On Stablecoins: Stability Mechanisms and Use Cases for Real People

Nathaniel Fowler
Cal Poly, San Luis Obispo

Eric Cuellar
Cal Poly, San Luis Obispo

Zachary Peterson
Cal Poly, San Luis Obispo

Research Short Paper

ABSTRACT

Stablecoins are a promising area of blockchain development. While there is utility in price-stability alone, the combination of stablecoins paired with Decentralized Finance (DeFi) smart contracts has the potential to do what blockchain has always promised: bank the unbanked. In this paper, we discuss two distinct categories of stablecoins: *asset-backed* and *seigniorage share-based*. Asset-backed stablecoins are backed by on-chain assets (e.g. cryptocurrency) or off-chain assets (e.g. fiat currency such as the US Dollar). Whereas Seigniorage share-based stablecoins are defined by one characteristic as a whole–the absence of collateral. While many papers have covered the benefits of stablecoins in providing stability to the cryptocurrency markets themselves, we aim to provide a comprehensive review of stablecoin architecture while using real world examples to illustrate how stablecoins can provide utility in the average person's day-to-day life. In this paper, we make the following contributions: (1) a comprehensive review of existing stablecoin mechanisms, (2) highlight current and future use cases, and (3) show that banking on the blockchain with stablecoins in their current state is more advantageous than traditional systems, both in developed and developing countries alike.

1. INTRODUCTION

Stability mechanisms are the core value of stablecoins, and several methods have surfaced. The first category of stablecoins discussed is asset-backed, which rely on a collateralized issuance of coins to maintain stability. This can be further broken down into two categories: off-chain and on-chain, which are pegged to, and backed by, fiat and cryptocurrency, respectively. The second category is seigniorage shares, which algorithmically fluctuates coin supply relative to its price deviation from the peg. This model is the most decentralized. The final category covered is a hybrid seigniorage shares–asset-backed model designed for mobile-phone users.

Third International Symposium on Foundations and Applications of Blockchain (FAB '20) May 1, 2020, Santa Cruz, California, USA.

1.1 Asset-Backed Stablecoins

The most popular stability mechanism, asset-backed, has found footing both off-chain and on-chain. Off-chain asset-backed stablecoins, such as Tether and Facebook's project Libra, are backed by private companies with US dollars (USD) held in banks or custody accounts. In the eyes of blockchain purists, this results in one fatal flaw: putting trust in a central entity to maintain adequate reserves of the collateral. For example, Tether has a market cap of over 4 billion USD; however, their most recent third-party audit performed in June 2018 revealed a reserve of merely 2.6 billion USD split between two bank accounts [1]. This 1.4 billion USD discrepancy in addition to centralization of governance undermines the intention of blockchain. Nonetheless, off-chain asset-backed stablecoins have the distinct advantage of being able to go from concept to market quickly. Other examples include the Libra project, which was initiated by Facebook and still in development, as well as US Dollar Coin (USDC), which actually has overcollateralized reserves [16].

On-chain asset-backed stablecoins aim to solve the issue of trust in another entity via collateralization with on-chain assets. On-chain here means on a blockchain, so on-chain asset-backed stablecoins are collateralized by other cryptocurrencies such as Ethereum. The most widely used stablecoin in this category is DAI, or multi-collateral DAI, which is a stablecoin created by MakerDAO (a decentralized autonomous organization). Additionally, their stablecoin SAI, or single-collateral DAI, is collateralized only by Ethereum, and was the first stablecoin released by MakerDAO. It is important to note the distinction between DAI and SAI after the most recent upgrade in November 2019. SAI are generated via locking ETH into a smart contract called a CDP (Collateralized Debt Position, which will issue new SAI). In order to maintain price stability against a volatile cryptocurrency, the CDP charges a stability fee of 9%, and are thus required to be "overcollateralized" by a value of 150%–that is to say, if a user wants to create 100 USD worth of DAI, they will need to lock 150 USD worth of ETH into the CDP. DAI, on the other hand, is an upgrade to SAI: instead of only being collateralized by ETH, a CDP can be collateralized by a variety of underlying assets. At present, users can use ETH or Basic Attention Token (BAT) to generate DAI; however, several other coins have been proposed, and can be implemented if MKR token holders vote to make it a reality.

