

A Survey of Techniques for Price Stabilisation of Cryptocurrencies

Robert Wessel Blokzijl TU Delft
Delft, The Netherlands
R.W.Blokzijl@student.tudelft.nl

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.

Index Terms—Stablecoin; Blockchain; Cryptocurrencies

I. 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[1] and programmable [2] 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 [3], 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

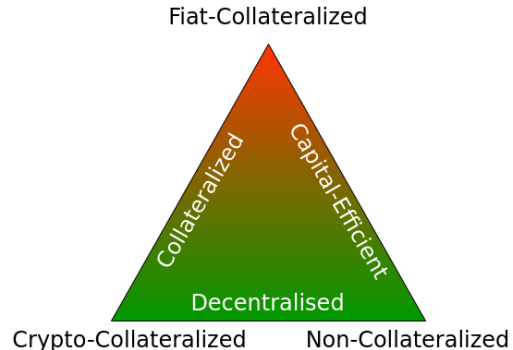


Figure 1. Inherent trade-offs of stablecoins



Figure 2. Taxonomy of stablecoins

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.

II. BACKGROUND

Before we get to the techniques used for stabilisation some concepts and terms need to be defined. In this section 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 collateralized.

A. The purpose of money and the requirements of a stablecoin

In “On the Origin of Money” [4] 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

B. 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 [5] 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.

C. 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 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” [6] 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 than 100% of tokens can be redeemed for the original asset, the token is considered under-collateralized. 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.

III. STABILISATION BY CENTRALISATION

With more control over the supply of a currency, the price stabilisation of a currency is significantly simplified. Minting more in times of high demand, though looked down upon, is a powerful way of controlling the value of a currency and preventing runaway deflation. Conversely, reducing the rate of minting slows down inflation of the currency.

Another way of stabilising a currency is to peg it to an already existing currency or commodity. This method brings with it questions about collateralization, transparency, risk, and the meaning of value.

In this section we explore the techniques employed by both central reserve, and pegged stablecoins.

A. The reserve bank stablecoin

Combining the proven success of central banks with the benefits of fast payment systems [7], organisations like JPMorgan [8] and the Libra Association [9] aim to create

a stable currency by using their reputation as established financial institutions. So far, no coin has managed to be stable off of its reputation alone, and whether this will ever happen is yet to be seen.

B. Pegged by currency reserves

Since stabilisation by reputation is often not good enough for investors looking for a safe store of value, a stablecoin with stringer guarantees about its future value is needed. The simplest way to do this is to simply peg the cryptocurrency to another currency and guaranteeing a 1:1 exchange rate by holding enough collateral in order to make any investor whole at any time in the future.

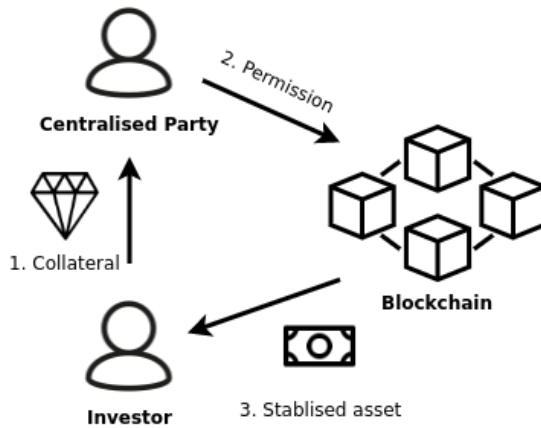


Figure 3. Minting a pegged crypto-asset

Figure 3 describes the general way in which pegged crypto assets are created. The centralised party in the image provides some guarantee about the exchange rate. For this example we assume a peg for 1 stabilised asset to always be worth 1 dollar. In this context, the dollar is provided as collateral for the asset in the following way.

1. 1 dollar is transferred from the investor to the centralised party using traditional payment systems.
2. The centralised party mints 1 stabilised asset and transfers it to the investor
3. The investor is free to use the asset as they please

Figure 4 illustrates the general way in which pegged crypto assets can be traded back for the original asset.

0. Anyone can obtain the stabilised asset by trading for it on some market or by having one minted by the centralised party.
1. Any investor who holds a stabilised asset can send it to the blockchain to be burned.
2. Upon receiving a proof of destruction, the centralised party will send an equivalent amount of dollars back to the investor.
3. The investor is now out of their position.

By guaranteeing that there is always a 1:1 exchange rate between the collateral and the stabilised asset, the asset

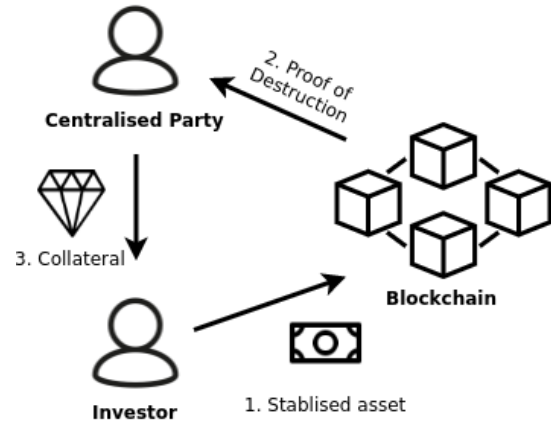


Figure 4. Burning a pegged-crypto asset

is pegged at a 1:1 ratio even in external markets. This illustrated using the following two scenarios.

When the stabilised asset trades for more than 1 dollar on the open market, anyone can make an instant profit by minting more assets, and immediately selling them on the open market. This process will continue to increase the supply of the asset until the price is back down to 1 dollar.

Conversely, when the stabilised asset trades for less than 1 dollar on the open market, anyone can make an instant profit by buying the coins on the open market, and immediately burning them. This process will continue to decrease the supply of the asset until the price is back up to 1 dollar.

