Demystifying Stablecoins

Cryptography meets monetary policy

JEREMY CLARK[*], Concordia University
DIDEM DEMIRAG, Concordia University
SEYEDEHMAHSA MOOSAVI, Concordia University

Stablecoins promise the functionality of Bitcoin without the rollercoaster ride of it's exchange rate. But can this new breed of cryptocurrencies really outsmart decades of central bank policy with algorithms and smart contracts?

1 INTRODUCTION

The first wave of cryptocurrencies, starting in the 1980s, attempted to provide a digitization of government-issued currency (or 'fiat currency' as cryptocurrency enthusiasts say) [5]. The second wave, most prominently represented by Bitcoin [4], provide their own separate currency — issued and operated independently of any existing currencies, governments, or financial institutions. Bitcoin's currency (BTC) is issued in fixed quantities according to a hardcoded schedule in the protocol.

In the words of Bitcoin's pseudonymous inventor, "*there is nobody to act as a central bank. . . to adjust the money supply. . . that would have required a trusted party to determine the value because I don't know a way for software to know the real world value of things. If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that. In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes*" [1].

Without active management, the exchange rate of BTC with governmental currencies has been marked by extreme volatility (see Figure 1). Squint at the chart to notice how the GBP drops around June 2016: this mild-looking pinch is actually the 'sharp decline' and 'severe swing' that followed the Brexit referendum in the UK. However, it is completely overshadowed when placed beside BTC's large fluctuations.

A third wave? Extreme volatility is not specific to Bitcoin (BTC), and can also be seen in its contemporaries Ethereum (ETH) and Ripple (XRP). This instability is an issue of practical importance: volatility encourages users to hoard (if it is going up) or avoid (if it is going down) the currency rather than use it. It makes lending risky, as currency movements can exceed interest payments. A lack of lending and credit inhibits the formation of mature financial markets. In response, a flood of proposals have been made for new cryptocurrency designs (called 'stablecoins') that purport to provide a stable exchange rate similar to (or exactly mirroring) a government issued currency like the USD.

Stablecoins have garnered a lot of attention recently, both positive and negative. According to CoinMarketCap, more value in Tether changes hands across a given day than Bitcoin. This despite questions about Tether's reserves and regulatory investigations into its affiliates. The announcement of Facebook's Libra made international headlines and has been remarked on by the Fed, US legislators, and the even the sitting President. Another project, Basis (*née* Basecoin) raised $133M in Venture Capital but folded up when it could not find a tenable path through US financial regulations. Central banks, including those of Sweden and Denmark, have explored the idea of government-issued stable cryptocurrencies.

[*] Authors listed alphabetically. D. Demirag and S. Moosavi should be considered equal first authors.

Authors' addresses: Jeremy Clark, Concordia University; Didem Demirag, Concordia University; Seyedehmahsa Moosavi, Concordia University.