1.2 Seigniorage Shares Stablecoins

Both on-chain and off-chain asset-backed stablecoins share the common weakness of being dependent on a fiat currency, cryptocurrency, or good to maintain price stability. Seigniorage (non-stable) shares rely on an on-chain mechanism that algorithmically governs the expansion and contraction of the stablecoin's supply to maintain stability. Without diving too deep into the technical aspects, the seingorage approach can be summarized by a common rule using coins and seigniorage shares (S.S.): for X percent change in the coin's price, adjust the supply by X percent at the end of an established time interval using S.S. [11]. This is carried out by an algorithm which mints new coins to buy S.S. from arbitrators when the price falls below its peg, and selling S.S. for coins which are burned when the price is above its peg. These two scenarios increase and decrease the coin supply, respectively. Since buying and selling S.S. is completely voluntary, this model relies on the existence of active bidders who believe the price will return to its peg [12]. With that being said, if the network loses confidence or migrates to a newer, more advanced project, the stability will likely be negatively impacted.

One of the more popular S.S. stablecoins is Terra. Terra launched in 2019 and comprises a family of stablecoins such as TerraUSD, TerraKRW, and more. When the price of any of the coins falls below the relative peg, supply is contracted by auctioning Luna, the S.S. in Terra. Luna serves as the reward for validators participating in their proof-of-stake network. These validators actively absorb stability in the short-term, as their reward is diluted when the reserve needs to contract coin supply. Since the reserves are algorithmically maintained, they must query prices via decentralized oracles, which essentially connects a blockchain to off-chain data (*e.g.* an API). Through decentralized governance, dApp creators can apply for S.S. funding through Terra Treasury, in which one-third of the network must vote yes or no to fund or blacklist the dApp respectively [7].

2. A POTENTIAL HYBRID, FULL-STACK STABLECOIN

One of the most compelling stablecoins in active development is Celo, an open DeFi platform built for mobile phones. Celo uses a hybrid seigniorage shares and multi-asset-backed stabilization mechanism which algorithmically pegs the Celo Dollar (cUSD) to the USD. Celo Gold, or cGLD, is the native reserve currency which backs the ecosystem, and is used to control cUSD supply and buy crypto-assets to increase reserve. To expand cUSD supply, the S.S. mechanism mints new cUSD and sells it for cGLD. To contract cUSD supply, the protocol liquidates cGLD for cUSD, which is then burned. Both these scenarios would be done to lower and raise the price of cUSD to stability, respectively. The auctions are carried out via a decentralized exchange, similar to Uniswap, and will support other currencies. To passively bolster the reserve, each transaction of cGLD has a constant transfer fee ($T = 0.5\%$) and block rewards have a non-constant tax of 25%. The latter percentage fluctuates proportionally to the reserve ratio [13].

Celo's protocol includes a Proof of Stake consensus mechanism forked from Ethereum that allows users to earn cGLD by participating as a validator in the network. Users have to stake their cGLD in order to participate in the validator lottery, with a greater number of coins and a longer amount of time stored increasing your odds of being elected. Celo's mobile-first, full-stack approach enables users to transact Celo coins similar to sending SMS by addressing transactions to phone numbers. This is achieved by their lightweight identity protocol, which maps hashed phone numbers to public keys stored on-chain, similar to the Ethereum Name Service. Light clients (mobile users) are able to achieve a a claimed 9000% faster block download times by using epoch-based syncing, BLS signature aggregation, and zero knowledge proofs, which enables them sync to the network without downloading the entire ledger [14].

Celo's ecosystem will not only support cUSD, but a full ecosystem of stablecoins (e.g. Celo Euro, Celo Peso, etc). New assets will be introduced and voted on via Proof-of-Bonded-Stake, where in theory stakers will only vote in favor for coins that they truly believe will help maintain the stability of existing assets within the ecosystem. Furthermore, the project highlights the ability to create a local reserve currency that negates the need to use the cGLD reserve. In this way, "This would support the creation of local and functional currencies backed by collateral specifically tailored to each environment. For example, one such possibility is that some of the local reserve currency could get distributed to local inhabitants, which would allow them to benefit from the adoption of the local stablecoin, acting like a social dividend in the process" [14]. Additionally, the ability to not only build EVM compatible dApps on Celo, but to build native mobile dApps, will empower developers to reach a wider audience in both developed and developing countries. At the time of writing Celo is currently running the second phase of their testnet, and awaits testing with real transferable value.