1) Benefits of Centralisation: Like illustrated in figure 1, fiat-collateralized pegs can not be maintained by a fully decentralised system. The limiting factor is the fact that fiat-currencies need to be held by some party.

Some argue the price guarantees of pegging to a fiat-currency outweighs the sacrifice of decentralisation. The success of currencies like Tether [10], Centres USDC [11], PAXos [12], and TrueUSD[13] illustrate this with their combined market capitalization of 5 Billion USD.

2) Critiques of Centralisation and solutions: It goes without saying that having a centralised storage of anything creates a central point of failure and control. Since trust in the crypto space has long been based on what is verifiable, proving the absence of fraud becomes a new challenge. To address the concerns of coin holders the different stablecoin market makers provide different guarantees with respect to the proper storage of collateral. Common ways to improve investor confidence include:

1. Regular audits providing proof of collateral (Tether [10], USDC [11], PAXos [12], TrueUSD [13])
2. Multiple independent collateral trust accounts (TrueUSD [TrueUSD:whitepaper], Stasis Euro [14])
3. Subjecting themselves to established regulations and providing FDIC- insurance. (PAXos [12])

Through these means stablecoin organisations aim to counteract the lack of transparency and the risk of under-collateralization.

3) *Expansions on fiat-currency pegging:* Essentially, a centralised currency-pegged stablecoin is just a tokenised fiat-currency. This concept can be expanded to more than just traditional currencies. Using tokenisation and central storage it is possible to peg the value of a crypto coin to anything that has value in the real world. As such some stablecoins peg their value to the original form of money: Gold. Today, stablecoins like PAX Gold [15] and DigixDAO [16] hold gold in trust for their crypto holders. Though the gold provides a strong guarantee that the stablecoin will hold its value, the coins are still less stable than the Dollar as there is no central agency stabilising gold.

Expanding even further on the concept of tokenised assets as stablecoins, any collection of assets that is stable on average can provide a stablecoin. Even though the US Dollar is seen as the most stable currency world-wide, it is still dependent on the stability of the United States economy. To address this stablecoins like Globcoin [17] and x8currency [18] aim to create an asset that tracks multiple currencies as well as gold. Thus creating a coin that is “more stable” than the US Dollar. Whether these coins will ever have a mainstream appeal is impossible to predict, but the theoretical value of having a globally stable coin is hard to dispute.

4) *Overview of the largest stablecoins:* To provide a glimpse of the usage of the techniques described in this subsection, Table ?? describes the 8 central stablecoins with the highest market capitalisation and some of their operational aspects:

Some interesting observations can be made from the table.

1. The PAXos company operates 3 of the top 8 stablecoins.
2. 3 of the top 8 stablecoins are operated by exchanges including the second largest stablecoin USDC.
3. Gold based stablecoins still make up a small portion of the market with PAX Gold being the largest with a market cap of 12 million.

IV. STABILISED WHILE DECENTRALISED

Though many centralised stablecoins are becoming more diversified in their collateralization, the organisations that run them remain a central point of failure. The risk of collateral depletion by market maker failure is always prevalent and though some stablecoins store their collateral with bankruptcy remote companies, this just moves the risk to a different central entity.

To protect investors from the failure of any central entity and even the failure of the financial system as a whole, new stablecoins have emerged that remain price-stable in a decentralised manner. These coins come in two main categories:

	Stablecoin	Market Cap	Pegged asset	FDIC-Escrow	Insurance	Launched	Notes
Tether[10]	4	Trillion USD	USD	Single organisation	No	2014	Largest Stablecoin, 4th largest cryptocurrency
USDC[11]	464	Million USD	USD	Single organisation	Some changes	2018	Created and owned by various crypto exchanges
PAXos[12]	238	Million USD	USD	Single organisation	Yes	2018	Regulated by the New York State Department of Financial Services
TrueUSD[13]	1361	Million USD	USD	Multiple independent	Some escrows	2018	Distributes risk with multiple independent escrows
Stasis[14]	35	Million USD	Euro	Multiple independent	No	2018	Largest Euro Stablecoin
BUSD[12]	18	Million USD	USD	Single organisation	Yes	2019	Issued by PAXos for the Binance exchange
USDK	28	Million USD	USD	Single organisation	No	2019	Owned and operated by the oklink exchange
PAX Gold[15]	12	Million USD	Gold (1 ounce)	Single organisation	No	2019	Gold held in custody by PAXos Trust Company

1. Crypto-Collateralized Stablecoins
2. Algorithmic Stablecoins

This section explains the mechanisms that keep these coins stable, provides a comparison of their advantages and disadvantages, and a general overview of the largest decentralised stablecoins on the market right now in each category.

A. Crypto-Collateralized Stablecoins

The success of the centralised stablecoins shows that the backing of a stablecoin with 100% collateral is a reliable way to keep a currency price stable.

The main problem with backing a decentralised stablecoin with some type of collateral is that there needs to be a mechanism of exchange between the stablecoin and the collateral. When the collateral is fiat-currency or some real world asset, there must always be a central party that holds the collateral and facilitates the mechanism of exchange.

Crypto-collateralized coins build on the idea that a holder of a stablecoin can always get their share of the collateral back, but in a fully automated and decentralised manner.

