Serenus Coin: Volatility and Stability in Cryptocurrency

Sivakumar Arumugam

Version 0.7; this document may be updated

3rd April, 2019

Cryptocurrencies that can achieve stability in value relative to real goods and services have several desirable properties. In particular they can be used as stores of value and as a medium of exchange while remaining decentralised, immutable and uncensorable. However, as relatively unproven and fast improving pieces of technology, cryptocurrency experiments in "sound money" that are programmable like bitcoin and ethereum are likely to remain fairly volatile when priced in US dollars for sometime. One solution is the creation of cryptocurrency stablecoins that peg their value to the US dollar or other state credit money.

Approximately 360 million dollars have been raised by teams building different varieties of stablecoin tokens. The current market cap of all such coins is roughly $2 billion dollars. There may be a way to take advantage of the contrast between the desired stability in the value of stablecoins and the volatility of bitcoin, ethereum and other "native" cryptocurrencies. Serenus Coin (SRS) is stable precisely because it seeks counterparties — "issuers" — that are willing to trade stability for volatility. This compares well to currently existing types of stablecoin and how they deal with volatility. The last section of this paper introduces Serenus Coin in its current implementation on the Ethereum mainnet blockchain. Serenus combines the best features of Tether, MakerDao's Dai and the Uniswap on-chain exchange system.

Qualities and features of a stablecoin

All stablecoins currently in existence choose trade-offs along these three axes.

1. Stability
2. Scalability
3. Decentralization

And there are three types of stablecoin design, broadly speaking.

- Dollar collateral
- Algorithmic supply management
- Crypto collateral

By market share, the largest by far is a stablecoin that is issued one-for-one with US dollars held in a bank account: Tether is the second most actively traded cryptocurrency. About 2.6 billion tokens have been issued in the past but some recent worries about its transparency and competition from other similar stablecoins have shrunk down their issuance to below 2 billion. Tether nevertheless represents about 75 percent of all stablecoins by market value. The recent similar additions using this type of design include Circle, TrueDollar, Paxos and GeminiDollar. In all cases, a token can be issued for each US dollar held in a dollar bank account.

Those tokens can then be traded on cryptoexchanges for other cryptocurrencies. This type of stablecoin emphasises stability at the cost of losing some of both scalability and decentralisation. Scaling is difficult because it relies on access to US dollars. The operation is of course entirely centralised. In the case of Tether, there have been serious questions about whether Tether the company does in fact hold as many US dollars as tokens they have issued. There is also significant regulatory risk and costs with respect to holding dollars in a bank for cryptocurrency related activity. Some of the recent entrants to this field have tried to emphasise the role of an external auditor vetting their own claims about a strict one-for-one mapping and highlight fully regulated relationships with local governments. These new stablecoins have built in features to censor transactions and freeze accounts.

A second type of stablecoin avoids collateral holding but tries to achieve stability through a mechanism that manages supply of the token. Securities are issued, as a second type of token, in exchange for the stable tokens if the stable token value has fallen below one-for-one with the US dollar. These securities are promises to pay tokens in the future if the token regains its value with respect to the dollar. In that case additional tokens can simply be issued to the securities holders as repayment at a positive yield. Basis and Carbon are the best known examples. This approach is relatively new, but one version — NuBit — has already failed. It broke its one-for-one value with the dollar at the beginning of 2018. More recently, Basis have returned all their remaining funds to their investors before the launch of their product. They have been unable to gain regulatory approval to algorithmically issue securities for sale to unaccredited investors. Aside from difficulties with securities regulation, this design is not well trusted in principle. It is not clear why investors should ever believe that a token worth less than a dollar should gain in value. Without that belief it would not be possible to restrict token supply. The telling contrast is with state credit systems like the US dollar. Here investors may willingly purchase US Treasuries, thereby reducing current money supply, because they know that there will be future demand for the US dollar. At the very least the US government will continue to pay for goods and services, and demand payment in taxes, in their own money.

The third type of stablecoin avoids fiat monies altogether. Instead it achieves stability by issuing tokens that are over-collateralised with other cryptocurrencies. MakerDAO's Dai token is the best known example of this, although BitShares' BitUSD uses a similar system and has been in existence for much longer. This kind of coin involves monitoring the value of the collateral and builds in mechanisms to deal with falls in value. If the price falls sufficiently, the token it backs is claimed in return for a discount on the collateral. As the stablecoin has to be over-collateralised this approach is capital inefficient, making scalability difficult. It is however decentralised and transparent. Anyone can see if the tokens have the correct collateral and act accordingly. MakerDAO's Dai has retained stability with respect to the US dollar throughout 2018 – a period in which the US dollar price of its current collateral has fallen by more than 90%. Observations of the issuance

of Dai make it clear that issuance is strongly correlated to the price of ethereum. When ethereum increases in value more Dai is issued and when ethereum falls, supply of Dai reduces sharply. This is unfortunate. The supply of a stablecoin should rise and fall in response to varying demand for the stablecoin itself, not the underlying collateral. There is no incentive to tune Dai issuance in response to demands for holding and using Dai as a store of value or as a means of exchange. Indeed, an issuance of Dai is in effect a borrowing of monies against locked-up collateral. A positive interest rate is charged for that borrowing by the MakerDAO system.

