An Inflation-Resistant Stablecoin-backed Stablecoin

Wednesday, February 28, 2024
12:21 AM

Note: This lite paper describes and entry to the Renaissance Hackathon managed by Colosseum.
Version 0.3

by C. Tapang

Introduction

The problem that cryptocurrency ought to be solving is the coming calamity of an inflated USD, before it makes life difficult for everybody.

Bitcoin (BTC) has been proposed as alternative money. It's been more than a decade, and a lot of startups have tried to make a currency out of BTC, but this hasn't happened, and it appears it will never happen. Nowadays we look at the BTC network effects as an investment, a way to take advantage of its usefulness as a store of value, but not as a medium of exchange nor as a unit of account. BTC "monetary policy" is very simple: a hard-limited quantity. This has helped it gain value on its own, without reference to (or backing by) any pre-existing common medium of exchange. BTC is like a commodity you buy from an exchange. Its price is its monetary value. Setting aside the question of why it has value, that value is directly proportional to demand while inversely proportional to its supply. Its supply is fixed at 21 million BTC (or less, depending on how many units have been lost), therefore its price is determined by demand alone. Market demand for BTC fluctuates wildly, and this is why it is very volatile.

Bitcoin is like gold, a real commodity. However, gold supply has been much more flexible than BTC's such that whenever its price rose, miners are incentivized to mine more of it. Gold supply therefore matches demand somewhat; that's why gold price has been much tamer than BTC price. Gold served as good money for centuries before paper money came along. The problem with gold is that it is heavy and not easy to carry around or just keep in one's possession; it was therefore superseded by paper money, even though paper money value was backed by gold value, for a while.

The problem with BTC is that it is volatile, with an ever-upward long-term trend. On the spend side, not too many people want to spend it because of its long-term upward trend. On the accept-side, not too many vendors want to accept BTC because of the risk it adds to the vendor's already risky business. A definite proof that, after more than a decade of use in crypto exchanges, BTC is still not being used as money is that BTC's daily trading volume divided by market cap (a good proxy for money velocity) remains among the lowest, all altcoins considered.

Now imagine this: take all the technology and characteristics of BTC - the fact that it is weightless, frictionless, fungible - and introduce another token with these characteristics but without BTC's volatility, and you get something that can become an honest to goodness medium of exchange, i.e., money, that is superior to fiat money. This is what stablecoins are all about.

The downside is that fiat-backed stablecoins are centralized: each stablecoin is controlled by a single entity, its issuer. Stablecoins can also be censored because this is what compliance requires. However, these shortcomings can be fixed if the law allows.

Stablecoins and Fiat Inflation

Just like paper money was backed by gold, the largest stablecoins today are backed by central bank money (fiat money). The promise behind these fiat-backed stablecoins is parity with fiat always (1 USDC will always be 1 USD, for example). What if the USD inflates? Fiat-backed stablecoins would inflate also because parity is the promise, and it would take a large amount of additional fiat backing (large amount of capital) to keep the value of a stablecoin with respect to its inflating backing.

In the aggregate, if we consider that USD held by stablecoin issuers to be non-circulating USD and for simplicity's sake we assume that such stablecoin is backed by USD (i.e., no other asset backs the stablecoin), then the corresponding stablecoin (say USDC) increases its quantity in circulation by the same amount that USD is no longer in circulation. In other words, if Qu is the simple count of USD in circulation (M2 may be) and Qs is the simple count of USDC in circulation, then if USD = USDC in value always and there is no USD inflation, then K = Qu + Qs should be constant. Therefore, whatever amount q is taken off the market from Qu gets added to Qs, such that.

$K = Qu = (Qu - q) + Qs = Qu' + Qs$
Where $Qs = q$ always, and Qu' is the quantity of USD remaining in circulation.

Stablecoins, even if q is large relative to Qu, by absorbing an increasing number of USD in circulation, cannot possibly cause inflation of USD because it reduces the overall count of USD in circulation by q. Even in the extreme case when q is so large that q approaches Qu, the process of absorption of USD by USDC cannot possibly cause inflation.