Crypto-collateral coins allow the exchange of the pegged currency such that even the organisation that created the stablecoin has no power over the collateral. Initially it may seem like we need a collateral with the following requirements:

1. Stable - to stabilise the stablecoin
2. Decentralised - to avoid central control
3. Fully programmable - to automate the collateral exchange mechanism

The problem here is quite obvious, we are looking for precisely the thing we are trying to create, a decentralised stablecoin. In order to solve this, crypto-collateralized stablecoins choose drop the 3rd requirement and use decentralised but unstable cryptocurrencies as collateral. The way this can still lead to a stable currency is as follows:

Instead of guaranteeing the direct exchange of the stablecoin for the pegged currency, say 1 token for 1 dollar, the system aims to guarantee that an investor can exchange 1 token for 1 dollars worth of the collateral at any time. This leaves a problem, what if, because of the volatility of the collateral, the market value of the collateral drops such that there is no longer enough collateral to back all outstanding stablecoins. This could lead investors to scramble to get their share of the collateral out before its gone, rapidly undermining the price of the stablecoin.

The solution to this is overcollateralization. In order to guarantee that there is always enough collateral in the system for every investor to be made whole, the creation of any stablecoin has to be paired with the deposit of **more** than 100% collateral.

This leads to one final question, what investor looking to hedge against the price stability of cryptocurrencies would lock up their crypto in order to get a token that has lower value than the underlying collateral. They are now neither hedged against the drop in value of their collateral, nor do they have any extra utility with their new token as the collateral was equally decentralised and programmable.

The solution to this is found in the concept of a swap. A financial swap is a derivative contract where two parties swap some properties of some underlying assets. In the case of our stablecoin, one party, lets call them the investor, offloads the risk associated with the price instability of the collateral to our second party, lets call them the speculator.

Figure 6 describes the process of minting a decentralised stablecoin that uses the swap mechanic:

0. Some agreement is reached between the investor and the speculator. This might happen on an individual basis, but sometimes the terms of the agreement are pre-defined by parameters of the network.

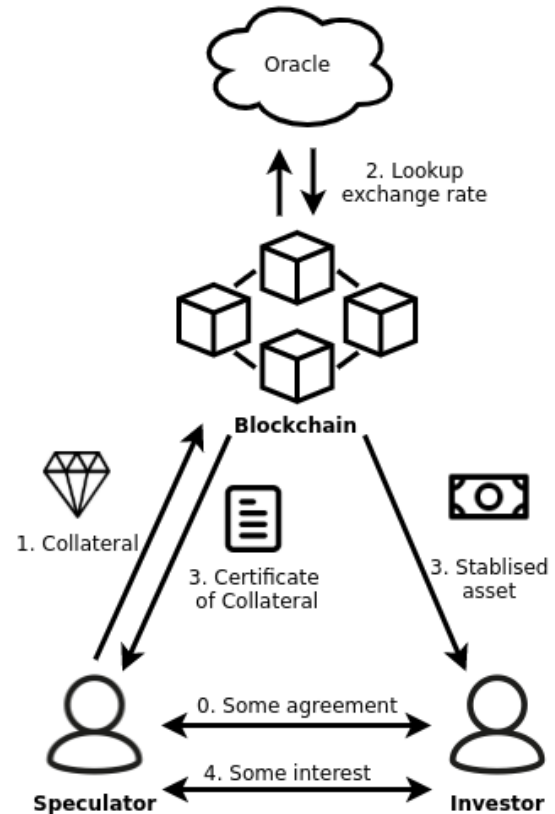


Figure 5. Stablecoin minting through debt creation

1. Some crypto, lets say Ether, is sent as collateral to a smart-contract. Some of this, usually 100%, might come from the investor, while the speculator provides the rest of the collateral, lets say 50%, for the stablecoin to remain overcollateralized by some ratio, in this case 150%.
2. A smart-contract checks the price of the Ether in terms of the pegged currency, lets say dollars. Mechanisms for the decentralised lookup of Ether prices vary between systems. We explore these differences later in this section.
3. The stablecoin is minted and issued to the investor, while the speculator gets some proof of deposit for their collateral. Lets call this the debt-contract.
4. Some interest might be paid from the investor to the speculator or vice versa.

The investor might pay interest to the speculator as a reward for providing the capital for overcollateralization and taking on the risk of the collateral dropping in value while the stablecoin is in circulation. On the other hand, the speculator might pay the investor as a reward for providing extra capital for the speculator to leverage their bet on Ether. The direction of interest depends on the design of the stablecoin and sometimes the market conditions.

While the stablecoin is in circulation the speculator is responsible for maintaining the collateral of debt-contract. Should the value of Ether drop, they must deposit more

Ether to the smart contract, or risk getting margin called.

A margin call is the automatic closing of a debt contract. A margin call happens when the value of the collateral drops below the minimum collateral requirement of the system. In the case of our example this means there is not enough Ether in the debt-contract to cover 150% of the outstanding stablecoins of the contract. A margin call opens the debt-position to be closed by anyone, and incentivises this by providing a reward for whoever closes it.

The closing of a contract is the burning of the stablecoin and the recovery of the underlying collateral. The process for this is illustrated in figure and includes the following steps:

0. Some agreement is reached between an investor willing to sell a stablecoin, and a someone willing to close out a debt-contract. This agreement could come be in the form of a speculator simply buying the coins from an investor at market rate, an investor acting on a margin call, or by some other matching mechanism between stablecoin and debt-contract.
1. The stablecoin is sent to a smart-contract, which burns the coin.
2. The oracle is consulted for the current price level of Ether in dollars.
3. The collateral is provided back to the speculator and investor at some defined ratio. Usually 100% of the stablecoin value goes to the investor while the remaining 50% or more goes back to the speculator.
4. Some settlement may be done, this could be the payment of interest between the two parties or some fee to the blockchain.

As an extra line of defence against the falling of the collateral value or some attack against the system, crypto-collateralized stablecoins often have a mechanism for global settlement implemented. In the case of a global settlement event, the underlying collateral gets returned to the investors without any conditions. All debt contracts will be locked, allowing all holders of the stablecoin to trade in their tokens for 1 dollars worth of collateral. After a period of time, the contracts will be released and return all collateral left back the the speculators.

