Institute of Decentralized Economics

BROUGHT TO YOU BY  sweetbridge™

Stablecoin Protocols

by Warren Weber

OCTOBER, 2018

October 2018

Stablecoin Protocols

Warren Weber[1]

Grab almost any economics textbook that discusses the characteristics of a good money and you will find that the ability to store value is very high on the list. People want a medium of exchange that they are confident will hold value until the time when they want to spend it. In other words, people want a currency with stable value.

One can see the desire that national currencies be good stores of value in the inflation targets set by some central banks today. In the Eurozone, the United Kingdom, and the United States price stability is now thought to be an annual consumer price inflation rate of 2%, and the European Central Bank, the Bank of England, and the Federal Reserve has all implicitly or explicitly adopted 2% as their inflation rate target.

Some issuers of digital currencies that have their own native monetary unit also want their currencies to enjoy (gain?) widespread acceptance and circulation. They realize that in order to achieve this objective, they have to provide confidence through their protocols that their tokens will hold value over time. One way to do this is to promise to redeem the token 1:1 against the USD. A second way is create a protocol that will keep the currency trading close to 1:1 against the USD in the market even though redemption is not promised. Tokens issued with either a redemption promise or an intention to peg to the USD are commonly referred to as stablecoins.

At present, existing and proposed stablecoin providers can, for the most part, be divided into three distinct groups. The first group are the 100% USD reserve stablecoin providers. They promise 1:1 redemption. The second group, which I will call "crypto financial entities," act very much like standard depository institutions except that (i) they issue digital currencies in their own native monetary units instead of deposits and (ii) they do not promise redemption. The third group, which I will call "crypto central banks," behave very much as central banks in the ways that (i) they issue of their own currencies and (ii) attempt to achieve confidence that their currencies will hold value over time.

Here I describe in general terms how each of these groups attempts to provide a stablecoin by considering: (i) the number of coins issued, (ii) the way in which coins are obtained by potential holders, (iii) the allowable collateral, if collateral is part of the protocol, (iv) the issuer's stability commitment (promised redemption versus pegging), and (v) the mechanism to achieve stability. Of these, the stability mechanism is by far the most important, and the one I focus on the most.

100% USD Reserve Stablecoins

Issuers of 100% reserve stablecoins issue only a single token. It is obtained from an issuer by sending USD to an exchange and receiving the issuer's tokens 1:1 in return. Issuers promise to redeem their tokens 1:1 in USD when the holder demands. This is accomplished by

[1]Owner, Webereconomics and former Senior Research Officer at the Federal Reserve Bank of Minneapolis.

the holder telling an exchange to undertake such a transaction. The effect of the redemption commitment is to turn these stablecoins into a liability of the issuer.

Obviously, promised redemption is only credible if the stablecoin issuer maintains USD reserves equal to (or greater than) the value of stablecoin issued. This immediately raises the question, *Quis custodiet ipsos custodes?* (who guards the guards?). How can the holders of such a stable coin be certain that the issuer is in fact holding 100% reserves? If the holder wants to verify the reserve, is it known where are the reserves are held and it what form? As it seems unlikely that the issuer will keep the USD in a vault somewhere, it is likely that the issuer holds the USD as reserves with some financial institution or institutions, a third party or third parties. The question then becomes how trusted are these third parties. Can these third parties come up with the promised USD should the stablecoin issuer demand payment from them?[2]

There is an opportunity cost to the issuers of 100% reserve stablecoins, the interest foregone by holding USD reserves rather than interest earning assets. This opportunity cost can be offset in two ways. If the reserves are held as deposits in a financial institution, the stablecoin issuer may earn interest on those deposits. Or, the issuer may charge as small fee for redeeming its stablecoin. Of course, this means that the promised redemption is not actually 1:1.

The stability mechanism for 100% reserve stablecoins is arbitrage. Any difference between market price and the 1:1 redemption "price" guaranteed by the issuer offers a guaranteed profit opportunity to current or potential holders of the stablecoin. If the market price is above 1:1, the holders can earn a guaranteed profit by taking their stablecoin to the market, selling it for USD and then getting back more stablecoin from the issuer. If the market price is below 1:1, then holders can earn a guaranteed profit by redeeming their current holdings at the issuer and taking the proceeds to the market to buy more stablecoin than they had originally. In either case, the actions of stablecoin holders to take advantage of the arbitrage opportunity work to drive the market price toward 1:1.