If 1 USDC = 1 USD, then it must be that $Qs = q$ at any time. Qs is the amount of USDC in circulation and q is its backing. Therefore, if Qu is not inflating (USD does not increase in quantity), then.

$K = Qu' + Qs$ and Qu' will always be less than the initial quantity Qu

Which tells us that, if $Qs = q$, the quantity of USDC in circulation cannot cause inflation of USD. In fact, by putting q of USD out circulation, USDC quantity Qs is disinflationary for USD.

Note that things get complicated if USDC is partially backed by T-Bills, as it is now. When the issuer of USDC (Circle) bought T-Bills, it used a large part of USDC backing (q) to do this. When this purchase occurred, suddenly the U.S. govt has billions more to spend and that part of q went back to USD in circulation. Did Circle cause this USD increase in circulation? If the U.S. government stopped borrowing money (stopped issuing T-Bills) can Circle even buy T-Bills?

If Qu is increasing (increasing USD broad money), K should increase by the same amount. This is inflationary for USD:

$K + d = (Qu - q + d) + Qs$

If $q = d$, it means that USD inflation just equals absorption by USDC backing. Inflation of USD remains proportional to d, and so does inflation overall (K inflation).

If q > d, it means the absorption of USD by USDC is larger than inflation; however, q still does not contribute to overall inflation.

The same is true about inflation when q < d.

Again, the whole point here is that, as long as every USDC is backed by a USD, the USDC stablecoin cannot cause inflation of USD. Only d (USD increase in quantity) can cause inflation.

Another way to look at the situation is that, if we imagine two economies, Qu' and Qs, the USD economy decreases in size by exactly the same amount (q) as the amount by which Qs increases. As Qs increases, the size of the economy in which it circulates increases also.

If USD inflation is not high (d is proportional to increase in size of world economy), USD backing for USDC remains equal to USDC in circulation and 1 USD = 1 USDC.

However, if USD inflation is high (d consistently higher than increase in size of economy), it should still be easy for Circle to keep 1 USD = 1 USDC during issuance and redemption, as promised, and USDC would therefore inflate with USD.

Inflation Resistance

Can we have a stablecoin that is inflation-resistant? Yes and this lite paper is about setting up an inflation-resistant stablecoin. The idea is very simple: make both issuance and redemption prices under absolute control of a smart contract and then calculate issuance price independently of redemption price. Issuance price can be greater than redemption price during times when fiat-backing is inflating. It is only when the fiat-backing is deflating (appreciating in value) that issuance price can be lower than redemption price. Issuance price can be determined by fiat inflation; however, redemption price is always equal to total fiat-backing divided by total amount of stablecoin in circulation. In other words, redemption price is always determined by total backing such that, even if all stablecoin holders redeemed, everyone can get back the equivalent amount of inflated fiat without causing a run.

Issuance price Pm is higher than redemption price Pr in an amount proportional to runaway fiat inflation. The price difference does not accrue to issuer profit, however; rather, it accrues to the backing alone. As the total backing amount q increases more than total stablecoin in circulation Qs such that q > Qs, so does redemption price increase because redemption price is simply equal to total backing divided by inflation-resistant stablecoins in circulation. That is,

Pr = q / Qs

Below we continue with specifics as it relates to a particular inflation-resistant stablecoin (ROKS). ROKS is backed by USDC or USDT and not directly by USD because of liquidity mismatch between stablecoins and USD and because both USDC and USDT exist in Solana as SPL tokens and are therefore amenable to programming with ROKS.

It may seem trivial, but the reason ROKS is named differently from other, USD backed stablecoins (which both incorporate "USD" in their symbols), is that, if USD inflates, it would be best for a new stablecoin not to be associated with USD. The non-USD derived symbol "ROKS" is an insurance against USD inflation. If ROKS inflates with USD, however, the symbol wouldn't mean anything. Clearly, we don't

want ROKS to inflate with USD (if and when it does). Let's now describe a game-theoretic system that can ensure this.