The triggers for a global settlement differ per stablecoin, but mechanisms include: global collateralization under a minimum ratio, high price instability, a decision by holders of some governance token.

1) *Governance*: In addition to triggering global settlement in the case of some black swan event, decisions need to be made about the network in general. Examples of this can be parameter tweaking like the collateralization ratio or network fees, as well as network upgrades. For this reason most decentralised stablecoins are part of a Distributed Autonomous Organisation (DAO). Shares in the DAO, or governance tokens, allow the holders some say over the inner workings of the network, as well as some claim of the

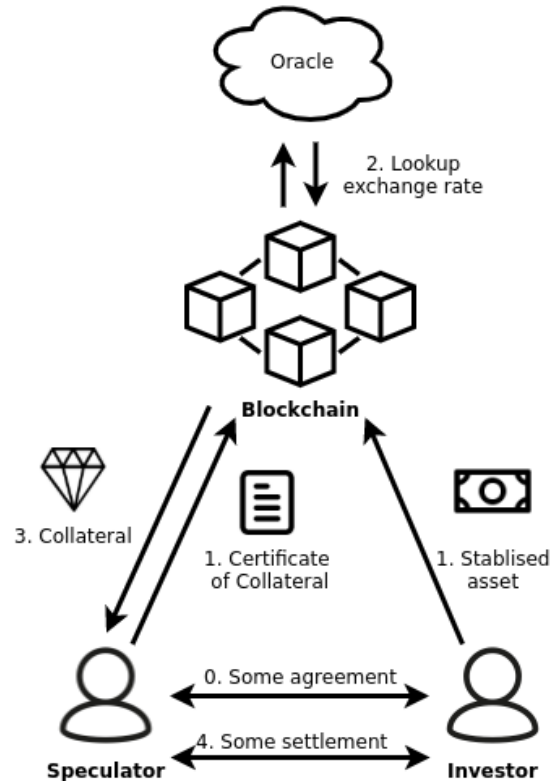


Figure 6. Stablecoin burning through debt-position closure

profits of the network. This ties the value of the tokens to the performance of the network, which in turn incentivises the holders of the governance tokens to remain invested in the network and to vote for parameters and mechanisms that improve the utility and stability of the stablecoin.

2) *Minimum Collateralization Ratio*: The minimum collateral required varies between systems. It is the responsibility of the speculator to maintain a collateralization ratio above the minimum requirement, or they get margin called.

The collateralization requirement depends on the volatility of the collateral used. Since the margin call of a contract takes time to find an investor someone willing to close it, there needs to be a buffer for the price of the collateral to fall even further. This buffer is the gap between the minimum ratio and 100%.

This means that network doesn't lose any collateral as long as the collateral doesn't drop to $1/c$ within the time it takes to margin call a contract. Where c is the minimum collateralization ratio.

3) *Mechanism for speculator to investor match making*: Stablecoins that utilise these derivative contracts are usually built with a system that aligns the incentives of the stablecoins within some structure. Variations in these systems leads to differences in features like:

- the direction of interest payments,
- the matching of investor to speculator,

- the amount of collateral put up by each party,
- the mechanism of a margin call or forced-settlement.

To explain the variation between the systems we use some examples. We show how defences in the purpose of the system leads to differences in the features, and how the price keeps stabilising.

a) Reserve bank speculator model:

In the first type of system the speculators collectively act like a reserve bank.

The creation and destruction of stablecoins are controlled by the speculator. Anyone can create a debt-contract, deposit collateral and mint stablecoin tokens as long as they remain properly overcollateralized. The contract can also be closed at any time by depositing an equal amount of stablecoins to get the same collateral back.

It is important to know that, in this system, the amount of stablecoins created is determined by the price, in say dollars, of the collateral at the time of minting. This leads to the following incentive structure:

If the market value of the token is higher than 1 dollar a speculator is incentivised to deposit more collateral and mint more tokens. These tokens can then be sold on the market. Increasing the supply, thus dropping the price back to one dollar. The benefit of the speculator here is that they were able to create a debt contract at a favorable rate. If, when they pay back the tokens, the market value of the token is lower than when they sold the coins, they will make a profit.

If the market value of the token is lower than a dollar, any speculator with an open contract can buy the tokens at a discount and close their contract out at a profit given that they bought/sold the tokens at a higher price. This leads to fewer coins on the market, thus increasing the value back up to a dollar.

This creates a “soft peg” as there is no guarantee for the speculator that when they mint and a coin they will be able to buy it back again at a lower price. This can lead to the market price of the token rising to a different price level, and the peg can stabilise at a price level that is higher or lower than any collateral held.

The price level of the token is thus determined by what the market believes it is worth. There is some indication however, that the coin will not drop below 1 dollar, since that is the value that is returned to investors in the case of margin calls or a global settlement scenario.

In this scenario, the speculator takes on a certain amount of risk speculating on the value of the collateral and the price of the token. Initially it seems like the speculator gets their value from speculation only. They can, for example, sell their tokens on the market for more of the collateral thus leveraging their speculation on the collateral by some factor.

Usually, the designer intended way for the speculator to make a profit is by peer to peer lending. Instead of selling the tokens on the market, the speculator can lend out the tokens to make some extra dividends while speculating on the collateral. In this way, the speculator acts as the reserve bank increasing the supply of the token by lending out more.

Irregardless of how the speculator chooses to use their tokens, anyone investor buying them has a some guarantee that they will be worth at least a dollar in the future, thus creating an asset that is more stable than the underlying collateral.

