A Survey of Techniques for Cryptocurrency Pegging, Financial Derivatives and Price Stabilisation on the Blockchain

true

November 26, 2019

Abstract

Stablecoins are hot in the crypto space. With the 5th largest cryptocurrency and stablecoin Tether, now the subject of a trillion dollar lawsuit, many look to other stablecoins as a safe store of value. The techniques used by these coins vary massively. This survey discusses techniques used by the largest and most promising stablecoins to hold a stable value.

1 Introduction

Centralisation, non-transparency and a trillion dollar lawsuit would normally lead to crypto investors avoiding you like the plague. For Tether however it lead to a market cap of over 4 Billion dollars. With Tether currently being the most the most traded cryptocurrency despite its controversies we are left to wonder what makes a coin that trades at 1 dollar so attractive to investors.

Cryptocurrencies have so far been notoriously volatile in price. Making the assets unsuited for both investments in the long term, and payments in the short term.

Another need for price-stable currencies exists among crypto traders. When the crypto-markets decrease in value, the entire market tends move as a whole. In this case traders want to move their assets out of the volatile "new world" assets and into traditional currencies like the Dollar to wait out de dip in de market. However these transactions are limited by the speed of the old payment networks. A coin that is stable with respect to the US Dollar would solve this problem by allowing traders to change positions between the Dollar and crypto currencies in a quick, decentralised[@Money_as_IOUs_in_Social_Trust_Networks] and programmable [@TrustChain] way.

With Tether having proves the need for a stablecoin, many cryptocurrencies have followed, some solving problems of those who have come before. MakerDAOs

DAI [@MakerDAO:whitepaper], currently the 5th biggest stablecoin and the 52th biggest cryptocurrency with a market cap of 103 million USD, aims to be a fully decentralised stablecoin that maintains a value of 1 USD. Dai provides a coin that enables distributed peer-to-peer lending with the stability of the Dollar while having no centralised component.

MakerDAO is part of a bigger movement. The Decentralised Finance movement is an open community of decentralised financial platforms that aims to revolutionise the financial world by replacing many of the worlds financial systems. Within this project there are a number of stablecoins and other tokens that are pegged to real world assets that use decentralised techniques for providing financial derivatives.

This survey presents a history of the significant stablecoins and pegged assets invented so far, and classifies and generalises the techniques that are common among them.

First we discuss the topic of the purpose of money, the meaning of value and stability, and some currency pegs used in our traditional monetary system in Chapter 2. We then describe the simplest and most successful stablecoins, namely the centralised coins in Chapter 3. In Chapter 4 we go into the more complex topic of decentralised assets and their methods for maintaining pegs to real world assets without a central party guaranteeing the peg. We then go deeper into the theory in Chapter 5 where we look at the research into the viability of stablecoins. We then end with a discussion of the research on stablecoins in Chapter 6 and a conclusion of the survey in Chapter 7.

2 Background

Before we get to the techniques used for stabilisation some concepts and terms need to be defined. In this chapter we define the purpose and requirements of money. We define what it means for a currency to be stable, and what it means for a currency to be collateralised.

2.1 The purpose of money and the requirements of a stablecoin

In "On the Origin of Money" [@On_the_Origin_of_Money] Karl Menger describes how people settle on a currency as a method of exchange. He describes that the willingness of people to exchange their goods for a commodity depends:

1. Upon their ability to trade it for goods (demand)
2. Upon the scarcity of the commodity (supply)
3. Upon the divisibility, durability and practicality of the commodity.
4. Upon the development of the market, and of speculation in particular.

5. Upon the limitations imposed politically and socially upon exchange, consumption and transfer from one period of time to another

2.2 The meaning of value and stability,

An certain configuration of these factors is required for a stable store of value, and need to be controlled by some mechanism in order to maintain a stable price of the commodity.

In the value of money [@Value_of_Money] Pigou describes the role of the money supply in the Quantity theory of money and its relation to the price. The quantity theory of money states:

$$M \times V = P \times T$$

Where M is the money supply, V is the velocity of circulation, P is the price of the coin and T are all transactions done with the currency.