The Ideal is Not Zero Inflation

There is wisdom in TradFi that we should not ignore. Some of these bits of wisdom, like that zero inflation is not the ideal, has more than a century of human experience behind it. Here's one view: https://fee.org/articles/zero-inflation-a-flawed-ideal/

At this stage, it would not be possible to measure inflation for any stablecoin directly because no stablecoin can yet compare with USD in terms of use as common medium of exchange. We think of stablecoins as merely substitutes for fiat money. As such, stablecoins use the value of fiat as reference. However, when fiat like USD inflates more than 2%, we would like our stablecoin to keep its value to within 2% inflation by increasing the amount of fiat backing - in this case USDC or USDT backing.

Keep the price on par with fiat (USD) if inflation is within 2%, but diverge (or "lose the peg") if USD inflation goes beyond 2%. This keeps the inflation-resistance mechanism simple.

Note that there will be a time delay from the onset of above-2% inflation until ROKS catches up and increases its USD backing. This time delay will depend on the level of user participation in the arbitrage . This period of adjustment allows participants to make a profit and also allows ROKS backing to increase such that q > Qs.

The DeFi program raises the minting price Pm almost immediately when inflation is detected; but Pr can be slow to catch up because the backing q must increase first (in USD).

Details of Mechanics

The price regulator that sets Pm and Pr will use another, pre-existing Concentrated Liquidity Automated Market Maker (CLAMM) or a complex order-book DEX. We have looked at Dexlab:
OpenBook | Dexlab - OpenBook Explorer
Dexlab is based on OpenBook V2: openbook-dex/openbook-v2: openbook-v2 monorepo, contains solana program and ts client (github.com). OpenBook V2 allows market participants to provide liquidity and earn yield.
Creating a standard AMM Pool - (raydium.io)
OpenBook | Dexlab - OpenBook Explorer

We decided to interface directly with OpenBook V2 because it has an extensive pre-existing ecosystem of developers and front-end businesses. Plus, it has a large community in which technical support is available.

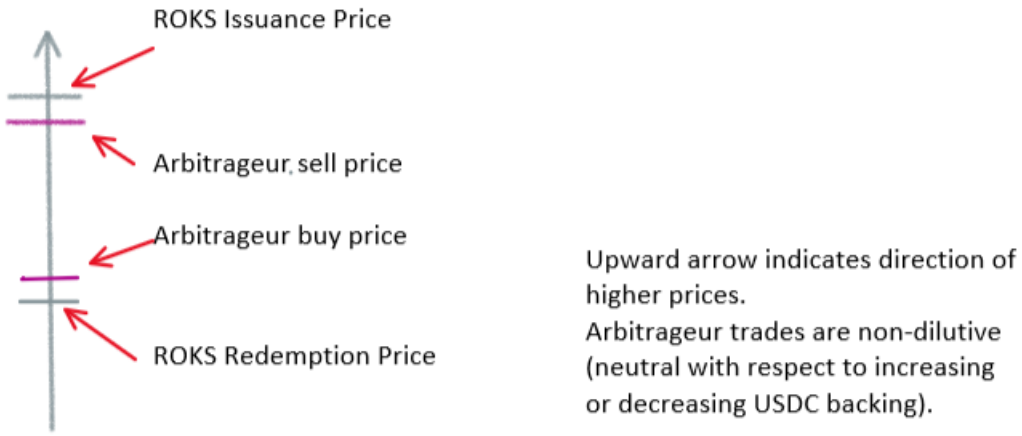
We started development work in time for the Renaissance Hackathon, with ROKS paired with just USDC. The issue rate and redeem rate should be fixed and slightly different, to start with maybe only 0.01 different: issue rate = 1.01 USDC and redeem rate = 1.0000 USDC. This level of difference between Pm and Pr won't be noticeable for amounts below 1,000 ROKS. These two rates are Rock Stable rates, which is set by the autonomous price regulator.