The complete risk acceptance and decision making of the speculator allows for a number of expansions on the already explained concepts. First, since the success of the network is dependent on everyone being properly collateralized on average, and this in turn is dependent on the market value of the collateral, it makes sense to diversify the collateral. Thus, a multi-collateral system, which improves guarantees for token holders can be created, where the speculators have a choice in what collateral they want to stake. This protects the system against a price crash in one collateral category, as speculators are incentivised to exchange the collateral that is dropping in value for more price-stable collateral.

b) Speculation market model:

In this model the stablecoin can still be bought by the investor to offload risk to a speculator on some market. On the other side of the coin, the speculator still puts up extra collateral to back the coin in order to speculate on the underlying assets and provide collateral in case of a price dip.

The first differences between this model and the reserve bank model is that the mechanism to match investor to speculator, hereafter called the “internal market”, is done through margin trading. This means that the internal market is effectively an exchange where speculators and investors put up offers to be matched with each other.

The model relies on the fact that the investor, at any time, can redeem the stablecoin for 1 dollars worth of collateral. This way the price should always be around 1 dollar.

When a speculator puts up an offer, it acts like a proposal to the investor. The offer describes the amount of collateral that the investor should pay into the debt position. The investor knows that they have some guarantee to redeem it for 1 dollar of collateral at any point later. This fact provide a lower bound on the value of the coin as coins sold below a dollar will immediately be bought up and redeemed. This creates a price for the investor of 1 dollar plus some premium. This premium acts as an incentive for the speculator to put up the extra collateral and is variable based on the market.

After two orders get matched on the internal market, the investor provides the agreed upon amount of collateral, and

the speculator puts up the rest of the collateral required to meet the minimum ratio and maintains this throughout the lifetime of the contract.

The generated stablecoin is given to the investor and is fully fungible as they can be redeemed for 1 dollar at any time regardless of how much collateral the first investor put up. The coin can now be traded just like any other currency on some external market.

Interest in this is paid from the speculator to the investor, as the investor allows the speculator to use their collateral to speculate on.

When finally a stablecoin holder wants to close out their side of the contract and redeem their dollar of collateral, they make another order on the internal market. They will then get matched with a speculator wishing to close out their contract.

The investor gets 1 dollar of collateral from the contract of the speculator, and the speculator gets the rest. At this point the speculator will take their earnings or losses as they will have got more collateral than they put in if the price of the collateral has gone up, and they will lose collateral if the price of the collateral has gone down.

In order to make sure there are always enough speculators willing to settle a stablecoin, this model can employ some ways of forcing speculators to match the settlement. The first way is a maximum lifetime for speculator contracts. This forces speculators to close out their contract within a set time, say 30 days. This guarantees that any investor can redeem their coin within this time as the full outstanding amount of stablecoins in the system have to be bought back every 30 day. The second way is to simply close out the speculators contract that has the lowest collateral ratio. This has the benefit that investors get their money back quicker than the first option. This also incentivises the speculator keep a high collateralization ratio.

This system, though similar, is fundamentally different from the reserve bank model in that the speculation is meant act like a prediction market while the stablecoin aspect is secondary. It also has the issue that there needs to be some exchange mechanism to match orders.

This system differs from the reserve bank model in the fact that the guarantee for the investor generated after 2 people create a coin together. The first and last investor are always interacting through the internal market, which causes the investor to be more than just someone looking for a safe position. As the investor buys the coin at some “premium” they are betting that the price on the market when they want to sell accounts for this premium.

However, when buying a coin on the open market this stablecoin is only subject to the change in the premium and not the volatility of the coin.

The feasibility of this mechanism is yet to fully prove itself in reality, though some steps have been made. The

BitShares exchange was the first to use this mechanism and originally implemented a 30 day limit for speculator contracts, thus guaranteeing a maximum liquidation delay of 30 days. This was stable for a while but eventually lead to a distrust in the “guarantee” that the coin was redeemable, as you essentially have to freeze your asset for 30 days to get your money back. This led to the value of BitUSD dropping, which led in turn led to people “shorting” BitUSD by taking worse and worse prices for the stablecoin, as they expected to be able to close their contracts while the price of BitUSD was even lower. This created a negative feedback loop where the dropping price of BitUSD actually provided an incentive to create more BitUSD.

As a result, the BitShares holders voted for global settlement to avoid the further loss of stability. Eventually the stablecoin was relaunched with the 30 day limit removed and a 24 hour guarantee built in that matches the settlement order with the lowest collateralized contract. The price has not made it back to one dollar and remains relatively volatile.

Other BitShares stablecoins like BitCNY also use this mechanism and are stable, likely because of a larger, thus more resilient, market.

c) *Debt-pool Tracker service:*

The final matchmaking system is very similar to the reserve bank system, but abstracts away from the concept of having a single stablecoin, and just aims to track the prices of many different assets.

The system tracks the total debt of a speculator, rather than the specific stablecoin assets. This means that, just like in the reserve bank model, a speculator can put up any amount of collateral and issue “debt” based on some collateralization ratio. This means that the speculator is again the party that provides the stability, and absorbs any price shocks to the collateral.

As an investor the story changes. Any holder of a stablecoin can directly exchange it for a different stablecoin of equal value, at any time, using only the blockchain. Like before, the investor buys the stablecoin on the market. Let's say they buy a stablecoin that tracks the dollar. The blockchain allows them to exchange it for a stablecoin that tracks the euro at some exchange rate between the dollar and the euro.

Since no money was created, the total value in the system did not change and thus no interaction with the underlying collateral was needed. This allows the system to create synthetic assets that track any underlying assets, including currencies, stocks, other cryptos, and even the inverse of these.

When a speculator wants to leave the system, they simply have to buy back some assets worth what they originally created before they get their collateral back.

