Institute of Decentralized Economics

BROUGHT TO YOU BY sweetbridge™

# Stablecoin Design: Lessons from Central Counterparty Clearing

*by Cyril Monnet and Warren Weber*

MAY, 2019

# Stablecoin Design: Lessons from Central Counterparty Clearing

Cyril Monnet and Warren Weber*

New stablecoins, cryptocurrencies intended to have a 1:1 exchange rate against a national currency, are appearing almost weekly. The reason for their appearance is that stablecoin holders do not have to worry that the coin will lose value, which simplifies trading, creates liquidity, and potentially increases broad adoption of the coin. How can stability of the coin against the national currency be achieved?

It is easy to maintain a 1:1 exchange rate if the value of the stable coin begins to increase. Using the principle that abundance erodes value, it suffices to issue more coins. But how can 1:1 be maintained if the stablecoin begins to lose value? Using the principle that scarcity increases value, one could be tempted to argue that it suffices to withdraw some coins in circulation, by buying them for example. However, it is too easy for speculators to short the coin, betting that the issuer will stop buying the coin because of a lack of resources. This is a well-known strategy that explains the demise in 2001 of the Argentinian peso currency board, as the Argentine central bank ran out of dollars to maintain the fixed exchange rate against USD. But if not even a central bank can maintain its exchange rate against another currency, then who can?

Here, we argue that an institution issuing a coin can work toward achieving stability by holding sufficient collateral. We then argue that a stable coin is akin to a futures contract cleared by a central counterparty (CCP). Once the equivalence is made clear, risk management techniques used by CCPs can be directly applied to institutions issuing a stable coin. Throughout we assume the stablecoin is attempting to maintain 1:1 against USD.

## 1 The need for collateral

Suppose that an issuer puts in circulation a coin designed to be stable but unbacked, in the sense that there is no collateral attached to the coin. Since the coin is designed to be stable, the issuer makes the implicit promise that the value of the coin will always be, say, one dollar. This implies that the issuer will have to use a “buy mechanism” whenever the coin’s value fall below one dollar. Redeeming coins – giving one dollar to any holder of a coin who asks for redemption – is one such mechanism.

Now, because the coin is unbacked, its value is determined by (1) the value of the future service it gives to its holders (one such service is the opportunity to exchange it for goods or other currency in the future) and (2) the credibility of the issuer to implement the buy mechanism.

*Monnet, University of Bern and Center Study Center Gerzensee; Weber, Owner WeberEconomics and Lead, Institute of Decentralized Economics

Whenever this service is thought to have an ever increasing value, the value of the coin increases and it is easy for the issuer to satisfy the exchange rate. The credibility of buy mechanism will not be tested.

However, if the demand for the service dwindles, so will the value of the coin. It may then be difficult for the issuer to satisfy the exchange rate, even more so if its credibility is eroding. The only way for the issuer to satisfy the exchange rate is to get unlimited access to dollars. Its credibility or reputation can help by allowing the issuer to borrow dollars if needs be. But, as was learned during the 2008 crisis, even secured borrowing can be fragile. Hence, it is unlikely that the coin will be stable unless the issuer of an unbacked digital coin is a central bank or has unlimited access to a central bank.

Now consider the case when the coin is backed by collateral. The coin then becomes a collateralized claim, secured by a specific asset, or a pool of assets. The collateral could be the issuer's equity for example.

A backed coin works as follows: The initial buyer of the coin pledges some assets as collateral to the coin issuer. This collateral can be cash or other assets. In the case of other assets, it is likely that the value of the collateral the buyer pledges will be higher than the value of the coins received. The difference between the value of the coins the buyer receives and his/her collateral pledged is a "haircut." The buyer may or not be required to "sell" the coins back to the issuer (pay back the loan) at some point in time. When the buyer sells the coins back to the issuer, he/she receives back the pledged collateral.

Using good collateral is useful to maintain the stability of the coin because it can be sold to fund the purchase of coins in case the coin loses value. There is one problem: the initial buyer of the coin has first lien on the collateral. However, this problem can be overcome with the agreement that the coin issuer could sell the collateral if some pre-agreed criteria are satisfied. This could be "easy" to do with smart contracts.

It may seem weird that the buyer would prefer to pledge her assets as collateral than to sell them to get cash (or whatever means of payment). There are several, possibly distinct, reasons why this might be the case. One explanation is that the collateral may be more valuable than the current market price to the buyer of the coins because she has some private information about the future value of the collateral. A second explanation is that she needs the assets in her production process.

In the next section, we take the argument that collateral is needed a step further and compare backed (or collateralized) coins to futures contracts cleared by central counterparties.