This implies that the price of a currency can be controlled by increasing and decreasing the money supply. Indeed this is a technique also currently used by central to prevent deflation of their currencies.

In this survey we will see currencies vary both M and V as a means to keep P at a stable level.

2.3 Making a market

The easiest way to keep a currency stable is to simply have it derive its value from a different asset that already has the desired stability. This is called pegging.

The pegging of a token to an asset can be achieved by allowing investors to trade the token for the asset at any time. Note that a this may involve the trade of a secondary asset as intermediary store of value.

The first pegs were tracking the value of gold. Every unit of a currency could be exchanged for a certain amount of gold. As described in “The Gold Standard” [@The_Gold_Standard] by Cooper, the US dollar has been pegged to Gold for some of its years to maintain the confidence of the public.

The most common way to guarantee an exchange rate is to hold some form of collateral. The most obvious collateral for the token, is the asset it is pegged to, but this can also be another commodity that can be traded for the asset at any time. Of course this requires some guarantees or assumptions about the price stability of this commodity to ensure that all outstanding tokens can be redeemed. If the amount of collateral, or the value of the collateral, is such that less that 100% of tokens can be redeemed for the original asset, the token is considered under-collateralised. This can have large ramifications to investor trust, and might thus undermine the stability of the coin and the viability of the network.

Any entity or system that facilitates the exchange of the token for the collateral is called a market maker. In this survey two main categories of market makers will make an appearance, centralised organisations and decentralised systems.

3 Stabilisation by Centralisation

Maintaining a stable price is hard to define in general rules and thus the simplest way to create a stable currency is to simply have an organisation guarantee that it is. Where the US Dollar is guaranteed to be stable by the Federal Reserve increasing and decreasing supply to match the demand, centralised stablecoins tend to do something similar.

3.1 Stabilised by reputation

A mostly theoretical way of creating a stablecoin is to simply promise as an organisation that your coin is going to be stable. This is the presumably the approach taken by JPMorgan Coin [@JPMorgan_Coin:whitepaper] and Libra [@Libra:whitepaper]. Whereas JPMorgan Coin, aims to provide fast inter-organisation value transfer backed by JPMorgan as a traditional financial product with a digital spin, Libra aims to be a replacement for traditional fiat currencies while not being backed by any type of collateral.

3.2 Pegged by currency reserves

Since stabilisation by reputation is often not good enough for investors looking for a safe way to store their value a more secure stablecoin is needed. The simplest way to do this is to simply peg the cryptocurrency to another currency by guaranteeing a 1:1 exchange rate while holding enough collateral in order to do so.

The most successful currency to do so and the 5th largest cryptocurrency as of writing this survey is Tether [@Tether:whitepaper]. Tether maintains a 1:1 peg to the US dollar by simply issuing 1 Tether for every Dollar payed to them. They hold the USD and will at any time buy the Tether back at 1 Dollar price. This intensives the 1:1 peg outside of the official Tether exchange as well as any investor able to buy Tether at under a Dollar can immediately sell it to the Tether organisation for profit thus reducing supply on the open market when demand drops. On the other hand, an investor able to sell a Tether for over a dollar can make a profit by buying newly minted Tether thus increasing supply when demand increases.

As mentioned, Tether is currently the largest stablecoin, however its centralised reserves draw controversy that reduces investor trust. An improvement on this concept is to have multiple holders of the currency with frequent audits to increase trust in the organisations that are making the market. TrueUSD [@TrueUSD:whitepaper] holds collateral in multiple escrows and is audited by third party as a result they used to be 2nd largest coin before being overtaken by USD Coin (USDC). USDC is a USD pegged stablecoin created by CENTRE [@Centre:whitepaper] a joint venture of the exchanges Coinbase and Circle which also holds their collateral in multiple audited accounts.