B. Non-collateralized Stablecoins

Stablecoin (System)	Peg	Collateral	Min. col.	Matchmaking	Interest paid	Governance (token)	Crypto collateralized stablecoins are dependent on the overall stability of their collateral currency. If the price of the collateral drops fast enough in relation to the pegged currency, many of these stablecoins would lose their exchange guarantee, and therefore lose investor confidence. Though these risks can be reduced in various ways, the general stabilisation of a currency without the reliance on collateral is a sought after feature that could improve significantly stablecoins.
DAI (MakerDAO)	USD	Ether (and more)	150%	Reserve bank speculator model	To Speculator (external)	DAI (MKR)	
BitAssets (BitShares)	Multi	BTS	300%	Margin Trading	Variable premium, once to speculator	DAI (BTS)	
Synths (Synthetix)	Multi	SNX	750%	Debt-Pool Tracker	Global interest calculation	Centralised, DAO soon	Some stablecoins, rather than offloading risk to speculators, aim to reduce volatility by controlling the demand and supply of currencies in other ways. In this section we describe the securities model for expanding and contracting the money supply, as well as some more theoretical techniques and currency parameters for reducing volatility.
USDQ (QDAO)	USD	Bitcoin	200%	Reserve bank speculator model	To Speculator (external)	DAI (QDAO)	

In this system interest is periodically paid from all investors to all speculators as incentive for the speculators to collateralize the system.

This system can provide a whole ecosystem for tracking real world assets and allows easy movement between them.

4) *Overview:* As can be seen in ?? There are a few large players in the crypto collateralized stablecoin scene.

MakerDAO is currently the largest most trusted system. They now allow for multiple different types of collateral, including Ether, BAT, REP and X0. They allow the community to vote using their (MKR) token. On which assets will be added for collateral.

BitShares is the system with one of the oldest working stablecoin, BitCNY, active since september 2014. BitShares is a decentralised exchange that allows users to speculate on a number of different BitAssets, including BitUSD, BitEUR, and BitBTC.

Synthetix describes itself as a “synthetic asset platform” and provides a number of stablecoins that track multiple real world currencies and assets. They allow direct conversion from one to another using the debt-pool tracker system where speculators are collateralizing the system at a minimum of 750%. The Synthetix platform started of centralised and is still a work in progress but is making major steps towards decentralisation. They offer many tracking assets like: sEUR, sUSD, sBTC, sETH. They also offer inverted assets to bet against some assets like: iBTC, and iETH. Currently they also support commodities like sXAU which tracks the Philadelphia Gold and Silver Index, and they plan to add trackers for various company stocks.

1) *Securities model:* The stabilisation of currencies is much older than cryptocurrencies. So to see how cryptocurrencies can be stabilised, some have taken inspiration from the way central banks stabilise traditional currencies. Specifically open market operations employed by central banks and the federal reserve.

When the fed wants to increase the money supply in times of deflation, they often buy government securities thus getting money out into the hands of the public. When they then want to decrease the money supply, they will sell the securities thus getting the money out of the system.

The securities stablecoin model utilises this concept. In times of inflation when the currency is undervalued, the blockchain will start selling bonds. These bonds lock up a buyers coins for a period of time, and will pay them back, including some interest, after a certain time. Since some of the money is now temporally out of circulation, the currency left on the market will go up in value.

In times of deflation when the currency is overvalued, bonds can be discouraged or disabled. Outstanding bonds can also be payed back prematurely in order to increase the money supply. When all bonds have released and deflation is still a problem, more money can be printed and distributed in some way until there the price is back down to the desired level.

Variables that can be tweaked to maintain the desired price level are:

- The interest paid over the bond - higher encourages purchase
- The lifetime of the bond - this is how long the money is out of circulation

These techniques have the potential to stabilise a currency without any collateral being needed. However, the choice of when the money supply should be expanded or retracted still needs to be made in a decentralised way. Consequently this is where the largest differences between the existing stablecoins lie.

Stablecoin (System)	Stabilisation		Duration	Interest	Governance	the guardians ran out of collateral, the currency lost its price guarantee, and the peg could no longer be maintained.
	Target	Mechanism				NuBits provides an example of the main flaw of the securities model, it requires trust in the mechanism, which lacks when it is needed most: in a down market.
Nubits	USD	Voting	Voted	Voted	DAO (NuShares)	Oracles
BitBay [19]	None	Voting	Unlimited	None	DAO (BitBay)	
Anchor[20] Basis[21]	USD	Oracle	5 years	Voted	DAO	
Ampleforth [22]						All stablecoins that peg to a fiat currency need some information about the price of that currency at any point in time. So far we have referred to Oracles as a source of this. In reality, this is a non-trivial problem and it is solved in a couple different ways.

a) Self stabilisation mechanisms:

By tweaking bond lifetime and interest rates a currency can be stabilised. However there still needs to be some decentralised mechanism that triggers changes to these parameters. Usually one of two self stabilising mechanisms is used:

- Share voting based parameter setting
- An Oracle based price feedback mechanism

Voting based parameter setting works how one would expect. The holders of a token, in some cases the stablecoin itself but usually a governance token, vote periodically on the stabilisation parameters of the network.

Within the oracle based system, the blockchain will activate an “expansion phase” in a time where the price of the coin is above the target, and a “contraction phase” when the price is below the target. The bond yield can be static or scale with how far the price is from the target, thus rewarding larger risk takers.

Note that even oracle based stablecoins are usually DAO’s that vote on the function that maps price target mismatch to bond parameters.

2) Overview of real world non-collateralized stabilising:

The first stablecoin to be stable for a year was NuBits[23]. NuBits stabilised by using a bond mechanism as well as voted in “guardians” who would get newly printed NuBits and would in turn provide liquidity to the market. These guardians would sell and buy the NuBits on the market at the price determined by the peg. In a way this turns the guardians into holders of collateral.