# 2 What are central counterparties (CCPs)?

Traders often use contracts that entail future promises, for example futures contracts. A futures contract specifies that one of the traders promises to deliver some goods or assets at a future pre-specified date for a pre-agreed price. It is easy to realize that once they sign the contract, both traders are exposed to counterparty risk, the risk that one of them will default on his or her promises: The trader who has to deliver the good or asset could default, or it could be that the one who has to pay for the good or asset defaults. To limit or even eliminate counterparty risk, traders have set up an insurance mechanism known as central counterparty (CCP) clearing.

Eliminating counterparty risk promotes market liquidity, the ease with which contracts can be traded. When they use CCP clearing, traders no longer have to care who they trade with, as they know they are insured by the CCP. Also, historically, CCPs have controlled the quality of the good to be delivered (e.g. grains at the Chicago Mercantile Exchange) thus making more uniform the types of contract that are traded on a platform. Trades can become seamless, as fewer steps (verification of counterparty quality, bargaining over the quality of the good to be delivered, etc.) are needed to conduct a trade. Because it promotes trade and liquidity, CCP clearing has been adopted on many trading platforms for many types of contracts (although not all).

The first step used to reduce counterparty risk, is a legal one. Once two traders agree on a contract, the CCP novates the contract. This means that the CCP interposes itself between the buyer and the seller and replaces the contract that the traders just agreed on with two contracts: One between the CCP and the buyer of the contract and another between the CCP and the seller of the contract. Following novation, the CCP becomes the sole buyer to the seller, and the sole seller to the buyer.

When all goes well, the seller of the contract delivers the good to the CCP, and the CCP in turn delivers the good to the buyer. The major consequence of the novation process is when one of the trader defaults. Then only the CCP has to deal with this default, and the other trader does not have to suffer as long as the CCP makes good on its obligations.

CCPs use different tools to make sure they can make good on their obligations. First, CCPs screen traders before granting membership in the CCP or clearance to use the CCP. For example the CCP may require a trader has enough equity or is vetted by a sufficient number of other clearing members. The CCP may also collect sufficient hard or soft information in favor of the trader (e.g. good reputation, etc.).

Second, CCPs discipline their members by requiring that they pledge resources, so that traders have enough “skin in the game.” They use two instruments: contributions to a default fund and margin calls. Default fund contributions are like membership fees: traders have to make their contribution – usually in cash – before they even know how much or how often they will trade the contract cleared by the CCP. Default fund contributions are normally calculated based on the previous volume of trades for a specific trader. The CCP has to manage this default fund in the safest way, maybe investing the cash in the fund in Treasury securities or other very safe and extremely liquid assets.

In addition to a default fund contribution, the CCP can require that traders post margins for each contract they clear through the CCP. Margins can be of two sorts: initial margins posted at the initiation of the contract, and variation margins which modify the amount posted initially, so that the value at risk for the CCP remains more or less constant.

As an example of how a CCP works, consider how a CCP would clear an oil futures consisting of delivering 10 barrels of oil on October 1st at a price of $35 each. Looking at the historical price of oil, the CCP expects the price of oil to increase to $40 with probability 0.25, to decline to $30 with probability 0.25 and to remain at $35 otherwise. For simplicity, suppose the CCP does not want to bear any risk. To clear the contract the CCP will require initial margin $m_s$ from the oil seller and $m_b$ from the oil buyer. Both traders also have contributed $d$ to the default fund, so that the total resources of the CCP are $m_s + m_b + 2d$. Denote the price of oil when the contract matures by $p$. So $p$ can be $30, 35 or 40.

When traders do not default the flows of funds and oil are as follows: On October 1st, the CCP collects 10 barrels of oil from the seller of oil, and $350 (10 × 35) from the buyer of oil. Then the CCP delivers the 10 barrels to the buyer and $350 to the seller. The seller's benefit amounts to $350 - 10 \times p$, so that he makes a loss whenever $p > 35$ as he could have sold the oil for $p > 35$ instead. The buyers benefit is the reverse $10 \times p - 350$ because she purchased 10 barrels for $350 but can now sell them at the spot price $p$. So if $p < 35$ the buyer makes a loss because she could have purchased the oil at $p < 35$ instead. Therefore, unless the realized price is the expected $35, one of the traders has an incentive to default on the contract.

To give traders the incentive to fulfill their promises, the CCP will require initial margin $m_s = m_b \geq 50$ and will only surrender these margins when the traders pay their obligations to the CCP on October 1st. This is enough to re-establish incentives because the seller's benefits of making good on the contract is now $350 + 50 - 10 \times p$. So even if the price of oil increases to $40, the seller will prefer delivering the oil as he would lose his initial margin otherwise. We can apply the same argument to the buyer to understand why $50 initial margins suffice to discipline her.