The next level of trust that a stablecoin can guarantee comes from the government. PAXos [@PAXos:whitepaper], though having centralised reserves, is licensed and approved by New York State Department of Financial Services and has secured FDIC-insurance. This has won the favor of investors as they are now the 3rd largest stablecoin after Tether and Centre.

The largest current Euro coin is the Stasis euro [@Stasis:whitepaper]. It represents over 31 million euros currently and has maintained its peg since its launch in December 2018. Stasis has built a network of liquidity providers and is thus not the market maker themselves.

3.3 Pegged by assets

Essentially, a centralised currency pegged stablecoin is just a tokenised asset. This can be taken further than just currencies. Using tokenisation it is possible to peg the value of a crypto coin to anything.

Digix Gold Token (DGX) [@DigixDAO:whitepaper] pegs its stablecoin to the value of an ounce of gold. DGX is thus a cryptocurrency on the gold standard. However with the tracking of real world assets comes centralisation. DigixDAO, the organisation that manages DGX, stores its gold in a single vault in Singapore.

When the goal is to have a stable currency the dollar is not necessarily the best option as it is tied to the economy of the United States. Globcoin [@globcoin:whitepaper] and x8currency [@x8currency:whitepaper] aim to solve this by creating an asset that tracks multiple currencies as well as gold.

3.4 Pegged by other centralised stablecoins

In order to peg perfectly to a currency that currency needs to be regained from the stablecoin at any time. This requires the storage of the coin by some party. In all stablecoins so far, this is relatively centralised. Even coins splitting their coins across multiple escrowed accounts are subject to centralised fraud.

As a result coins are being developed that try to diversify the collateral. Reserve [@Reserve:whitepaper] aims to collateralize using USDC, TUSD, PAX. They aim to go through multiple phases with a final state where they are no longer pegged to the Dollar at all but a stable currency in itself.

4 Stabilised while Decentralised

Though many centralised stablecoins are becoming more diversified in their collateralization, a central point of failure remains in the organisations. The risk is depletion of collateral by market maker failure is always prevalent and there are so far no mechanisms for restoring collateral back to 100% when a failure does occur. As a response to this problem decentralised stablecoins have emerged.

4.1 Collateralized

Just like centralised stable coins the most successful stablecoins are collateralised in some manner. The difference between them is that decentralised collateral comes in the form of other crypto currencies. Even though the collateral is not US dollars, MakerDAO's Dai [@MakerDAO:whitepaper] still manages to maintain an average price of 1 dollar without any central form of governance. Similarly BitShares' [@BitShares:whitepaper] various fiat pegged coins, and Synthetix's [@Havven:whitepaper] various pegged assets track other real world assets without holding any of these assets.

4.1.1 BitShares

In July 2014 the BitShares [@BitShares:whitepaper] foundation launched BitUSD, a stablecoin that tracks the US Dollar and is collateralised in BitShares. BitShares are shares in the distributed autonomous company (DAC) also called BitShares. BitShares aims to be a decentralised exchange providing financial derivatives on the blockchain.

The role BitUSD plays in the exchange is best described as an order-matching between investors going "long" and "short" on BitUSD. An investor speculating on BitUSD will exchange some BitShares for 1 BitUSD. They can force settlement and sell the BitUSD back for 1 dollar worth of BitShares at any time. If the price of BitUSD goes up, they make a profit, but if it falls they are protected.

On the other side of the coin, there is the BitShares investor going short on BitUSD. This investor creates a short order and stakes enough BitShares collateral to cover an increase in BitUSD or drop in BitShares. When the order gets matched with a long investor by the exchange, the investor gets 1 BitUSD and the shorter is responsible for maintaining enough collateral to back the BitUSD at a 2:1 ratio. If the investor fails to maintain collateral above this ratio, the BitUSD contract will get margin called.

A margin call means that the blockchain will automatically create an order for anyone to sell their BitUSD for a profit. This profit comes out of the stake of the shorter as they did not properly maintain the collateral in the contract. Whatever is left after the margin-call is returned to the shorter.