NuBits lost their peg twice and successfully recovered once in 2016, but after the “Christmas crash” of late 2017-2018 investors massively bought the stablecoin as presumably it was safe compared to the rest of the crashing crypto market because of its peg to the dollar. This grew the market cap of NuBits by 1500% over a few months while the guardians mostly held collateral in bitcoin. When then the crypto market started to recover, many sold their NuBits putting large pressure on the guardians who were now forced to buy NuBits for fewer bitcoins than they bought then for during the crash. This under-collateralized NuBits to a point where

The simplest solution is having a centralised source, this does create a central point of control and thus a central point of failure. When there is a central party that facilitates the exchange, this is not a problem.

Efforts have been made to decentralise the oracles as well. When every other aspect of the network is decentralised, a decentralised oracle will provide more security, which in turn boosts investor trust as this removes the central point of failure.

One way to decentralise the network is to have all nodes in the network vote on the value of the input. Here a proof of stake system can be used that punishes bad inputs to the system. If there are multiple different values given, the median can be taken.

Some decentralised currencies have a DAO token or similar that is tied to the health of the network. Since the value of the DAO token is dependent on the health of the network, holders of this token are incentivised to act honestly. In addition, some punishment for bad behaviour can be added in the form of proof of stake to aid in determining the correct price.

This mechanism also more specifically applicable, just determining precise price levels. Some stablecoins do not track the price, but have token holders vote whether the price is too high or too low, and based on that will trigger either “inflationary”, or “deflationary” periods [19].

This concept can also generalised even further. A long desired goal is to get real world information onto the blockchain in general. Solutions have emerged [24] that aim to solve this problem by creating a general infrastructure of nodes that access real world data and record this data onto the blockchain. To incentivise honesty of nodes, they stake an amount of network tokens that can be taken from them if the rest of the network disagrees with their votes. In addition node reputation can be tracked on-chain in order to allow users to choose the most trustworthy nodes.

D. General techniques for adding stability to any currency

Collateralized stablecoins by definition are pegged currencies. They rely on other currencies to provide their stability.

Without the stability of the US dollar or other, none of these currencies would work. When it comes to inherent stability of blockchain currencies, a number of academic papers are available. Following is a survey of techniques to reduce the volatility of any decentralised blockchain based currency.

1) Changing proof of work parameters to dampen demand shocks: Taking the quantity theory of money as a given, the price of a currency depends on the total supply, velocity of circulation, and the total amount transacted. These things are often set by the parameters of a blockchain network.

In the case of Bitcoin, the total supply is set, and slowly increased at a set rate without reacting to supply and demand. However, there is a link between the price levels and mining efforts [25]. If the price of bitcoin drops below a certain level, the mining reward will no longer outweigh the electricity costs. This miner response to the markets gives a natural input that somewhat tracks the price.

The block speed, and therefore the rate of supply of new coins, increase as the price increases. Therefore, if the mining difficulty stays the same, the currency will naturally respond to, and dampen, demand shocks [25].

Additionally, if the block speed is changed, the transaction throughput changes proportionally. This has the extra benefit of changing the velocity of money, which dampens the demand shock even further.

It is important to keep in mind that there are both upper and lower technical limits to the block speed. Set it too low and the transaction throughput suffers. Conversely if the block speed is too high forks are more likely, which undermines the security of the network.

2) Allowing for inflation: This method of controlling price levels has some implications [25] on long term price. In bitcoin, long term inflation is curbed by periodically halving the block reward. If these changes were used, this system would unnecessarily lower the mining incentives for miners, thus leading to a lower block rate.

One solution is to no longer halve the block rewards, thus turning Bitcoin into an inflationary currency. This is very controversial and has large economic implications who's details go beyond the scope of this survey.

As it is not possible to remove currency from the market, some rate of coin depreciation might be desirable to allow for absorption of future demand shocks [26]. A coin depreciation rate can be applied by gradually increasing the mining rewards over time.

3) Open mining using Proof of Sequential Work: If block speed should remain constant, a different way to build a more stable currency is to build a secondary token. This token would use Proofs of Sequential work (PoSW) [27] 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 less when it is low.

PoSW has the benefit of scaling better into the future as the sequential speed of processors improve at a much slower rate than parallel speeds.

V. DISCUSSIONS OF STABLECOINS

Stablecoins are an even younger development in the young field of cryptocurrencies. As such it isn't yet clear how the future of stablecoins will look. In addition to the currently existing stablecoins and proposed stablecoin concepts, research is being done into the general viability and security of stablecoins. This section discusses the viability of stablecoins and aims to answer more general question about their future and usefulness.

A. Centralised Stablecoins

Centralised stablecoins have so far found their usecase as a stable way to store your crypto away from volatility and bear markets. When looking to the future, much literature is available exploring where stablecoins can become useful.

When looking at ways cryptocurrencies can improve the current financial system centralised stablecoins can be seen as a midway solution [28]. It marries the stability and legal security of central trusted organisations, with the benefits of fast, programmable and more transparent payment systems [7] [29]. This leads to a system that relies less trust in large banks.

B. Crypto Collateralized Stablecoins

Decentralised currencies are more aspirational. Where Bitcoin provided a completely trust less currency. Decentralised currencies aim to do the same, but with guarantees about price stability. Though this is much more difficult to get working securely [30], the benefit of these coins to society might be much greater than that of any centralised currency.

Separate from the issue of price stable currency, many decentralised stablecoins have shown decentralised alternatives to mechanisms like contracts for difference [TODO cite something]. Even if these mechanisms don't end up working for stablecoins in the long term, they still mark an important step in the world of Decentralised Finance (DeFi).