3. USE CASE: STABLE REAL RATE OF RETURN

We now explore some real world use-cases that can benefit the layman. But first, we must paint the backdrop of what the average American faces when it comes to banking. We get the average FDIC-insured interest rate of 0.09% APR for savings and 0.06% for our checking account. Perhaps some of us took a financial literacy course, where we were told to put their funds into a money market account, earning an average of 0.28% APR today. The most we could earn from our bank would be 0.95% APR on average for a 60-month CD [2]. Given the most recent official numbers on inflation from the St. Louis Fed of roughly 2.25%, the best we can do is earn a real interest rate of -1.3% in the case of the 60-month CD, and a real interest rate of -2.16% in the case of the savings account [2]; *i.e.* the average American is guaranteed to lose between 1.3 to 2.16% of their savings every year. This is a problem for the average American who lives paycheck to paycheck.

Let us move this average American's life over to the blockchain; they will use one cryptocurrency exchange located here in the United States, DAI and DeFi smart contracts to replace their current bank savings account. The person transfers their savings into DAI via interfacing with the cryptocurrency exchange. They lock their DAI into the Oasis smart contract (a MakerDAO product), where they receive the DSR (DAI Savings Rate, set by the community of MKR token holders); as of writing, they now earn 8.75% APR for their savings–almost 100× what they earned for

their savings at a bank, and 9.21× what they would have earned for a 60-month CD. They now earn a real interest rate of 6.5%. They are also free to withdraw their DAI at any time, without a penalty–something that cannot be said for the 60-month CD. The issue of a guaranteed negative return presents a problem that can be solved by stablecoins and DeFi smart contracts. The implications are even greater for people living in developing countries.

Stablecoins paired with DeFi and an FDIC insured bank account carry distinct risk and reward characteristics. On one hand, customer deposits at an FDIC insured bank are insured up to a value of 250,000 USD, ensuring that if there is some type of "black swan" event, customers will still have access to their funds. On the other hand, the FDIC has created a moral hazard problem [15]. Customers are less likely to pay attention to a bank's business practices; therefore, banks are more willing to make riskier investments because they know that their customers' deposits are insured. The risks associated with DeFi returns are in some ways more complex, but also more straightforward in identifying. There is no FDIC and no insurance for DeFi; users are responsible for custody of their funds. Smart contract risk is present–the risk that a fatal flaw exists in the code governing a smart contract that can lead to loss of funds (though users can audit smart contract code to identify potential flaws before depositing funds). Interest rate risk also exists–rates on DeFi platforms are dynamic on a day-to-day basis and are set by community consensus, not by a central authority, which can lead to difficulty in accurately forecasting long term returns. Further, a more complex and recently identified risk is price oracle risk–a discrepancy between the current fair market price of an asset and the price reported by a decentralized oracle, which can have implications in maintaining the collateralization ratio of a CDP. The removal of a central authority who insures deposits presents unique risks for DeFi. However, we argue that DeFi users are adequately compensated for these risks with a commensurate positive real rate of return.

4. USE CASE: STABLE REAL RATE OF RETURN (DEVELOPING COUNTRIES)

We have discussed a tangible use case for DAI and DeFi contracts: the average American. The fact remains that they have access to more financial services than most of the rest of the world. However, according to the World Bank, there are still 1.7 billion people who are unbanked in the world. Kenya in particular has a high population of unbanked people who use a "mobile money" service called M-Pesa on their mobile phones. It is important to highlight how mobile money platforms benefit users as well as harm them. M-Pesa has built significant infrastructure in the area which enables Kenyans without an account at a financial institution to make transactions. However, they are inherently not a bank by definition; they do not take customer deposits and lend them out, in turn giving a return to the depositor. This does not bank the unbanked, and is why DeFi and stablecoins must be used in order to achieve that goal. Rather, M-Pesa has given Kenyans a convenient payment rail in their local currency, which collects high fees [4]. According to the Safaricom website (the owner of M-Pesa), fees for M-Pesa ATM withdrawals can range between 0.985-14.0%, and they do not pay interest on balances held on their platform [10]. Those fees are prohibitively high just to get access to your money, and the alternative is to just hold cash (while also earning 0% APR) and to suffer a guaranteed loss in purchasing power.

