speed of successful mining, keeping supply limited depends on speed

of mining . However, these protocols don't take in consideration market demand of the underlying token, that can lead to high volatility of the token value. Some research attempts exist to solve this problem and implement techniques to stabilize underlying cryptocurrency exchange rate [10].

2.3 Motivation

Financial system cannot function properly without low volatility low risk assets. They play a major role in risk management and stabilization of the system. In newly formed alternate world of cryptocurrency finance there is a significant lag between types of crypto assets and real world assets exist. Such a constantly growing token would form a building block for the crypto financial system. Stable coins, which pegged to a real fiat currency, appeared just recently. But there are no low volatility, stable growng token present. In this paper we aim to design such a protocol which can be used later for more sophisticated applications.

2.4 Related work

Maker team [12] made an attempt to create a non-collaterelized stablecoin system pegged to US dollar using interest rate price stabilization mechanism. In their protocol design they created a kind of growth (MKR) token which value appreciates based on inflow from fees gathered from leveraged creation of a stablecoin Dai.

Exeum is another attempt to create a stablecoin system..... [5]

3 Protocol design

In the creation of low volatility growth coin we need to be very clear about what we are trying to achieve and the role it will play in the crypto-financial system. Stablecoins play a significant role in stabilizing cryptocurrency market, but there is no value appreciation mechanisms embedded to use it as a safe investment vehicle. Therefore we can define goal we are trying to achieve:

1. Continuous value appreciation based on pure market forces, not market manipulation.
2. Low price volatility. Comparable to other stablecoin protocols.
3. Stability of the system in the case of catastrophic cryptocurrency market moves.
4. Robustness of the system to all types of adversarial attacks: security, governance and speculative attacks.
5. Decentralization of the protocol.

Lets define market forces which can drive value appreciation of the token. There are several types of market forces which can drive value appreciation of the token:

- *Dynamic and constant decrease in supply*

  In this case we should dynamically keep supply of tokens less than demand, but control it adequate to market environment. This approach doesn't seem sustainable as its not clear how to drive value appreciation in the case of constant low demand.

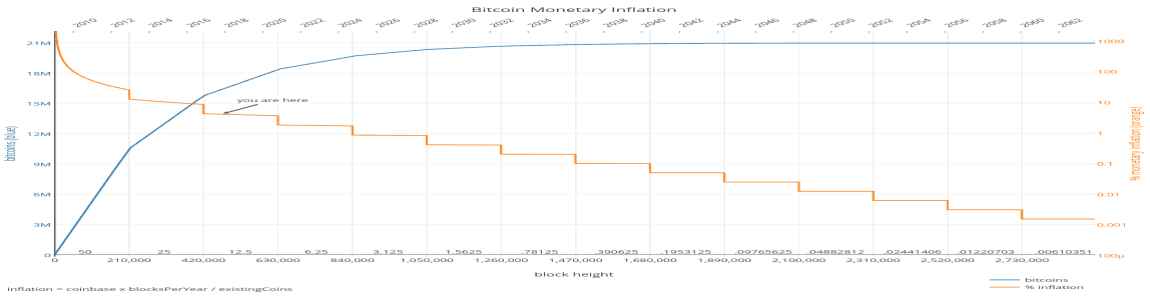

Figure 1: Bitcoin inelastic sypply (source: http://bashco.github.io/)

Moreover, its difficult to implement price stabilization mechanisms and unclear which role this token will play.

- *Open market interventions*

  This approach doesn't seems sustainable also, as it artificially affect the price of the token and requires some authority to sell and buy tokens on the open market. Moreover, there is a limit in which market price can be affected which depends on the reserve amount devoted for market interventions.

- *Interest rate on borrowing*

  This approach based on the principle in the real economy when the Central bank lend/borrow money effectively increasing and decreasing supply. Also, there are speculators, who use leverage to speculate on the price of the asset and ready to pay interest on the leverage they create. In this case, the value appreciation of the token can have a more sustainable source, but other mechanisms like market interventions can be used for stabilization of the token.

As we postulate that the main driving force in the cryptocerrency finance is interest rate on borrowing for marging speculating, as there is no Central bank present and no inflation is observed. Some form analogues to the Central bank can be implemented through decentralized governance system. This type of monetary cryptocurrency system can be called private comparing to the existing Central bank monetary system. As the Central bank target inflation by manipulating money supply through the interest rate and direct interventions with interest bearing instruments, the private system can take this principle as a basis and adjust for decentralized governance settings, effectively producing interest bearing token and a relatively stable pegged token.

We are going to refer to Maker DAO project [12] where two types of tokens are used, a pegged to USD token Dai and a governance share token MKR. In our case the most interest is lies in the governance token, which by design should appreciated in value based on fees are taken from the system for taking the risk of global margin call. ***In contrast of this approach we are going to focus on both - the governance token and the pegged token and try to***

link it to the modern monetary theory [14].

Main parts of the system from the high level perspective:

- *Decentralized lending mechanism* (similar to Maker Dao [12]). Enables third parties to borrow funds from the system using native token.
- *Decentralized governance subsystem.* Should be an effective voting system in place to get votes from the main stakeholders. Will represent a decentralized central bank system. The governance system based on the voting mechanism of the main stakeholders. At the end of each epoch token holders will have a right to vote on the main interest rate set in the system. Because, the growth token is freely traded on the market, to get a vote right they should hold it at least a full epoch.
- *Oracle subsystem* to gather information about pegged currency exchange rate, CPI and other required indicators.
- *Price/volatility stabilization subsystem* for the pegged and growing tokens.
- *Reserve subsystem and safety mechanisms.* The reserve system represents the collateral and acts as a guarantor for the main users and stakeholders.
- *Security monitoring/enforcement subsystem.*

The core mechanism of the system is the global interest rate on lending to other cryptocurrency market participants, similar approach is taken by Maker project, but with novel contributions discussed further.