To understand variation margin, suppose the price distribution is now $p \in \{20, 30, 35, 40, 50\}$ with probability $\pi = \{0.01, 0.24, 0.5, 0.24, 0.01\}$. So there is a 1% chance of an abrupt oil price increase, and a 1% chance of a sharp oil price decline. The CCP may still choose to set initial margins to $50. But now suppose the CCP receives a public signal on July 31st that the price of oil is very likely to increase to $50. Then the CCP may require the seller to pledge additional margins $\upsilon$ such that $350+50+ \upsilon -10\times 50 \geq 0$, that is $\upsilon \geq 100$. This additional margin is called variation margin and is used to control the imbalances in the amounts due from traders when the contractual environment has changed since the novation of the contract.

Finally, CCPs mutualize the losses of members: CCPs will tap into their default funds in case they need cash to make good on one of their contracts. For instance, let us return to our example and assume that the seller defaults while the price unexpectedly increased to $50 per barrel. This means that the CCP only has $m_s = 50$ from the seller and the $350 received from the buyer. But the CCP needs to buy $500 worth of oil to deliver the 10 barrels to the buyer. So the CCP is short $100. Because the CCP must honor its contract, the CCP will put the default fund to contribution. If the CCP has 11 clearing members, it will first use the contribution from the defaulting seller (say $20) and then split the remaining $80 on the remaining 10 members. So they will each pay $8.

In short, the CCP mutualizes its losses among all clearing members. Mutualization is an essential element of the insurance mechanism inherent in the CCP: Members in the CCP arrangement agree to have to their own resources at stake in case a large default occurs. Initial and variation margins are important, but in the case of a large set-back, mutualization is the guarantee that the contract will go through.

CCPs have been pretty successful at guaranteeing contracts. Even during the height of the financial crisis in 2008, no CCPs failed and no CCP had to tap into the members' default fund contributions.

## 3 Secured crypto coins as futures contracts

Now consider the following situation. There are two traders, who for convenience we will name Bob and Alice. Bob has no cash but wants to purchase some goods from Alice. However, Bob has some assets that he could use as collateral if Alice deems it of sufficiently high quality to accept it as such. The implicit assumption here is that Bob does not want or cannot part with the asset, so that the asset itself cannot be used as means of payment. For example, Bob may have ETH but believes that ETH will be more valuable in the future so that he prefers to hold on to it rather than sell it at today's price that he thinks is not in line with ETH's future value.

In this context, Bob and Alice could trade in at least four ways. First, Alice could agree to extend an unsecured loan to Bob. Bob, the borrower would promise to repay the loan plus interest at a later date. In this case, Alice is fully liable in case Bob cannot or is unwilling to pay. For example if Bob goes bankrupt, Alice has no recourse to Bob's assets and may be left empty handed once the bankruptcy procedure is terminated. So Alice will only extend an unsecured loan to Bob if she can trust that Bob will repay.

Now suppose that Bob is not trustworthy. Then, the second way in which Bob and Alice could trade is to agree to a secured loan. Precisely, they would agree that Bob borrows money/goods from Alice by pledging some of his assets as collateral directly with Alice, or held in custody by a third party –the custodian – against the loan with the understanding that Alice or the custodian releases the collateral as soon as Bob pays back the loan at a pre-specified date and rate. In a secured loan, Alice is directly subject to counterparty risk if Bob cannot pay back the loan as agreed. But in case of default, the custodian releases the collateral to Alice who would sell it to recoup part of her loss.

In this case, Alice may be subject to the market price risk of the asset used as collateral, the risk that the price of the asset is low. To protect against this risk, although imperfectly, Alice may require Bob to pledge assets for a higher value than the principal value of the loan. The difference is called a "haircut." In financial markets, it is common that haircuts for safe assets are set around 2%, so that borrowing $100 requires the pledge of $102 worth of assets. But haircuts can be negotiated bilaterally and higher haircut levels are possible.

Unfortunately, haircuts do not insure Alice against a large drop in the collateral value – in which case Bob may not be willing to repay Alice to get his collateral back – or insure Bob against the risk that Alice is not willing or able to give back the collateral when Bob pays back the loan. So counterparty risk is pervasive even in secured loans, and this limits their usefulness, especially when Bob and Alice do not know or trust each other.