Serenus Coin and volatility management

The three types of stablecoins treat the central problem they are trying to solve — volatility — in different ways.

1. Submerge crytocurrency volatility in the relative stability of the US dollar
2. Trade volatility in the present for volatility in the future
3. Underleverage cryptocurrency volatility to make it more stable

Serenus Coin takes a new, fourth, approach. One that is more transparent about where the volatility goes when creating a stablecoin.

4. Transfer volatility to a willing holder of the collateral

Each new serenus token that is issued by the Serenus Coin system implies a long position on the part of issuers who have deposited ethereum with an issuer contract. The issuers are paid a commission on each trade as an incentive to respond to changes in the demand for holding serenus. In addition the price of the trade is adjusted to reflect the liquidity constraints faced in hedging the amount of ethereum sent into the system by users on each trade. An example process looks like this:

1. Issuers store ethereum on their own Serenus issuer contract
2. A user sends one ether to the contract
3. The oracle reports a current ETH/USD rate of 200 dollars
4. The Serenus ERC-20 contract mints 200 serenus tokens
5. The issuer bears that risk and may hedge accordingly elsewhere
6. The token can be held or traded for services by the user

7. The market price of ETH/USD may go down to 100 dollars
8. The issuer will be penalised if insufficient ethereum is available in the contract
9. The tokens could be returned to the smart contract
10. The contract will return 2 ether (i.e. 200 dollars of value)

But how can the contract return 2 ether? In the background, anyone creating a contract as an issuer in a permissionless way will be responsible for maintaining sufficient collateral in the contract. They are free to do this manually, however the Serenus Coin system is designed to encourage market-makers to act as issuers and hedge their risks accordingly. The easiest way to do this is to hedge the tokens issued by the contract on derivatives exchange markets. The digital value stored in the hedge will match the liability the issuer has on the contract no matter which way the ETH/USD price moves. Any profits and losses can be programmatically transferred between the external exchange and the smart contract. An example implementation of this process will published on GitHub shortly.

Alternatively, an issuer may simply elect to take on the price risk of holding ethereum and monitor their collateral levels to make sure they do not lose control of their contract. It would appear that MakerDAO CDPs are often created for the sole purpose of leveraging long ethereum holdings and there are active derivatives markets that also offer leveraged long and short access to ethereum. This suggests that increasing demands for serenus can be easily met by a ready supply of issuer capital looking to be exposed to increased ETH/USD risk.

Issuers are strongly incentivised to maintain sufficient collateral in their contract. If the amount of collateral falls below a cut-off level in an issuer contract, another issuer (including new participants) will takeover ownership of that contract. They will add more ether to an issuer contract because they will receive an additional boost in capital that is drawn from the old issuer. Specifically, if an issuer's contract falls below 120% collateral, anyone can takeover that contract and gain all the ether stored in that contract. Against those assets they will also have the total serenus issued by the contract as a liability. Their net gain will be the difference between assets and liabilities. The percentage gain will likely be quite large for anyone acting quickly enough.

Unlike fiat-coin systems like Tether and the MakerDAO system, any token holder can send in their serenus in return for ethereum at any time. There are no charges for converting serenus back into ether. This may aid with the adoption of serenus as a store of value and medium of exchange. Users may also convert ether into serenus and are currently charged 20 bips per transaction — 0.20% of the value of the ether sent to the contract — by the issuer contract. The Serenus ERC-20 contract charges an additional 10 bips fee on minting new Serenus coins that will go towards product development. The price that the users trade at is currently drawn from an average of the Uniswap ETH/DAI pool contract and Kyber

Network's ETH/TUSD and ETH/USDC reserves. Serenus is in effect pegged to an average of the values of DAI, TUSD and USDC.

The price is then adjusted proportionally to the size of the user trade to reflect liquidity costs on external exchanges. The result is a much tighter spread than is currently available on all decentralised exchanges trading in ETH/USD. However, Serenus is not designed for active trading in and out of ether as all trades occur on the mainnet. Only market orders are accepted and the time and price for trade settlement will depend on congestion and gas prices on the Ethereum mainnet. The web interface to Serenus Coin system pools together all issuer contracts and automatically selects from them randomly. It has no special privileges and can be replicated freely on other platforms or websites.

Contract design for Serenus Coin

Serenus Coin is made up of six smart contracts on the Ethereum mainnet. The source code in Vyper is available on Github.