We can distinguish three main stakeholders in the system: users interested to invest in low volatility/risk cryptocurrency asset and get passive return; main stakeholders of the system responsible for the governance; users of stabilized cryptocurrency pegged to real-world currency; borrowers from the system (usually active traders).

The system has three main types of tokens freely circulating on the market:

- Bond-like token, which value appreciates constantly with low volatility.
- Pegged to real currency token (USD).
- System utility token.

System description:

Borrowers from the system generates new pegged to real-world currency tokens by creating a collaterized debt position by sending their cryptocurrency (Bitcoin, Ethereum, etc.) to a smart contract. The smart contract locks assets as a collateral and generates pegged tokens in the amount equals to 0.5 of the collateral value to keep a leverage at 1.5 level. To close this borrowing position and receive back collateral borrowers should send created tokens back to the smart contract.

The borrowers pay a fee determined by the global interest rate, which is set through the decentralized governance system. This will affect the demand to our target growth token, which represent an alternative to treasury bonds, but is perpetual, accumulates interest in the form of value appreciation. Users of the system will buy this growth token in the open market creating

a reserve which will be carefully monitored by the stakeholders and stabilization mechanisms. High level system design and economics is presented in figure 2.

3.1 Decentralized governance system

4 Collected reusable garbage

Three functions of money:

- Unit-of-Account
- Medium-of-Exchange
- Store-of-Value

market forces which will affect this type of growing stablecoin.

As a result of the protocol we are going to create thee types of tokens: stablecoin pegged to USD, low volatility growth token based on interest rates in the system, and a share token.

References

[1] Shaun Djie Anthony C. Eufemio, Kai C. Chng. Digix white paper: The gold standard in crypto assets. Technical report, 2016.

[2] Andreas M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, 2017.

[3] Andreas M. Antonopoulos and Gavin Wood Ph. D. *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media, 2018.

[4] Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform, 2014. Accessed: 2016-08-22.

[5] Jaehyung Lee and Minhyung Cho. Exeum: A decentralized financial platform for price-stable cryptocurrencies, 2018.

[6] Makiko Mita, Kensuke Ito, Shohei Ohsawa, and Hideyuki Tanaka. What is stablecoin?: A survey on price stabilization mechanisms for decentralized payment systems. *CoRR*, abs/1906.06037, 2019.

[7] Lawrence Diao Nader Al-Naji, Josh Chen. Basis: A price-stable cryptocurrency with an algorithmic central bank. Technical report, 2017.

[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.

[9] Ingolf G. A. Pernice, Sebastian Henningsen, Roman Proskalovich, Martin Florian, Hermann Elendner, and Björn Scheuermann. Monetary stabilization in cryptocurrencies - design approaches and open questions, 2019.

[10] Kenji Saito and Mitsuru Iwamura. How to make a digital currency on a blockchain stable. 2018.

[11] Robert Sams. A note on cryptocurrency stabilisation: Seigniorage shares. 04 2015.

[12] Maker Team. The dai stable coin system. Technical report, Maker DAO, 2017.

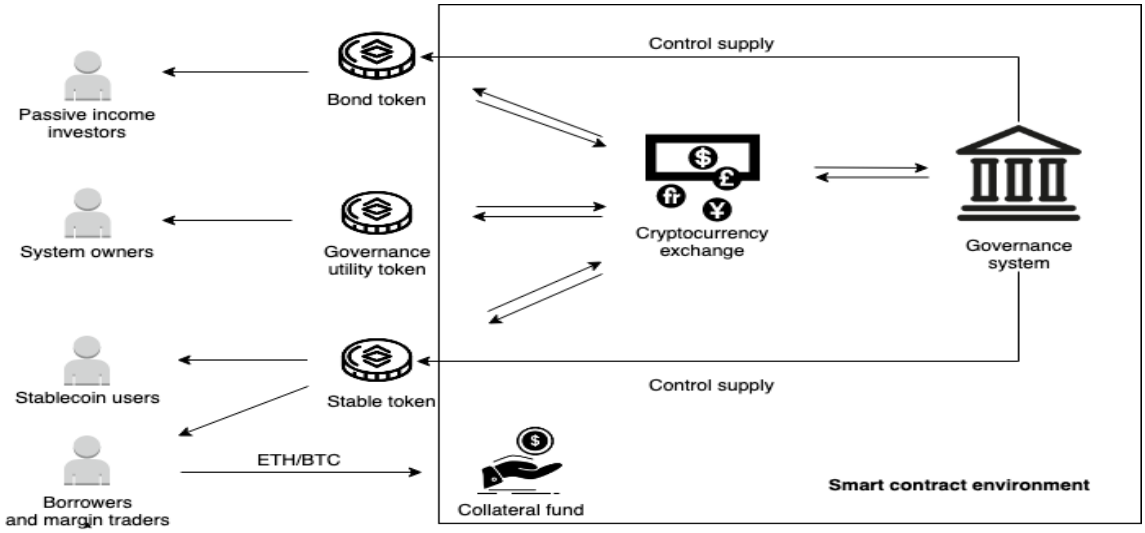

Figure 2: General schema reflecting participants: passive income investors)

[13] J.R. Willett. Tether: Fiat currencies on the bitcoin blockchain. Technical report, Tether Limited, 2012.

[14] L. Randall Wray. *Modern Money Theory: A Primer on Macroeconomics for Sovereign Monetary Systems*. Palgrave Macmillan, aug 2012.