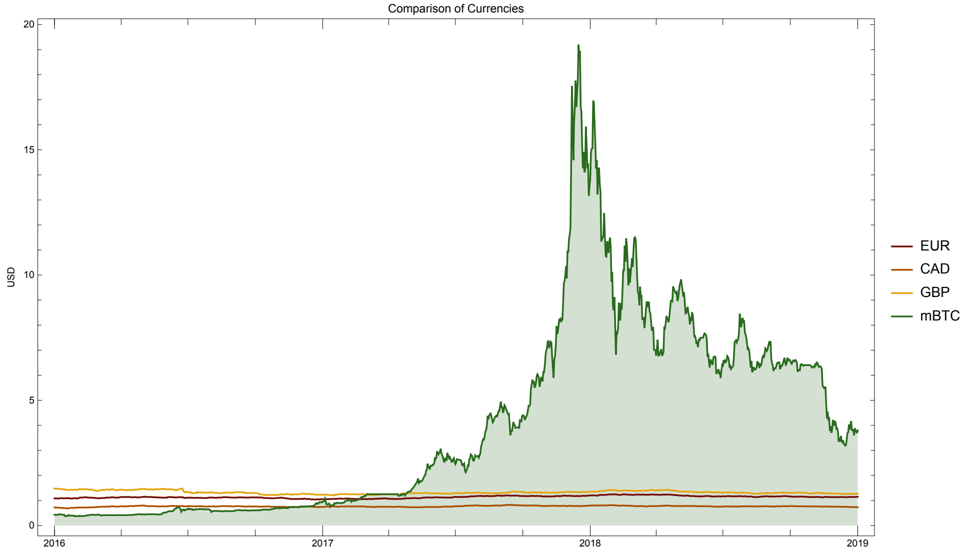

Fig. 1. Comparison among fiat currencies and Bitcoin: The values are retrieved daily between 01 Jan 2016 and 01 Jan 2019. Note that 1000 mBTC = 1 BTC.

Knowledge gap. Understanding how stablecoins work should be easy when they are marketed to the public. Most firms/projects have a whitepaper outlining the design, and there is no shortage of online articles surveying various designs. Unfortunately there are a number of pitfalls in systemizing this knowledge. Many whitepapers are obfuscated with jargon—terms left undefined and/or used inconsistently with other projects and with the financial literature. In other cases, system components appear mislabled. For example, a component that cleanly meets the definition of a security or a derivative might be instead labeled a bond or a loan. Maybe this is a lack of precision, or maybe it is a play to make an unconventional protocol appear more conventional? Or maybe they are unconscious attempts at keeping any regulatory red flags at half mast? In any case, we made a concentrated effort to offer direct and simple explanations (see Table 2). In parallel to our work, other academics have produced their own taxonomies [3, 7].

Sidebar: **Exchange Rates.** asf

Sidebar: **Bitcoin Primer.** Blockchain. coinbase transactions. DApps. Tokens. DApp holds ETH. [6]

Sidebar: **Ethereum Primer.** Blockchain. coinbase transactions. DApps. Tokens. DApp holds ETH.

2 HOW DO STABLECOINS WORK?

We started by finding stablecoin projects on *CoinDesk*, an online news source for cryptocurrencies, using search queries like "stablecoins," "stability," and "price-stable." We read 185 articles up to January 11, 2019.[1] For the 25 projects for which we could find sufficient documentation, we classified them in Table 1. This classification is done according to what the projects assert they do—we provide no warranty of what the projects do in reality. We sort projects according to their rank on *CoinMarketCap* which ranks cryptocurrencies that are actively traded on an exchange service. Unlisted projects are ranked $\perp$.

Next, we distilled each proposal into their core stability mechanism. Instead of enumerating the intricate details of how each 'brand' of stablecoin works—details that could change tomorrow—we concentrate on communicating the fundamentals. Broadly, the proposals can be split into two categories: (1) ones that try to directly match the stability of a second asset, such as the USD, and could not exist without this underlying asset, and (2) ones that propose independent currencies with algorithmic and/or human intervention mechanisms for providing stability. Fuller detail is provided in Table 2.

3 TYPE 1: BACKED STABLECOINS

3.1 Directly-Backed and Redeemable

For stablecoins in this category, the firm operating the currency will obtain a reserve of some valuable asset—it might be USD or another fiat currency; gold or another commodity; or a basket of multiple assets. It will then issue digital tokens that represent a unit of the underlying asset (to illustrate, assume a token is redeemable for 1 USD) which can be exchanged online.

This idea predates Bitcoin: Liberty Reserve provided a similar digital currency, with some caveats about its redeemability, not to mention its legality. However Liberty Reserve, e-gold, and similar pre-blockchain services would maintain transaction details and account balances on a private server. Blockchain enables decentralized trust for the transactions, while the coin creation and redemption processes rely on a trustworthy firm. In short, this type of stablecoin is more centralized than Bitcoin but less than Liberty Reserve. For analysis, we need a finer grained approach to trust assumptions which Table 3 tries to capture. Also consider that while decreasing centralization can be good for trust and transparency, additional measures are needed to ensure it is not harmful for privacy.