Serenus token

The core of the Serenus system is an ERC-20 compatible token contract. The contract can access the Issuer and Governor contracts to make sure that any Issuer contract trying to mint or burn serenus has updated system-wide variable values. Only Issuer contracts created by the Factory contract have the right to mint or burn tokens.

Oracle

The Oracle contract gets prices for ether from the Uniswap ETH/DAI pool and Kyber Network's ETH/TUSD and ETH/USDC reserves. It will be updated to include PAX and GUSD when on-chain liquidity for these currencies improve. These stable coins are all pegged to the US dollar in various ways. Serenus in turn will be pegged to an average of their values.

There are some interesting trade-offs in oracle design. The Serenus system gains from having wholly on-chain access to market prices from these sources but loses from not having direct access to ETH/USD prices on centralised exchanges like Coinbase. The latter would need a Schelling point style design to be truly decentralised and trustless. No project has such a system currently in place.

The Oracle sets prices for individual trades and also helps determine if an issuer contract is under-collateralised. One potential attack point for the latter involves using a contract to manipulate Uniswap and Kyber prices and thereby force an issuer into under-collateralisation. The attacker contract could push very large trades through Uniswap and Kyber, trigger a takeover of an issuer, and then push the prices back before being picked off by arbitrageurs. This works because these

streams of actions all happen atomically. There would be no moment in which an arbitrageur could take advantage of the 'fake' prices.

The Serenus system provides the following counter-measure: to takeover an issuer contract, you have to call a function on the issuer that marks the issuer ready for takeover. You then have to wait at least one whole block before taking over the issuer. On both occasions, the oracle has to report a price that means that the issuer in under-collateralised. In the meantime, in that one block space, anyone can unmark the issuer for takeover if prices are actually much higher and the collateral correctly available.

Governor

The Governor contract controls system-wide variables. Specifically, it sets issuer fees on all minting operations, the minimum collateral ratio for all issuer contracts, a liquidity multiplier that controls the amount of slippage in ETH/USD prices with each mint or burn, and addresses for the ERC-20 token and the Oracle contract.

Factory

Anyone may access the Factory contract to create an Issuer contract with sufficient privileges to mint or burn serenus. Only such contracts have those rights.

Issuer

This is the key contract for controlling ether collateral in the Serenus system. No permissions are required for creating issuer contracts. However, each one has to be collateralised sufficiently to enable the minting or burning of serenus on demand from users of the system. Issuer contracts draw system-wide variables from the Governor contract and set their own desired leverage ratio, as long as it is more conservative than the minimum set by the Governor. Anyone may send ether in to any issuer contract. If it is able, it will return serenus. Anyone holding serenus may send their serenus in to any issuer contract. The contract will return ether.

If an issuer contract is under-collateralised, the first ethereum address to send enough extra collateral into that contract wins control of the contract and 80% of the remaining ether in that contract. For example, suppose an issuer contract hold 20 ether. Perhaps the minimum collateral level and current price of ETH/USD is such that the contract should hold a minimum of 19 ether. Then ETH/USD falls 10 percent. The contract should now hold about 21 ether but does not. Anyone sending in at least 1 ether will gain ownership of the contract. The original owner will have lost their 19 ether. 75% goes to the new contract owner and 25% is sent to the insurance contract. In this way, the first person to act in an under-collateralised situation has the most to gain. The new owner may now pay back all the serenus issued by this contract and close at, very likely, a large profit.

Insurance

In case ETH/USD falls quickly enough that an issuer contract ends up with less than 100% collateral, there is no longer any incentive for a takeover of ownership of that contract. A less than 100% collateral level implies that the net worth of the contract is less than zero because the dollar value of the ether in it is less than the dollar value of the tokens it has issued. In this case, anyone can call the insurance contract. If the insurance contract has sufficient ether in it, it will top up the collateral level in that issuer contract to a 110% level. Now, it is again attractive to send sufficient ether to take that issuer contract back up to at least 120%. Ownership will be passed along to the new owner. The insurance contract will over time hold enough ether to backstop any sudden "fat tail" sustained drops in the value of ETH/USD. The parameters that control how ether is fed into the insurance contract is controlled by the governor contract.

Summary

The roadmap for product development is currently focused on the development of a trustless user interface to the Serenus Coin system through an implementation of burner wallets and gas-less meta-transactions. Working on easier user access to Serenus is a high priority. An active area of research is also creating an appropriate DAO structure to control the Governor contract.

The new approach Serenus takes is a very attractive alternative to the three types of stablecoins outlined above. In particular, it scores high on all three axes of stability, decentralisation and scalability. The Serenus Coin system does this by carefully separating out the incentives for taking on ETH/USD dollar exposure from the need to create and use a dollar-stable cryptocurrency. It is an immediately accessible and cost-effective way for any holder of ether to purchase and make use of a trustless dollar-pegged stablecoin.