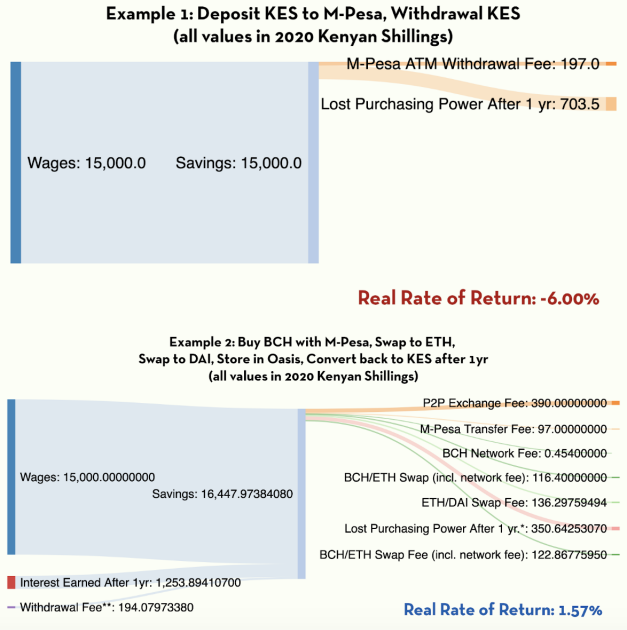

Figure 1: A Kenyan stores 15,000 KES, which is approximately 2% of the average annual income [8], then withdraws all balances to KES. Real rate of return is shown, and adjusted for inflation (Note: DAI is pegged to the US Dollar, therefore the US Dollar inflation rate of 2.25% is used.) The Withdrawal Fee is replaced by a positive P2P exchange fee, less the M-Pesa ATM withdrawal fee of 197 KES for a cash withdrawal of this size [3] [17].

We will illustrate how existing M-Pesa users in Kenya can benefit from using DAI and DeFi smart contracts for their savings to generate a positive real rate of return. This unbanked population will, admittedly, experience some friction even if they want to use DAI and DeFi as their bank account. Namely, they won't be able to deposit their savings from their current bank account (because they don't have one) to a cryptocurrency exchange, where they can purchase DAI. There are still options for them. The simplest way for people to purchase cryptocurrency without a bank account is on a peer-to-peer exchange like `local.bitcoin.com` or `localBitcoins.com`, where they will pay between 1-5% for a variety of payment methods including cash and M-Pesa. We used the average percentage fee for the top three listings on local.bitcoin.com using M-Pesa for calculations.

Finally, it is worth noting that stablecoins provide a frictionless bridge to the gig-economy to people who may not have a bank account, or even a government issued ID. Mechanical Turk services could be deployed through a smartphone app with an integrated stablecoin payment system. This not only provides a fiat-less onramp for stablecoins, but more importantly, it creates new avenues to economic prosperity for those who need it most.

5. FUTURE USE CASES

Over-collateralization of DAI makes the coin stable in conjunction with the stability, but consider if somebody wants to make a 100 dollar purchase when they only have 20 dollars? In traditional finance, this would just be called a personal loan–or perhaps a credit card. In DeFi, this is called undercollateralized lending, and it is in development at the time of writing. The Aave Protocol has made the first steps towards this form of undercollateralized lending with their Flash Loan feature [6]. Another area where Aave is making progress in the future of DeFi is allowing users to select a variable APR or a stable APR (the APR on Aave is set based on supply and demand of coins within the protocol, unlike the DSR which is set by community vote and tied to the stability fee). Micro-loans could also be used to spark economic growth in developing countries with low-capital risk on lenders. Stablecoins are finally providing a frictionless gateway to do so.

A childhood allowance is often one of the first ways that we are introduced to money as we grow up. Using Sablier, we can teach our kids the time value of money by "streaming" stablecoins to a specified address over a specified period of time. In the instance of the childhood allowance, perhaps a parent chooses to stream 5 dollars to their child for their allowance over the course of 5 business days. 1 dollar is sent by the end of the first day, 2 dollars by the end of the second, and so on and so forth until 5 dollars has been paid out after 5 days, or the parent decides to cut off the stream. The child now sees that: "If I wait one day, I can withdraw 1 dollar and buy something small, like a pack of gum. If I wait two days, I now have 2 dollars, and can buy something that is a little bit nicer, like a candy bar!" While the mechanics of what is actually occurring on Sablier are entirely disconnected from the core concept of the time value of money and interest rates, services such as Sablier can teach young people far more about how money works than a magical 5 dollar bill that appears out of thin air at the end of the week.

Using the Interledger Protocol, users could stream stablecoins and have them converted to any currency, which can be used for pay-per-use services such as listening to music or watching a film, where the content creator can be paid directly immediately [9]. This method could also apply to the use of data sets, creator content, and idle GPU, as well as electric vehicle charging, paying road usage fairs, ridesharing, and more. Streaming donations could be used as a means of behavior change, where money can be streamed to charities while one is on social media, or while their alarm is on snooze. As more devices become sensory enabled, more physical actions can be paired with steaming payments. For example, on-demand office rentals could use WiFi signals and device IDs to automatically bill tenants by the minute.