Coins that use the 100% reserve approach: Tether, TrueUSD, StableUSD, Circle.

Crypto "Financial Entities"

I call the second approach to issuing stablecoins crypto financial entities (CFEs) because it has many similarities to how commercial banks operate. Under the protocols that use this approach, individuals obtain new stablecoins by borrowing. That is, individuals obtain stablecoins from the issuer in exchange for promises to pay them back in the future. These promises are backed by pledges of collateral. Thus, CFE coins are analogous to the depsits individuals obtain from banks when they take out loans.

Under the protocols that use this approach, the amount of stablecoin borrowed plus any fees must be paid back in that particular stablecoin. Borrowings cannot be extinguished by a payment of USD.

There are two kinds of collateral that can be pledged under the CFE approach. The first is outside collateral. Outside collateral is assets issued by entities that exist outside outside the protocol. Examples would be bonds, stocks, promissory notes, receivables, property, and

[2]The "who guards the guards?" problem occurs with respect to any coin that promises redemption be it in USD, gold, or something else.

so forth. The other is inside collateral. Inside collateral is an asset or assets issued inside the protocol itself. That is, inside collateral is any additional coins issued by the protocol.

As is the case with most borrowing from commercial banks, the USD value of the collateral pledged is required to be greater than the USD value the coins received. Collateral is only released back to the borrower when the loan is paid off.

In an attempt to make certain that borrowers can always pay off their loans, CFE protocols contain provisions for the revaluation of collateral to ensure that the ratio of the market value of collateral to borrowed stablecoin is always greater than some value α, which is much larger than 1. If the ratio of the market value of collateral to borrowed stablecoin should fall below α, the protocols generally contain a "call provision." That is, they demand that the borrower either provide additional collateral or reduce the amount borrowed, so that the ratio of the market value of collateral to borrowed stablecoin is once again greater than α. Should the borrower fail take these actions, the protocol gives the issuer the right to sell the collateral to pay off the loan. (If the proceeds of the asset sale are greater than the amount borrowed, the excess is returned to the borrower.)

Despite the similarities between crypto financial entities and commercial banks, there is one extremely important difference. The currencies issued by commercial banks are liabilities of the bank because the bank promises to redeem them 1:1 in USD. The stablecoins issued by CFEs, however, are not liabilities of the issuer because there is no promised redemption. In place of the redemption promise, CFE protocols include one or more mechanisms intended to keep the market value of the stablecoin in range $1 \pm \delta$ with respect to the USD, where δ is some small number.

One stablization mechanism for CFEs is arbitrage. Arbitrage works for CFEs similar to how it works for 100% reserve stablecoins, except that the agents on the other side of the transaction are the borrowers themself. Suppose that the market price of the stablecoin were to fall below 1:1. Then it would pay for borrowers to buy stablecoin with USD in the market and use the proceeds to pay off their loans. The saving would be the difference in the market price and 1:1, which is the ratio at which the borrowers have to pay back the loan. If the price of the stablecoin were rise above 1:1, then the borrowers should sell their stablecoin in the market and end up with more USD than used initially to obtain the loan. Either way, the actions of borrowers should affect the market demand for the stablecoin and drive the price to 1:1.

This is how the stabilization mechanism is supposed to work. However, there are two weak links in this stabilization mechanism that may prevent the necessary changes in demand from occurring:

1. In the case in the market price is below 1:1, borrowers may not have the resources to take advantage of the possibility of paying off loans more cheaply. Their pledged collateral is locked until the loan is paid off. Other assets that the borrower might have on hand may not be liquid in the sense of being converted to USD in a timely way with incurring large losses. In fact, the desire to liquify not very liquid assets may have been the reason for taking out the loan in the first place.

2. There may be stablecoin in existence that were not generated by borrowing, but rather came into existence by an ICO or some other means. The holders of these stablecoins

may not have the same arbitrage incentives as borrowers. In fact, their incentives could be the polar opposite. If they were to see the market price decline, they might fear future price declines and "run" the stablecoin by putting their holdings on the market, driving the price away from 1:1.