Price Stability. Recall the mechanism in Table 2. If buyers are willing to pay more than \$1 USD for 1 AliceCoin, new coins can be generated for \$1 USD and sold to these buyers for a profit, ensuring bids return to \$1 USD (it corrects overvaluation). If sellers are willing take less than \$1 USD for 1 AliceCoin, these coins can be bought and redeemed for a profit, ensuring offers return to \$1 USD (it corrects undervaluation). In reality, transactions are not free, efficient, or entirely frictionless and some price deviation is expected. If redemption is ever in doubt, then the price can fall freely from \$1 USD (although this will not necessary happen, see next section). The trustworthiness of the operating firm and the custodian of the reserves is essential, and financial audits are an important step to establishing confidence (although many pitfalls exist when auditing blockchain-based assets [8]).

[1] Given its high profile, we also include Facebook's Libra Coin which was released after this date.

Class	**Mechanism**	**Resembles**	Rank
Backed	Directly-Backed & Redeemable[†]	USDC	20
		TrueUSD	26
		Paxos	38
		Gemini Dollar	52
		StableUSD (USDS)	685
		Stronghold USD	891
		Petro	1210
		Libra Coin, Ekon, WBTC, emparta	⊥
	Directly-Backed	Tether	6
		EURSToken	95
		BitCNY	304
		Terracoin	1280
		Saga	1495
		GJY, Novatti AUD, UPUSD	⊥
	Indirectly-Backed	Dai	57
		BitUSD	398
		Nomin	⊥
Intervention	Money Supply Adjustments	Ampleforth	⊥
		RSCoin	⊥
	Asset Transfer	NuBits	892
		CarbonUSD	1262
		Basecoin	⊥

Table 1. Stablecoin proposals as of January 11, 2019. † *Disclaimer:* Projects are classified according to what they assert; *e.g.,* we provide no warranty that projects classified as 'redeemable' provide actual redemption of the assets that back their coins. Rank corresponds to *CoinMarketCap*.

3.2 Directly-Backed

What if a stablecoin operated exactly as in the previous section but did not offer a redemption process for the coin's underlying assets? If we could not find a clear assertion of redemption, we listed the project under this category in Table 1.

Price Stability. Recall the mechanism in Table 2. Bids will not exceed $1 for the same reason as the previous section. However there is no longer a way to profit if offers vary between $0 USD to $1 USD (*i.e.,* the mechanism does not prevent undervaluation). Generally coins in this category are in fact 'redeemable' by one user: the firm operating the coin. It could purchase undervalued coins to release $1 USD from its reserves. For this reason, stablecoins in this category are scrutinized (to the extent made possible by the firm) to ensure reserves are intact. If every AliceCoin was not backed by $1 USD, Alice could overissue AliceCoins to enrich herself.

The largest coin is this category is Tether. Tether claims to be redeemable, but the redemption process is reported by users to have a lot of friction, it is accused of issuing coins to manipulate markets [**?**], and it has not always maintained full reserves of USD to allow all Tether to be redeemed (for these reasons, we categorize it here). It is a mystery to most why Tether remains highly liquid with daily trading volumes exceeding all other cryptocurrencies in value (according to *CoinMarketCap* at the time of writing). One explanation is it is too useful to fail.