The issue rate and redeem rate are a big factor in determining the market rate, which is expected to be somewhere between Pr and Pm. The difference between Pr and Pm is used to earn more backing when USD and USDC inflate together: the issue rate can be raised while keeping the redeem rate the same, thereby increasing the USDC backing and the ROKS redeem rate. (The "redeem rate" being total backing divided by total ROKS in circulation.) The increase in USDC backing would be necessary if USD inflates (USDC is assumed to inflate with USD because USDC promises to be always 1 to 1 with USD).

Note: in this discussion, the word "issuing" means the same as the informal word "minting".

We are going to use a very simple mechanism to prevent ROKS from inflating with USD (and with USDC, its direct backing). At all times, when USD is inflating normally (2% or less), the ROKS issuance price Pm with respect to USDC is slightly higher than our redemption price Pr, by 0.01 USDC. There is not much room for arbitrageurs to make money, except for very large deals.

To increase USD backing when USD is inflating above the normal 2%, the price auto-regulator will increase the minting price Pm of ROKS. The increase should be proportional to the increase in USD CPI as broadcast by an oracle. For this we need a reliable USD inflation oracle (see Balaji's challenge on this and Trueflation's response). This would simultaneously reduce the demand for ROKS, especially because the redemption rate will not be raised similarly. This presents an opportunity to current ROKS holders and arbitrageurs. Current ROKS holders profit by offering ROKS at a lower price than the official issuance price; while arbitrageurs can buy ROKS higher than redemption price and sell ROKS at a lower price than issuance price and still make a profit. Participants can provide liquidity at these prices between Pr and Pm:



ROKS Redemption Price (Pr)

However much the arbitrageur buys, she also sells; therefore, her activity is neutral with respect to increasing or decreasing ROKS in circulation (and therefore also with respect to an increase or decrease of the backing). It is only an actual increase in overall demand that can cause the market price to increase up to the official ROKS Issuance Price and new ROKS would have to be issued. The market price cannot increase above the Issuance Price because the Rock Stable auto-regulator contract can simply

supply the demand, at whatever quantity. The Issuance Price therefore sets the upper limit of ROKS price with respect to USDC.

Note also that the arbitrageur/trader can choose to either hold ROKS or USDC after either or both trades:

- If arbitrageur currently holds ROKS and wants to keep ROKS, she sells and then buys back.
- If a trader currently holds ROKS and wants to end up with USDC, she just sells.
- If arbitrageur currently holds USDC and wants to keep USDC, she buys and then sells ROKS.
- If a trader currently holds USDC but wants to end up with ROKS, she just buys ROKS.

The most important thing to note is that, by increasing the issuance price without increasing the redemption price, the ROKS auto-regulator contract can increase the USDC backing of ROKS such that USDC backing > ROKS in circulation (or q > Qs, where q = USDC backing and Qs = ROKS in circulation). Another important thing to note is that it would be very risky for arbitrageurs to end up holding more backing USDC than when they started – arbitrageurs would always want to count their profits in ROKS rather than USDC or USD.

Nobody wants to hold an inflating currency, and by establishing that ROKS cannot go down in value along with the backing, we expect there to be increased demand even when the Issuance Price is increased. What better way to get rid of inflating USD than use it to buy USDC, and then use that USDC to buy ROKS. People can also buy BTC, but that is much riskier.

The redemption price can be adjusted by the auto-regulating smart contract such that 1 ROKS = (q / Qs) USDC which is absolutely safe because, even if all of Qs ROKS is redeemed, there is enough USDC backing q, showing that there is no possibility for a run even at a higher redemption rate. As q continues to increase above Qs, the redemption price can increase also, until it approaches the Issuance Price.