A second stabilization mechanism is the collateral backing for the borrowed stablecoins. Presumably these assets can be sold on the market for USD, which can then be used to buy stablecoin in the market and support its price. A problem with collateral as a stabilization mechanism is that USD the value of non-USD assets is not guaranteed in all states of the world. This means that it is always possible that the CFE will not be able to have enough USD to intervene in the market and buy up the quantity of its coins necessary to maintain the desired price peg. Another problem is that the CFE cannot sell the collateral until the borrower is in default on some aspect of the loan contract, which may be too late.

A third stabilization mechanism, use by some CFEs, is "parking." If the market price of the coin falls outside the desired price range, the protocol automatically initiates an action to induce holders to "park" tokens with the issuer for some period of time rather than putting them on the market. Although the specifics differ by stablecoin, in all of these automatic mechanisms the incentive for holders to park their stablecoins rather selling them is that "interest" is paid on coins parked in terms of that stablecoin. A variation on this mechanism is that the CFE buys its stablecoin with its second token (usually called a "bond") that pays principle and interest in the future. Purchased stablecoin is "burned."

This stabilization mechanism also has a weakness, and it is one that affects all fiat currencies – multiple equilibria. All fiat currencies have one equilibrium in which they are valued and another in which they are not. Which of the two equilibria occurs depends on expectations. If agents expect that the currency to be valued in the future, then it will be valued today. If they do not expect it to be valued in the future, then it will not be valued today. If price of a stablecoin starts to fall, but holders believe the stablecoins will have value in the future, then they will keep them off the market today to earn the interest. However, if they do not believe the stablecoins will have value in the future, they will put them on the market and exacerbate the downward price pressure. In other words, parking as a stablization mechanism works if holders believe it will work, and it does not work if holders do not believe it will work.

Of course, often what can be achieved with positive rewards can also be achieved by negative rewards. One crypto financial entity, Havven, uses the negative reward rather than the positive reward approach. Rather than offering an incentive to not put stablecoins on the market, it punishes borrowers who do not reduce their borrowing (reduce their fraction of the supply of the stablecoin in the market). They do this by reducing the share of the protocol's revenues that that a borrower receives until she reduces her borrowing to what is considered the appropriate level.

Coins that use the crypto financial entity approach: Bridgecoin, Dai, NuBits, Nomin, Havven

Crypto "Central Banks"

The reason for calling this approach crypto central banking is that it has many similarities to how the Federal Reserve System and other central banks can affect the supply of money in

the economy and, in that way, influence the price level. The Fed, for example, can affect the money supply through open market operations. To increase the money supply, it can buy government securities with new Federal Reserve notes (money) it creates. To decrease the money supply, it can sell government securities for Federal Reserve notes, which decreases the amount of its money in the economy.

Crypto central banks (CCBs) act much the same way. Their stablecoin is their counterpart of Federal Reserve notes. Their counterpart of government securities is a second, interest-bearing token that is also issued by protocol. This second coin is explicitly a non-stablecoin and is distinct from the stablecoin, having its own name and symbol.

The supply of a CCBs stablecoin is changed by buying and selling it for the second token according to some rule that is supposed to stabilize the stablecoin's price against the USD. Although the specifics of the rule differ by protocol, all share the features of having stablecoin holders willingly decrease their holdings and reduce supply to receive interest through the second token when the prices falls below 1:1 and of exogenously increasing supply when the stablcoin's price rises above 1:1 against the USD in the market.

In the CCB approach, no holder of the stablecoin in is debt to the issuer. No holder has an obligation to pay back a debt, just as no holder of a Federal Reserve note has any obligation to pay anything to the Fed. This is the major difference between crypto central banks and crypto financial entities. Thus, the protocols of CCBs contain no discussion of collateral. It should also be noted that the discussions of the CCB protocols contain no discussion of how the stablecoin comes into existence initially. The focus is on how the supply is changed to achieve 1:1.

The weakness with the CCB approach to stablization lies with the second coin. Again, it is a fiat currency, so multiple equilbria. There is nothing in the CCB protocols that back the value of the second coin. Whether this coin has value solely depends upon people's expectation that it will have value in the future. Should this expectation become questioned, the second coin will immediately lose its value and be worthless to act as a part of the stabilization mechanism. This is a major difference between crypto central banks and actual central banks. Government debt will always have value because of the ability of governments to tax to obtain the resources to pay it off. Crypto central banks have no such power.

Coins that use the crypto central banks approach: Basecoin, Carbon, USD Fragments