Stability Mechanisms
Directly Backed and Redeemable. Alice is a trusted third party and uses Ethereum to instantiate a decentralized application (DApp) which issues 1000 AliceCoins as standard tokens (*e.g.,* ERC20). She asks $1 USD for 1 AliceCoin and promises to redeem any AliceCoin for $1 USD. If Bob buys 10 AliceCoins for $10 USD, Alice deposits the $10 USD in a bank account. Any time Alice receives a buy order for AliceCoins and does not have any left to sell, she creates new ones to sell. If Carol wants to redeem 5 AliceCoins, Alice withdraws $5 USD and exchanges it with Carol, taking those AliceCoins out of circulation. Alice frequently publishes bank statements showing that her account holds enough USD to redeem all coins in circulation (the number of AliceCoins can be checked anytime on Ethereum).
Directly Backed. Again, Alice is a trusted third party that issues 1000 AliceCoins as ERC20 tokens. She asks $1 USD for 1 AliceCoin and promises to deposit and hold the payment in a bank account. As before, Alice creates new AliceCoins when she runs out and publishes frequent bank statements. Unlike above, she offers no direct redemption of AliceCoins for USD.
Indirectly Backed. Alice is no longer assumed to be trustworthy. She sets up a DApp that can hold ETH and issue tokens. The DApp determines how much ETH is equivalent to $1.50 USD using the current exchange rate, provided to the DApp by a trusted third party oracle, and Alice deposits this amount of ETH into the DApp. The DApp issues to Alice two places in a line — each place is a transferrable token. At some future time, the holder of the first place in line can redeem up to $1.00 USD worth of the deposited ETH at the future exchange rate, and the holder of the second place in line gets any remaining ETH. Alice will transfer the first place in line (as a stable coin called AliceCoin) to Bob for $1.00 USD, and will hold or sell the second place in line. When Bob redeems the AliceCoin, it will be worth $1 USD in ETH when the entire deposit of ETH is worth more than $1 USD. If the exchange rate drops enough, the deposit will be worth less than $1 USD — Bob will get all of the deposit and the holder of the second place in line will get nothing.
Money Supply Adjustments. Alice forks Bitcoin to create a new altcoin called AliceCoin. She tweaks the schedule for releasing new AliceCoins (called the coinbase amount in Bitcoin) according to the rules outlined below. She sets up a trusted oracle for the latest exchange rate of AliceCoins to USD. AliceCoin is programmed to apply an intervention when the price of an AliceCoin exceeds $1.02 USD or dips below $0.98 USD. If the price exceeds $1.02 USD, the miner is allowed to increase the coinbase amount (the amount is determined by some mathematical relationship with how much the price exceeds $1.02 USD). If the price dips under $0.98 USD, the miner must decrease the coinbase amount based on the same relationship. The correctness of the claimed coinbase is verified by other miners in deciding to accept or reject a mined block, as per all other checked conditions in Bitcoin.
Asset Transfer. Alice instantiates a DApp with an ERC20 token called AliceCoin. The DApp is programmed to apply an intervention when the price of an AliceCoin exceeds $1.02 USD or dips below $0.98 USD according to a trusted oracle. If the price exceeds $1.02 USD, the DApp creates new a set of AliceCoins (as above, according to some mathematical relationship) and transfers them to users waiting in line for them. How do users wait in line? When the price dips under $0.98 USD, the DApp creates new positions at the end of the line and auctions them off to the highest bidder. The payment for a place in line is made in AliceCoins from the bidder to the DApp and the DApp destroys the payment. The place in line is a transferrable token. If the line is empty, AliceCoins are distributed according to a fallback policy (see main text).

Table 2. Major types of stability mechanisms for stablecoins.

A key use-case, illustrated by Tether and the affiliated exchange Bitfinex, is as a temporary store of value for traders and speculators. A trader that wants to divest their BTC for USD has three options. She can (1) hold the USD in her exchange account, which can be used only on the same exchange and requires the exchange to be a trustworthy custodian. She can (2) withdrawal the USD from the exchange but this requires identity verification (in most jurisdictions), a bank that will accept proceeds of cryptocurrency trading, and a substantial time delay. A balanced alternative is to (3) exchange BTC into a stablecoin which can be withdrawn from the exchange (*i.e.,* moved from the exchange to Alice's private key) with little friction, delay, and regulatory oversight. The withdrawn stablecoin can be moved onto a different exchange, transferred other other users, or used for direct purchases without involving the original exchange. This enables more flexibility than withdrawing USD. In short, it offers more flexibility than USD left on an exchange account and less friction than withdrawing actual USD.