The third way that Bob and Alice could trade is for Bob to buy the good from Alice using a custodian secured coin. In this set-up, the trade is the same as in a secured loan except that the custodian, Ivan, intermediates the trade between Bob and Alice by giving a receipt (a coin) to Bob when getting his collateral. This is useful when Alice does not know or cannot check that Bob holds collateral with Ivan. Here is how this works: Bob would first place his assets in custody with Ivan. Ivan would then issue coins to Bob specifically linked to Bob's collateral. The "link" is that the holders of such coins can trigger the release of Bob's collateral held in custody after a pre-specified date. Ivan could require haircuts: for each $1 worth of coins Bob would have to place $1.02 worth of his assets in custody. Bob would then use Ivan's coins as collateral with Alice. If Bob pays back Alice, he gets back the coin and so regains access to his collateral. If Bob does not pay back Alice at the convened time, Alice redeems the coins with Ivan who releases the collateral to Alice. So the outcome of trading a secured loan or using custodian secured coins is the same. In particular, Alice is not made whole if value of Bob's collateral drops when Bob defaults. The reason is that the role of the custodian is merely to hold assets in custody. The custodian is not guaranteeing the value of the coins. Also, notice that Alice could sell the coin before Bob's repayment date. In this case, Bob could repurchase the coin at the repayment date from whoever holds it in order to get back his collateral from Ivan.

It is important to notice that Ivan's coins are similar to tradable and secured (although not safe) futures contracts: They specify that Bob delivers some goods or assets at a future pre-specified dates to Alice for a pre-agreed price, and Alice can trade Bob's promise by just selling the coins to another trader. Now, the coins may not be easily tradable because other traders may not know the quality of the collateral backing the coins. So the next step is to denominate the coins in currency (say USD) rather than in terms of Bob's collateral placed in custody.

Consider one final arrangement where Bob could buy goods from Alice using a custodian secured coin denominated in its own native currency. The only difference with the previous arrangement is that the custodian's coin is no longer a claim to Bob's collateral or linked to the value of Bob's collateral. Rather, a coin denominated in its own native currency entitles its holders to a certain amount of that currency, either by trading it or by redeeming it, or both. Under this configuration, Bob would first place his assets in custody in exchange for some of Ivan's coins. Again, the custodian could impose some collateral haircuts, so the face value of Ivan's coins could be lower than the market value of the collateral placed in custody. If Ivan promises to redeem his coins in USD, say, there could be a redemption date specified on the coins, either for their USD redemption value or for the collateral pledged by Bob. However, in the end it is important that Bob can repurchase his collateral from the custodian, either by returning the correct value in coins or in currency.

How does the trade between Bob and Alice happen then? With Ivan's coins in hand, Bob can now purchase goods from Alice. Alice can now either hold on to these coins, or spend them with whoever accepts them in trade. If the value of the coin is stable, Alice will obtain the face value of the coin when she sells it. After the redemption date, the holder of Ivan coins can continue trading them or can redeem the coins with Ivan. For example, Bob can buy the coins back from Alice or whoever holds them, and redeem the coins for his collateral if he prefers the collateral to currency. While the coins are redeemable for dollars, they are still not safe: Ivan only has the USD value of the collateral and so may fail to redeem the coins if the dollar value of the collateral drops. In some sense, Ivan is like a fractional reserve bank, where Bob's collateral plays the role of reserves.

How does Ivan make sure that redemption is always possible at face value? If Bob's collateral value drops, can Ivan still redeems notes and what are the consequences on the value of Ivan's notes if he does? In other words, how can Ivan make the value of his notes stable?

# 4 Stable coins as CCP cleared futures contracts

In the previous section, we have seen that the custodian's coins can be seen as futures contracts. In this section, we argue that a custodian wanting to issue a stable coin can be compared to a CCP, so that management techniques of CCPs can be applied to custodians to stabilize their notes. In particular, the mutualization mechanism can be put in place in order to make the coin stable.

Let us understand why the custodian issuing currency denominated coins functions like a CCP. First, the custodian Ivan is interposing himself between Bob and Alice, because when he issues the coins to Bob in exchange for collateral, he effectively is the only counterparty to Bob. Also, in the redemption process, Ivan is the only counterparty to the coin holder Alice. Therefore, Bob and Alice are no longer subject to counterparty risk of Alice and Bob respectively, but only to the risk that the custodian fails to fulfill his promises.

Finally, in the context of CCP clearing, the CCP guarantees that the contract will go through (the buyer receives the good whatever happens to the seller, and the seller is paid upon delivery, whatever happens to the buyer). Here, the custodian's goal is to make sure that the borrower receives his collateral back if he wants to (whatever happens to the lender – Bob just has to repurchase Ivan's notes), and the lender gets her money back (whatever happens to Bob – either Bob repurchases the coins back from Alice, or Alice can redeem the coins with Ivan). So, the fact that the custodian's coins remain stable is akin to the CCP successfully insuring its members against counterparty and market price risk.