If a shorter wishes to close out their position, they must buy a BitUSD to get their collateral back. If the price is lower than what the investor paid them, they make a profit, if BitUSD got more expensive the shorter now has to cover those costs.

This mechanism stabilises the price of BitUSD through its interaction with the market. BitUSDs are fully fungible, meaning any BitUSD can be bought to close out a short. This means that if an investor is able to buy a BitUSD for under a dollar, they can immediately force the settlement.

Note there is no hard mechanism for adjusting the price down. This means the currency can move up to whatever the markets think it is worth. It relies on the shorters buying the BitUSD at a loss when the price starts going up. If the market as a whole chooses to collateralize up to the new value, a new peg will be created there, except for the guarantee of forced settlement. The market does move as a whole however, as every short seller that doesn't collateralize up will get margin called.

4.1.2 MakerDAO

MakerDAO[@MakerDAO:whitepaper] is a Distributed Autonomous Organisation that consists of 2 main coins. A governance token called Maker and the stablecoin Dai. As opposed to BitShares, Dai is not backed by the governance token, but rather by Ether. There is also no matching of "long" and "short" sellers, but simple smart-contracts can allow contract for difference trades like BitShares.

Dai is stabilised by a single class of investor, namely someone speculating on Ether. Dai is created in a process where an investor locks their Ether into a smart-contract called a Collateralized Debt Position (soon to be renamed to Vault). This allows the investor to mint Dai that is now backed by the locked Ether. At any time, the investor can pull out their Ether by trading it back for the amount of Dai that had previously been created.

The investor has to lock over 150% of the value of the Dai created in order to make sure that the system is always properly collateralised. So if the investor prints 100 Dai there has to be at least 150 dollars worth of Ether locked away.

The investor can use their Dai as they see fit. A common use case is peer-to-peer lending. Another is to buy more Ether to stake, thus taking a leveraged position on Ether. Note that since the position has to be over-collateralised by at least 150%, that the maximum leverage is a ratio of 3.

This leads to a mechanism similar to the one that stabilises centralised coins. If the price on the market is below 1 dollar an instant profit can be made by buying them and resolving the open CDP. Like BitShares, there is no direct mechanism to reduce the price should it trade for more than a dollar.

Multi-collateral Dai aims to solve the problem of collateral devaluing. By having different collateral assets that are uncorrelated, the devaluing of one form of collateral can be safely handled by investors buying a non-devaluing form of collateral in order to pay off the failing CDPs.

4.1.3 Synthetix

After BitShares and Maker showed how a non-blockchain asses can be tracked in a fully decentralised manner, Synthetix [@synthetix:whitepaper] builds on it by tracking any real world index that can be fed to the blockchain.

Originally Havven [@Havven:whitepaper], Synthetix generalises stablecoin to pegging to any off-chain trackers. By putting up Synthetix Network Tokens (SNX) as collateral, an investor can create any synthetic asset within a 500% collateralization ratio. These synthetic assets tracking some index are called synths.

Since any synth can be exchanged for SNX and then into any other synth, Synthetix chooses to allow direct trading between synths. This allows for a full peg as any pegged asset can be exchanged for another using the blockchain Synthetix exchange. This peg is much harder to break than the soft pegs of BitShares and MakerDAO.

As opposed to MakerDAO and BitShares, in the Synthetix network the investor that stakes the collateral gains an interest on their stake from the transaction fees between the synths. Stakers in the MakerDAO system have to pay a yearly stability fee (currently 5%) in order to be able to retract their collateral. In the BitShares network, stakers pay an interest rate to the BitUSD holders. This mechanism of incentivising stakes can lead to profits for stakers even in a bear market.

4.1.4 Dependencies

So far we have discussed three systems for asset stabilisation using decentralised means. However, all these systems rely on having correct pricing information on the asset they are aiming to peg.

Currently some projects are using [@Oraclize:whitepaper], but as their oracle is centralised most DAO project are moving away to their own solutions or to

Chainlink[@Chainlink:whitepaper]. Chainlink describes itself as a middleware between the real world and the blockchain. It can also provide information about blockchains to other blockchains. Thus linking them together. This system lends itself to tracking of asset prices very well.