	Corrects undervaluation	Corrects overvaluation	Decentralizes issuance	Decentralizes redemption	Decentralizes transfer	No trusted oracle
Mechanism	Price		Trust			
Traditional Digital Cash	●	●				●
Traditional Cryptocurrency			●	×	●	●
Directly Backed and Redeemable	●	●			●	●
Directly Backed		●			●	●
Indirectly Backed	○	●	●	●	●	
Money Supply Adjustments	?	○	●	×	●	
Asset Transfer	?	○	●	×	●	

Table 3. Comparative evaluation of mechanisms to design stablecoins: ● indicates the properties (columns) are fulfilled by the corresponding mechanism (rows) within reason, ○ means the property is fulfilled but the fulfillment is bounded, ? indicates a heuristic has been proposed for stability and the conditions under which it will work are not well-established enough to evaluate, and × indicates the property is not applicable.

3.3 Indirectly-Backed

Price Stability. Recall mechanism in Table 2.

4 TYPE 2: INTERVENTION-BASED STABLECOINS

4.1 Money Supply Adjustments

Price Stability. Recall mechanism in Table 2.

4.2 Asset Transfer

Price Stability. Recall mechanism in Table 2.

Discussion. Consider an ideal stability mechanism: one could deposit a highly volatile coin and receive a low volatility coin. Such a mechanism might be impossible. Stablecoins of this category attempt a trick: they do turn high volatility coins into low volatility coins, however they also produce extreme volatility 'coins.' In other words, two types of coins are output and the volatility is pushed from the one type of coin onto the other. This is not unlike some financial assets which do not reduce overall risk, but simply push it from one tranche of the asset to another.

We also remark that we took some time to develop a clear presentation of this stability process. Projects describe our 'place in line' asset very differently: for example, as purchasing bonds (Basecoin), as parking assets (NuCoin), or with confusing terminology like seignorage shares.

5 DISCUSSION.

Why so many?

Regulation.

Ethereum's Gas.

Oracles Everywhere.

Centrally Banked Digital Currencies. Curse of cash

Stability.

6 CONCLUSION.

A more detailed version of this article is available as a whitepaper [2]. It includes detailed descriptions of each coin and a consideration of Ethereum Gas as a stablecoin.

ACKNOWLEDGMENTS

J. Clark acknowledges support for this research project from the Autorité des Marchés Financiers (AMF) and from the NSERC/RCGT/Catallaxy Industrial Research Chair in Blockchain Technologies. S. Moosavi acknowledges support from The Fonds de recherche du Québec - Nature et technologies (FRQNT).

REFERENCES

[1] Phil Champagne. 2014. *The book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto.* e53.

[2] Jeremy Clark, Didem Demirag, and Seyedehmahsa Moosavi. 2019. SoK: Demystifying Stablecoins. SSRN 3466371.

[3] Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. 2020. SoK: A Classification Framework for Stablecoin Designs. In *Financial Cryptography.*

[4] Satoshi Nakamoto et al. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).

[5] A Narayanan, J Bonneau, Edward W. Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies.* Princeton.

[6] A Narayanan and J Clark. 2017. Bitcoin's academic pedigree. *Commun. ACM* 60, 12 (2017).

[7] Ingolf G A Pernice, Sebastian Henningsen, Roman Proskalovich, Martin Florian, and Hermann Elendner. 2019. Monetary Stabilization in Cryptocurrencies: Design Approaches and Open Questions. In *CVCBT.*

[8] Erica Pimentel, Emilio Boulianne, Shayan Eskandari, and Jeremy Clark. 2019. Systemizing the Challenges of Auditing Blockchain-Based Assets. SSRN.

Related Articles on ACM Queue.

Bitcoin's Academic Pedigree
by Arvind Narayanan and Jeremy Clark
https://queue.acm.org/detail.cfm?id=3136559

Blockchain Technology: What Is It Good for?
by Scott Ruoti, Ben Kaiser, Arkady Yerukhimovich, Jeremy Clark, and Robert Cunningham
https://queue.acm.org/detail.cfm?id=3376896

A Hitchhiker's Guide to the Blockchain Universe
by Jim Waldo
https://queue.acm.org/detail.cfm?id=3305265