Pm = q / Qs
In units of USDC

The purpose of the higher issuance price is not for the issuer to profit, but rather to increase the backing q such that q > Qs, resulting in a higher Redemption Price Pr. A higher Issuance Price Pm therefore is a mechanism that protects ROKS from USDC (or USD) inflation.

How would RockStable profit? During the pre-inflation phase, RockStable earns mostly from the taker fees charged by OpenBook V2.

Minting or Issuance Price (Pm)

ROKS minting price is determined by two oracles: USD inflation and USDC exchange rate with USD. Our DeFi program picks up these two pieces of data from oracles and then follows a simple formula to set the minting price Pm:

Pm = Xr (1 + Yr)

Where Xr == market exchange rate between USDC and USDC (price of USDC in USD)
And Yr == last month's inflation rate or CPI when above 2% (set to zero if inflation rate is less than 2)

For example, if Xr = 1.0 and inflation is 3%, then Yr = 0.03 and Pm = 1.0 (1.03) = 1.03 USDC

It could be lower at 1.01 USDC (minus 2%); but 1.03 is better to speed up accumulation of USDC backing.

Can Pm be Set Lower than Pr?

Currencies become volatile on the way down. It may appear to make sense for Pm < Pr at times. However, setting Pm < Pr means the absence of a higher limit, and ROKS can go up in price uncontrollably (not good). Therefore, Pm > Pr always, even if the difference is small. That small difference can be part of the issuer's profit.

Participation

Anybody can participate in the profits to be made by LPs, by simply depositing either ROKS or USDC (USDT) into the liquidity pool for ROKS, at prices between Pr and Pm.

The automatic pricing mechanism for ROKS prevents it from inflating with the backing by accumulating more backing. More backing, beyond 1 to 1 parity, is accumulated by raising the issuance price Pm above Pr. The increase in backing would then raise Pr towards Pm. Once Pr approaches Pm, backing accumulation stops.

Whenever Pm is raised automatically, the spread between Pm and Pr gives an opportunity for participants to earn yield by opening bid and ask position at prices between Pm and Pr.

Initial Conditions

Initially, total ROKS in circulation is zero to very low. There is therefore practically no redemption that can occur. We, the issuers of ROKS, are going to deposit ROKS into a one-sided liquidity pool in OpenBook V2 at a fixed sell price and fixed buy back price. This allows anybody to exchange USDC for ROKS and maybe deposit ROKS (or USDC) as arbitrageurs, in order to earn more ROKS or more USDC.

Arbitrage

To prevent arbitrageurs from taking away some of the incoming USDC backing, We can increment Pm only when Pr reaches 90% of Pm.

Should we slowly Increase Pm so that arbitrageurs can't capture too much of the backing?

NO, we don't have to slowly increase Pm. Let the arbitrageurs make money. At least they would help increase market cap, which can only increase trust in ROKS. This would slow down the accumulation of backing and increase the time it takes for Pr to catch up with Pm, but that's fine. The important thing is that people would know for sure that the difference between Pm and Pr accrue to the benefit of the ROKS ecosystem. Having whale arbitrageurs helps ROKS by increasing the level of trust in the ROKS ecosystem. Besides, remember that it’s very risky for arbitrageurs to end up with more inflating USDC in their hands than they started with.

Soon enough, some of the big buyers will buy simply to avoid the effects of inflation. This kind of buyer won't care about Pm - they'd buy anytime and not sell. This kind of buyer helps Pr to catch up with Pm faster.

The size of the RockStable position at Pm in OpenBook depends on market size. Initially, we can set it to $100m. Once this size is almost sold-out, we can revise to double that initial size ($200m), maybe at a higher Pm, depending on USD inflation and USDC price. The size of the next increase will depend on how fast the next replenishment needs to be done. Just remember that we can mint up to the maximum number that can be accommodated by the integer size in Solana, minus 9 decimal places.

The ROKS amount that we can mint is very large. This is why no arbitrageur can beat us in this (our) game. A whale arbitrageur can buy as much ROKS as she can, but in the ROKS ecosystem there can be nobody that can have enough ROKS capacity as we do.