C. Related Work

[Bladwijzer - All above is somewhat done, all below is worked on]

1) *Surveying the stablecoin space*: In “The State of Stablecoins”[31] 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” collateralized, crypto collateralized 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.

2) *Speculating on the future of stablecoins*: In [7] 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.

In “Stablecoins in Cryptoeconomics. From Initial Coin Offerings (ICOs) to Central Bank Digital Currencies”[29] 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 [28] 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.

3) *Critiques of common techniques for cryptocurrency stabilisation*: Chohan discusses the difficulties in maintaining a properly collateralized peg in “Are Stable Coins Stable?”[32]. Chohan describes how maintaining a true 1:1 peg leads to funding and scalability issues.

In [30] 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-collateralized 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.

VI. 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.

REFERENCES

- [1] R. Fugger, “Money as ious in social trust networks,” MONTHH YEARR.
- [2] Martijn de Vos and Johan Pouwelse, “TrustChain.” <https://repository.tudelft.nl/islandora/object/uuid:c51ac99d-3013-44b3-8ddd-fbd951a2454a>, MONTHH-YEARR.
- [3] The Maker Team, “MakerDAO whitepaper.” <https://makerdao.com/whitepaper/DaiDec17WP.pdf>, MONTHH-YEARR.
- [4] K. Menger, “On the Origin of Money,” *The Economic Journal*, vol. 2, no. 6, pp. 239–255, Jun. 1892.
- [5] A. C. Pigou, “The Value of Money,” *The Quarterly Journal of Economics*, vol. 32, no. 1, pp. 38–65, Nov. 1917.
- [6] R. N. Cooper, R. Dornbusch, and R. E. Hall, “The gold standard: Historical facts and future prospects,” *Brookings Papers on Economic Activity*, vol. 1982, no. 1, pp. 1–56, 1982.
- [7] D. Duffie, “DuffieDigital and fast payment systems,” MONTHH YEARR.
- [8] JPMorgan Chase & Co., “J.P.Morgan coin announcement.” <https://www.jpmorgan.com/global/news/digital-coin-payments>, MONTHH-YEARR.
- [9] “Libra whitepaper.” <https://libra.org/en-US/white-paper/>, MONTHH-YEARR.
- [10] Tether International Limited, “Tether whitepaper.” <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf>, MONTHH-YEARR.
- [11] CENTRE Consortium, “Centre whitepaper.” <https://www.centre.io/pdfs/centre-whitepaper.pdf>, MONTHH-YEARR.
- [12] Charles Cascarilla, “PAXos whitepaper.” <https://account.paxos.com/whitepaper.pdf>, MONTHH-YEARR.
- [13] LLC TrueCoin, “Trust token.” <https://www.trusttoken.com/trueusd>, MONTHH-YEARR.
- [14] STASIS Foundation, “Stasis whitepaper.” <https://stasis.net/>, MONTHH-YEARR.
- [15] Charles Cascarilla, “PAX gold whitepaper.” <https://www.paxos.com/paxgold/>, Sept-2019.
- [16] Anthony C. Eufemio, “DigixDAO whitepaper.” <https://digix.global/whitepaper.pdf>, MONTHH-YEARR.
- [17] Reserve Currency Solutions, “Globcoin whitepaper.” <https://globcoin.io/assets/pdf/whitepaper-Globcoin-v3.1.0.pdf>, MONTHH-YEARR.
- [18] X8 AG, “X8currency whitepaper.” <https://x8currency.com/wp-content/uploads/X8-Project-TGE-Whitepaper>.

pdf, MONTHH-YEARR.

[19] David Zimbeck, “BitBay whitepaper.” <https://bitbay.market/downloads/whitepapers/bitbay-dynamic-peg.pdf>, MONTHH-YEARR.

[20] Anchor AG, “Anchor whitepaper.” <https://theanchor.io/whitepaper/>, MONTHH-YEARR.

[21] Josh Chen Nader Al-Naji and Lawrence Diao, “Basis whitepaper.” https://www.basis.io/basis_whitepaper_en.pdf, MONTHH-YEARR.

[22] Brandon Iles Evan Kuo and Manny Rincon Cruz, “Ampleforth.” <https://www.ampleforth.org/paper/>, MONTHH-YEARR.

[23] Jordan Lee, “Nubits whitepaper.” <https://nubits.com/whitepaper>, MONTHH-YEARR.

[24] Steve Ellis, “Chainlink whitepaper.” <https://link.smartcontract.com/whitepaper>, MONTHH-YEARR.

[25] K. Saito and M. Iwamura, “How to make a digital currency on a blockchain stable,” *Future Generation Computer Systems*, vol. 100, 2019.

[26] M. Iwamura, Y. Kitamura, T. Matsumoto, and K. Saito, “Can we stabilize the price of a cryptocurrency?: Understanding the design of bitcoin and its potential to compete with central bank money.”

[27] R. B. Yuhao Dong, “Elasticoin: Low-volatility posw,” MONTHH YEARR.

[28] J. P. Koning, “Fedcoin_Central_Bank_R3.pdf,” <https://www.r3.com/reports/fedcoin-a-central-bank-issued-cryptocurrency/>, MONTHH YEARR.

[29] M. Dell’Erba, “Stablecoins in cryptoeconomics. from initial coin offerings to central bank digital currencies (cbdc),” MONTHH YEARR.

[30] A. M. Arian Klages-Mundt, “(In)stability for the blockchain: Deleveraging spirals and stablecoin attacks,” MONTHH YEARR.

[31] T. B. Team, “The state of stablecoins,” MONTHH YEARR.

[32] U. W. Chohan, “Are stable coins stable?” MONTHH YEARR.