MakerDAO makes plans to shift from their “medianizer” smart-contract to Chainlink soon. As well as Synthetix, which currently uses a centralised oracle, switching to the decentralised middleware.

4.2 Algorithmic

Of course, stablecoins as a pegged currency are only a band aid on the real problem. Cryptocurrencies need to be stable on their own if they are ever going to replace fiat currencies.

4.2.1 Theory

When it comes to algorithmic stability of blockchain currencies, there is a lot more academic research available. Most actual working blockchain based distributed systems that provide any value are built by DAOs and foundations and end up falling more in the pegged currencies and crypto-derivative markets. This makes sense as these are the first most obvious use cases of blockchains. However as the space starts to age and the rate of progress starts to slow, academia will likely find their place in the space again.

For now the research into stablecoins mainly aims to model and improve the mining algorithms. In “How to make a digital currency on a blockchain stable” [@How_to_make_a_digital_currency_on_a_blockchain_stable] Saito et al. describes a number of improvements that would make bitcoin more capable of responding to fluctuations in price.

Saito argues that the absence of a link between newly minted currency and the supply and demand leads to unnecessary instability. Since miners will increase and decrease their mining efforts as the price of bitcoin fluctuated, this behaviour can be build upon to respond to both demand and supply shocks.

Saito suggests that mining reward should go up when mining rate increases as this only happens when the price of bitcoin has risen. Thus increasing the supply and absorbing some of the demand shock. Inversely mining reward should go down when mining rate decreases.

According to Saito this should be done by not resetting the block mining time to 10 minutes unless a minimum/maximum threshold is reached. When the threshold blocktime is reached the reward for the block should simply be scaled with the mining difficulty.

Saito also suggests no halving in mining reward. To cull inflation he suggests a mechanism for deflation of the currency every 100 blocks all bitcoins are depreciated in value by deleting a percentage of them universally.

In “Elasticoin: Low-Volatility Cryptocurrency with Proofs of Sequential Work” [@Elasticoin_Low-Volatility_PoSW] Dong et al. argues that as the mining rate should remain constant, a better way to build a more stable currency is as a secondary token. Dong argues for using Proofs of Sequential work (PoSW) to generate currency at a fixed rate. This allows anyone to mine a coin by putting in some work. This leads more mining when the price is high and nearly none when it is low.

Dong argues that PoSW will scale much better into the future as the sequential speed of processors improves at a much slower rate than parallel speeds. Dong presents a non-interactive PoSW. And an algorithm for minting based on this Proof.

In “Can we Stabilise the Price of a Cryptocurrency?” [@CanWeStabilize] Iwamura et al. preset “Improved Bitcoin” (IBC). A theoretical currency where the reward to the miners is adjusted based on the price. Iwamura argues that there is a need for a mechanism of reducing circulating supply of the currency in case of a negative demand shock. Just like Saito, Iwamura argues for allowing blocktime to vary with mining power.

Since it is not possible to withdraw currency directly from the market, Iwamura argues for some rate of inflation to absorb demand shocks. Iwamura argues for a depreciation rate applied by gradually increasing the mining rewards.

4.2.2 Practice

In practice we have seen some notable distributed cryptocurrencies attempt to create a stable cryptocurrency without collateral.

The first stablecoin to be stable for a year was Nubits[@Nubits:whitepaper]. Nubits incentivised holders to park currency during low demand periods. They successfully recovered from a large demand shock in 2016, but after the crash of 2017-2018 it lost its peg again and never recovered.

BitBay [@BitBay:whitepaper] is a cryptocurrency by the trading platform BitBay. BitBay suggests a “dynamic rolling peg” a system whereby all users of the system vote on the inflation and deflation of the supply for an interval. BitBay also freezes the fastest assets for a period of time. Going back to the quantity theory of money, this corresponds to changing the velocity of the money rather than the supply.