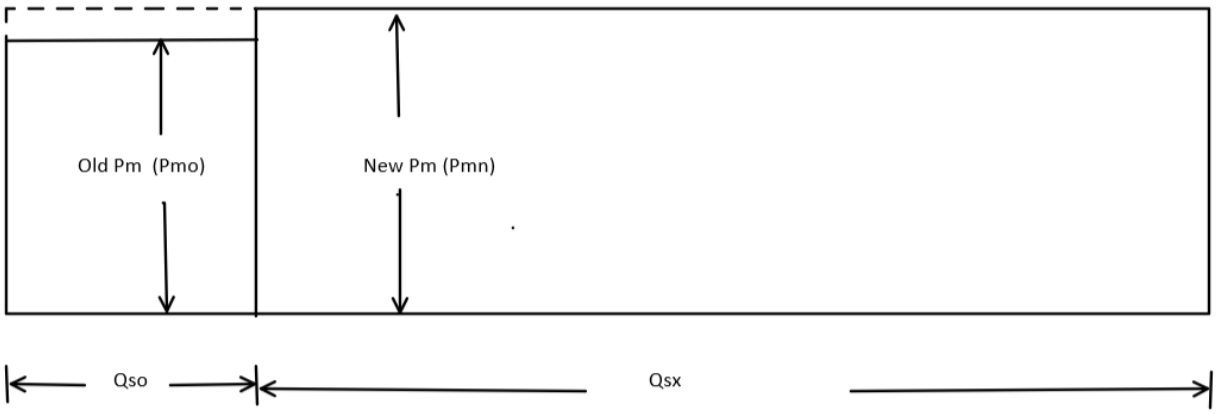
If / when USD hyper-inflates to oblivion, ROKS (and other competitors) would be there to take its place. At this point, ROKS would have become a worldwide medium of exchange and would have established its own inflation measure. ROKS would then have become its own "fiat" currency in the sense that we understand it today. This fiat currency can continue to keep the trust of its billions of users if it keeps its value (stability). We the issuer would manage ROKS the same way the Fed is managing USD now, but with no other motivation than to keep it stable. Keeping ROKS stable increases the number of people who trust it, thereby increasing its market share.

Nevertheless, the incremental jump in Pm cannot be more than 0.1% especially in the beginning, increasing by 0.1% again only after Pr catches up, until the target Pm is reached. A good arbitrageur would then buy so much ROKS at the price just before the rise, especially if this arbitrageur knows how much the USD would inflate and how fast. Many traders would also chase the rising Pm. The arbitrageurs would then sell at a time when they think the inflation would have peaked, and this action would slow down the accumulation of USDC backing.

Pm and Pr Sampling Rate

The sampling rate is dynamic in that the trigger for every sampling is either a minting or a redemption (ROKS sell or buy event in OpenBook V2). We can use Solana’s SPL program which allows us to trigger the inflation-resistant program on a minting or redemption event, or to capture events more specific to minting and redeeming, just consume OpenBook V2 buy/sell events.

Pr can never quite reach Pm (Pr is asymptotic to Pm)



For Pr to approach Pm, the small area Qso * (Pmn - Pmo) must be very small compared to Pmo * Qso + Pmn * Qsx

Pr = (Pmo * Qso + Pmn * Qsx) / (Qso + Qsx) in which only Rx changes and where total USDC backing q = Pmo * Ra + Pmn * Rx and
Total circulating ROKS is Qs = Qso + Qsx.

As Qsx (ROKS in circulation) increases, the rectangle on the right increases its area (q - Pmo * Qso) because the right edge moves rightward, and, looking at the above equation, Pr approaches Pmn.

The Outcome Totally Depends on How USD is Managed

If the Fed does not lose control of USD inflation, then all is well and good, and ROKS would remain just like any other stablecoin. If the Fed loses control or in people's judgment would lose control, then other stablecoin issuers would come out of the woodwork adopting the same algorithm as this ROKS algorithm.