Once we realize that the custodian issuing stable coins can function just like a CCP, we can learn from the risk management techniques that CCPs use in order to fulfill their promises and apply them to the custodian so that his coins remain stable. Recall that CCPs use different instruments to fulfill their promises toward their members. These instruments are (1) screening and monitoring members, (2) disciplining them through default fund contributions, initial and variation calls, and (3) mutualizing losses. Here we describe how this set of tools can be applied by the custodian issuing coins so as to make them as stable as possible. To guarantee the value of his coin, the custodian must have, at any time, access to enough sufficiently liquid assets in order to fulfill the demand for redemption of his coins in circulation.

When the custodian has a similar structure as a CCP, the custodian has several sources of funds: collateral held in custody, margins, membership fees, and own equity.
When Bob places collateral in custody to obtain coins, Ivan will want to minimize the collateral price risk by requiring that the assets used as collateral are relatively safe. Depending on collateral quality, the custodian will haircut the collateral to protect against fluctuations in the value of the collateral. Still, it could be that the assets pledged as collateral lose value before the redemption date of the coins above and beyond the size of the initial haircut. In this case, the value of the collateral no longer covers the face value of the coins Bob obtained from Ivan. As for CCP clearing, the custodian can then call margins on Bob to cover the collateral shortfall. These margin calls could be made in terms of the original assets placed in custody, another type of assets, or cash.

If Bob satisfies the margin calls, then the custodian's coins retain their stability. In the case Bob fails to come up with the necessary margins, either unwillingly because he failed, or willingly because the margin call is too large, Ivan must come up with the additional funds. The fact that Bob did not satisfy the margin call can be considered as a breach of contract. In this case, Ivan gains ownership of Bob's total collateral held in custody. At this stage, Ivan has several options. If Ivan believes that Bob's collateral will lose more value in the future, he can sell it at market price before the redemption date. Otherwise, he can keep it until he considers the price is right in order to sell it. In any case, the custodian has to come up with the shortfall using other means than margins.

At this stage, the custodian's rules should be structured such that it has to use a pre-set fraction of its own capital. The reason is well known: By having its own funds at stake early on, the custodian's incentives are better aligned with a good management of its membership policy and collateral pool. If the pre-set fraction of the custodian's capital is not enough to cover the collateral shortfall, then the custodian would be allowed to tap into the funds set-up from member's contributions before notes have been issued. This is akin to the CCP's default funds contributions, and members should understand that the custodian can use these funds to maintain the stability of its coins if need be. These funds can be seen as membership fees. If this is still not enough, the custodian can contribute more of its own capital, or call for new equity injections from existing members, for example by selling some of the fraction of the collateral pledged by other users that is above the needed haircut (if Bob placed $102 in custody to get $100 worth of custodian coins, the custodian could sell $2 worth of that collateral). Using a similar argument as "proof of stake," existing members have all the incentives in the world to guarantee the value of the custodian's coins because the custodian may be holding their collateral and they may be holding some of the custodian's coins. In dire straits, it is key that the custodian has the ability to require and enforce contributions from its members. In the end, it is this insurance mechanism that plays a key role in guaranteeing the stability of the coin. So it is essential that the custodian screen users of the collateral custody – but not necessarily users of the coins which can be anybody – before granting membership to ensure that custodian users are trustworthy and able to satisfy margin calls and other calls to contributions favoring the stability of the custodian's coins.

We know it is impossible for CCPs to guarantee the settlement of all contracts under all circumstances. So, it should be clear that it is also impossible for the custodian to guarantee the stability of its coins under any circumstances. But notice that the mutualization of losses in both arrangements (that other members have to contribute their own funds to cover losses in value originating from a contract they did not sign) is an important element of the insurance that contributes to the stability of the mechanism.

Finally, it is important to stress that most stablecoins whitepapers do not mention membership conditions. But we can draw from the experience of CCPs to conclude that vetting members (or a subset of members) who can be put to contribution in order to stabilize the value of a coin could prove essential to the success of the coin.

# 5 Conclusion

Here, we have argued that borrowing arranged through the issuance of a cryptocurrency shares many traits of clearing futures trades via a central counterparty. As such, many features of CCPs can be used in order to maintain the stability of a cryptocurrency: screening, monitoring and disciplining members, and mutualizing losses. A large part of the stability relies on collateral, but also contributions by all members of the mechanism issuing the cryptocurrency. It will be important to vet members who have access to the coin directly through its issuer.