Just like Nubits and BitBay, Anchor[@Anchor:whitepaper] incentivises holders of the currency ANCT to trade it for DOCT when the currency is listed at under 1 “MMU”. When the price of the currency goes above 1 “MMU” the holders of

DOCT are incentivised to get their ANCT back. In this way anchor found a way to reduce the money supply and thus the price. As opposed to being pegged to the dollar it is pegged to the “Global Economic Growth” by MMU oracle (Monetary Measurement Unit). Anchor just launched so very little information is available about their success or failure.

Ampleforth [@Ampleforth:whitepaper] doesn’t call itself a stablecoin. It doesn’t aim to maintain a stable price, it just aims to be uncorrelated with both Bitcoin and the real world financial markets. While Ample does maintain a peg to a target, the system does not aim to maintain the value in its holders accounts. Say the price of Ample doubles due to high demand. Ampleforth will double all existing coins in place to make 1 coin equal to the target again. A rebase of the price happens at most every 24 hours.

Basis[@Basis:whitepaper] was a project that aimed to stabilise a currency by auctioning bonds for its coin during a time of low prices to decrease the money supply. These bonds can then be redeemed at a time of high demand for exactly 1 basis. This mechanism is similar to that of freezing assets, just that the frozen assets are referred as bonds in this case. Basis never launched.

5 Discussions of Stablecoins

Besides the papers describing techniques, some research has been done into existing stablecoins, quantifying their prevalence, and discussing their criticisms.

In [@DuffieDigital_and_Fast_Payment_Systems] Darrel Duffie describes the use of stablecoins for banks aiming to digitise both inter-organisation value transfer and governments wanting to implement a digital currency with the utility benefits of cryptocurrencies and the stability of fiat.

Chohan discusses the difficulties in maintaining a properly collateralised peg in “Are Stable Coins Stable?”[@Are_Stable_Coins_Stable]. Chohan describes how maintaining a true 1:1 peg leads to funding and scalability issues.

In “The State of Stablecoins”[@THE_STATE_OF_STABLECOINS] the “blockchain team” present an empirical study of 57 live and pre-launch stablecoins showing adoption, trading volume and market cap. They describe a taxonomy where they differentiate between “traditional” collateralised, crypto collateralised and algorithmic. They describe many pros and cons of these types of coins. The survey is very extensive and describes all 57 currencies in terms of their investors, tech, legal structure and collateral format.

In “Stablecoins in Cryptoeconomics. From Initial Coin Offerings (ICOs) to Central Bank Digital Currencies”[@Stablecoins_in_Cryptoeconomics] Erba discusses the stablecoins in the context of the law in both the united states and Europe. Erba argues for crypto-currencies “fully backed by Central Bank reserves”

In “Stablecoin: Yet Another Layer of Cryptocurrency Complexity”[@Stablecoin:_Yet_Another_Layer_of_Crypt
Lee looks at the way that stablecoins can fit into the modern legal system. Lee argues for Bankruptcy Courts to treat stablecoins as a commodity as opposed to a currency.

In [@Fedcoin] Koning describes the requirements and considerations for a stable currency controlled by a central bank. Koning describes the monetary policy and choices that comes along with implementing a digital currency on a large scale.

In [@In_stability_for_the_Blockchain] Klages-Mundt et al. look at the existing stablecoins through a critical lens and describe some ways in which the currency pegs can be broken. Klages-Mundt build a generalised model of decentralised crypto-collateralised stablecoins. It describes possible attacks on these systems where the pegged currency is bid up so an extent where collateral starts to get margin-called creating a run-away feedback loop.

6 Conclusion

There is a lot happening in the stablecoin and DeFi space right now. Stablecoins are being tested in a trial by fire in the real-world as we speak. Through this organisations such as MakerDAO and Synthetix are developing completely systems that promise to either revolutionise the world by taking Decentralised Finance to the next level, or they will spectacularly go up in a ball of fire. Only time will tell.

7 References