If the Fed loses control, the backing of ROKS and other similar stablecoins would not be so useful, but by then this new crop of stablecoins would have established their own network effects. Each such stablecoin would then become private fiat money, able to earn seigniorage profits, competing for market share in which the most stable coin wins. Only a few private stablecoins would win in the end. Given the size of the market, it is most unlikely that only a single stablecoin would remain; using game theory, we should be able to prove that this is not a winner-take-all kind of business.

What Would It be Like for Users?

The experience of the end-user shouldn't be bad either. We know how facebook dominates: it’s because their currency is user data, which cannot be shared with other social media (not even with the users themselves). In the money world, exclusivity of currency is not going to be an advantage. Money needs to go from one user to another user (even a user holding a different stablecoin). If you hold stablecoin x and the grocery you want to buy goods from only accepts stablecoin y, obviously there is a problem. But even in previous chapters of the history of money in which private banks issued notes (currency), these private banks made sure that they accept other banks' notes for redemption. Any bank that rejected any

other banks' note became isolated until all its users got rid of this bank's notes. In the money competition, the last thing you want is to be isolated. To increase market share, you have to accept all other banks' notes. The same thing will happen among competing stablecoin issuers. When you go to that grocery with your x coins, the grocery would have no problem accepting your x because it will simply be converted to y, and you wouldn't even have to be aware of it.

Decentralization

About the important topic of decentralization: having competing private currencies is a form of decentralization; more importantly, each competitor can only compete well according to each competitor's further decentralization of money processes. In other words, competition will push competitors towards monetary arrangements with the best Nakamoto index of decentralization (see Balaji's article on the subject).

ROKS backed by both USDC and USDT

It would seem difficult to prevent runs of one backing when there's more than one backing. The system would have no way of determining how a set of ROKS that were minted for USDC, say, is now being used to redeem USDC or USDT, without losing fungibility. Let's say an economic actor bought a million ROKS using USDC; and then, for arbitrage reasons, now suddenly want to redeem such million ROKS for USDT. The effect of this action is to reduce USDT backing without correspondingly reducing the ROKS in circulation (that were minted using USDT), thereby exposing the system to runs with respect to USDT. In this situation, the Pr calculation for USDT would be inaccurate. How can we obtain a more accurate Pr?

The math gets more complicated in the case of multi-stablecoin backing, but essentially the idea is to modify the calculation of Pr such that it is not totally dependent on ROKS in circulation due to USDT and the quantity of USDT backing alone, but rather also on USDT market price relative to USDC price. At any rate, Pr is a lower limit and the market price of ROKS should stay between Pr and Pm. The auto-regulator is provided with oracle input regarding relative market exchange rates between USDC and USDT and can therefore adjust Pr accordingly. Pm can continue to depend on oracle measure of inflation, while Pr can be a function of relative prices and backing quantity.

As USD inflates, there will be a price difference between USDC and USDT, which would require "portfolio rebalancing". The rebalancing should happen without doing anything on our part. Arbitrageurs will take advantage of the imbalance. It's like dealing with the situation of two exchanges not having the same price for a commodity that is sold in both exchanges. Arbitrageurs would immediately sense an opportunity and take advantage of the imbalance.

With USDC and USDT, the arbitrageurs won't have to deal with two exchanges: they can sense the imbalance in the same DEX OpenBook V2 market for ROKS. Arbitrageur activity would rebalance the two backing stablecoins. Let's take the example of that arbitrageur buying a million ROKS with her USDC and then redeeming ROKS for USDT. The reason she would do this is most probably because USDT price is going up with respect to USD, while USDC is not. If this price difference is not yet reflected in Pr and Pm for both stablecoins, then the arbitrageur would be making a profit by her action. From the standpoint of ROKS, the action reduces USDT backing and that's fine, because USDT value is now higher than USDC. The risk for a run either on the USDC side or USDT side does not increase by arbitrage.

--end--