On Celo, savings circles could be built to allow families in developing countries to pool their funds and provide interest free, zero-collateral loans to each other. This example could be extended to small businesses with strong relations. Celo could be used to efficiently and transparently distribute donations to NGO's in developing countries, and from NGO's to businesses and citizens. Cheap and fast cross-boarder payments could be carried out on a mobile phone. The ubiquitous access to the currency means any business, physical or digital, could implement Celo as a new means of payment. Tangentially, stablecoins could be launched that are backed by natural capital (e.g. forests, carbon, etc) to incentivize the preservation of asset backing the coin. Backing a currency by a relatively fixed asset typically increases the asset's price by increasing demand, and could therefore be used to make people pay the true cost of Earth's integral natural capital [5].

Universal Basic Income (UBI) has resurfaced as a potential remedy for global economic disparities, but there lacks an efficient and transparent distribution mechanism for such a task. Proof of Stake stablecoins paired with digital wallets could be used to address the concerns around the distribution of funds. For example, if every community had a pool of validator nodes proportional to their population, then UBI funds could trickle in and be transparently funneled to citizens. Another method would be to implement demurrage–a negative interest rate. This could be applied to wallets that have balances that exceed a certain threshold.

6. CONCLUSION

We have shown that not only is banking on the blockchain with stablecoins relatively frictionless in its current state, but that it can offer distinct economic incentives for people in developed and developing countries. Off-chain asset-backed stablecoins suffer from issues of trust and accusations of fractional reserve banking, which is the exact type of behavior that cryptocurrencies were designed to remove in the first place. We believe that the initial first mover advantage that off-chain asset-backed stablecoins were able to benefit from will become less powerful over time, as people realize the true potential of next generation stablecoins that simply were not possible when creating the coins that exist today. The sheer amount of development activity and human capital being invested into future stablecoin designs such as Celo is indicative of this. Likewise; the creation of increasingly complex and useful smart contracts that can work with the limitations of on-chain asset-backed stablecoins like we have seen at the start of 2020 points towards a promising future. A future where all you need to access stable financial services that benefit the user (rather than toll collectors) is an internet connection and a dream. Given the current economic climate–where negative nominal interest rates have become a reality–stablecoins provide an attractive alternative.

While the future of stablecoins is bright, it is important to note their shortcomings in serving an existing non-blockchain economy. Currently available on-chain asset-backed stablecoins, such as DAI, are limited by the economic bandwidth of the underlying collateral that backs them. That is to say–*ceteris paribus*, in order for the money supply to expand, the USD value of ETH also needs to rise. That situation is a hindrance in the existing financial system, where central banks have made the money supply extremely elastic to fit the demands of the world economy through the issuance of debt. This desire for elasticity in the money supply was a motivating factor in the US abandoning the gold standard. We make no comment about the long-run feasibility of running a monetary system based on debt, instead focusing on the reality of moving an economy on to the blockchain, where stablecoins are the unit of exchange. Until development of seigniorage shares and other more elastic stablecoin protocols are furthered, stablecoins and DeFi will exist to merely benefit the end-users who are bold enough to take a chance.

References

[1] Aleksander Berentsen and Fabian Schär. Stablecoins: The quest for a low-volatility cryptocurrency. 2019.

[2] Federal Deposit Insurance Corporation. FDIC: Weekly National Rates and Rate Caps.

[3] CEIC Data. Kenya Average Wage Earnings.

[4] Leora; Singer Dorothe; Ansar Saniya; Hess Jake Richard Demirguc-Kunt, Asli; Klapper. The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. 2017.

[5] Charles Eisenstein. *Sacred Economics*. North Atlantic Books, 2011.

[6] E Frangella. Flash Loans, One Month In. 2020.

[7] Kwon D. D. Maggio M. D. Platias Kereiakes, E. D. Terra white paper. 2019.

[8] H Plecher. Kenya - Inflation Rate from 1984 to 2024.

[9] Interledger Project. STREAM: A Multiplexed Money and Data Transport for ILP. 2019.

[10] Safaricom. M-pesa rates. 2017.

[11] R. Sams. A Note on Cryptocurrency Stabilisation: Seigniorage Shares. 2015.

[12] Smith and Crown. The Cryptoeconomics of Seigniorage Shares Stablecoins: Basis and Carbon.

[13] C Labs Team. An analysis of the stability characteristics of celo. 2019.

[14] C Labs Team. Celo: A multi-asset cryptographic protocol for decentralized social payments. 2019.

[15] H.M. Thomas. 16th Annual IADI General Meeting and Annual Conference. 2017.

[16] Grant Thornton. December 2019 Independent Accountant's Report. 2020.

[17] Verivox. Negativzinsen.