# 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 its exchange rate. But can this new breed of cryptocurrency 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) [8]. The second wave, represented prominently by Bitcoin [7], 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*" [2].

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 that purport to provide a stable exchange rate similar to (or exactly mirroring) a government-issued currency like the USD. These designs are called stablecoins.

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.

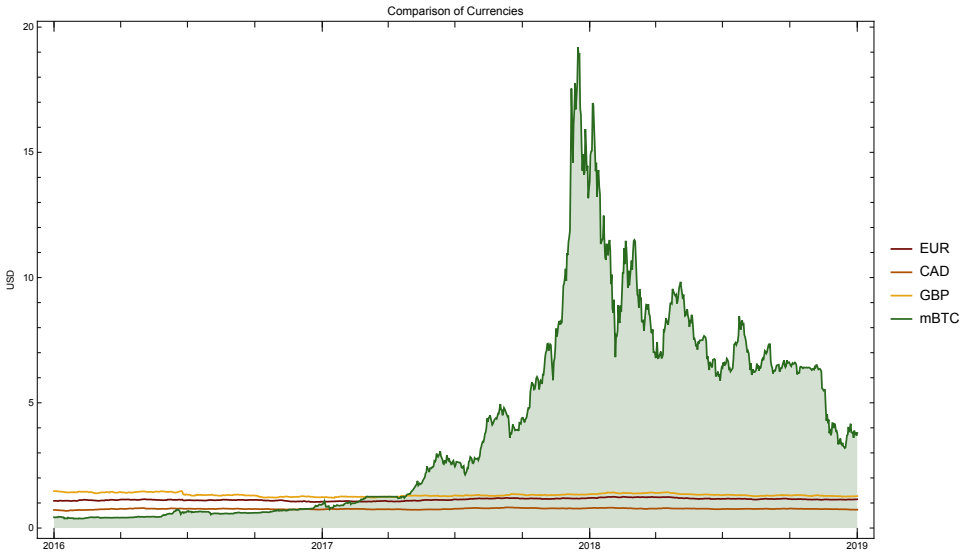


Fig. 1. Comparison among fiat currencies and Bitcoin: The values are retrieved daily between 01 Jan 2016 and 01 Jan 2019. Note that 1000 mBTC = 1 BTC.

*Knowledge gap.* Understanding how stablecoins work should be easy. Most firms/projects have a whitepaper outlining the design, the coins are marketed to the general public, 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 to be mislabeled. For example, a component that cleanly meets the definition of a security or a derivative might instead be 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 [6, 9].

Sidebar

**Prices.** A cryptocurrency (like any asset) has two prices: (1) the most someone is willing to pay and (2) the least someone is willing to sell for. These are referred to as the best bid price and best offer (or ask) price respectively. Note that the best bid price should logically be less than the best offer price, otherwise an exchange would happen (such prices might occasionally 'cross' but this should be temporal and quickly resolved with an exchange). Say a stablecoin is designed to ensure one unit is always priced at $1 USD. To argue stability, one must show both that (1) the bid price should never exceed $1 USD and (2) the offer price should never dip below $1 USD. Note, conversely, that bids can dip below $1 USD (everyone prefers to pay less than something is worth) and asks can exceed $1 USD (everyone prefers to receive more than something is worth).

Sidebar

**Bitcoin & Blockchain Primer.** A public blockchain is a type of distributed database (or ledger) that is open to anyone who wants to maintain it, robust against faulty and malicious participants, and runs without anyone in charge. When a participant looks at her local copy of the ledger, she is assured that (1) everyone has the exact same records and (2) each record was validated by the majority of participants before it was written into the ledger. Bitcoin is a digital currency that introduced the idea of a blockchain to track how much BTC is held by each account, and to write 'smart' transactions for BTC payments. Transactions are added to the blockchain in a batch (called a block) by a network participant (called a miner) and miners include a special transaction that pays themselves newly minted BTC (called a coinbase transaction). The amount of new BTC released to miners follows a schedule built into the protocol and will decrement over time, eventually reaching zero once a determined amount of BTC has been made available.

Sidebar

**Ethereum & DApp Primer.** Ethereum is a blockchain protocol with a BTC-esque cryptocurrency called Ether (ETH). To a degree much greater than Bitcoin, Ethereum allows users to code verbose 'smart contracts' or 'decentralized apps (DApps)' that can be stored on the blockchain (for a fee). Once a DApp is deployed, users can run its functions (again, for a fee). The functions are executed by the miners and the output is written to the blockchain. Among other things, DApps can hold ETH and write functions that define how the ETH will be transferred from the DApp. DApps can also create their own currencies and circulate them as tokens. ERC20 tokens are compliant with a widely used Ethereum standard and can interoperate with existing wallet software, web-based exchanges, and token-tracking websites.

## 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 a 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.

[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 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 sovereign 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.

Recall the mechanism for issuing AliceCoins 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 to take less than $1 USD for 1 AliceCoin, these coins can

| Stability Mechanisms |
|---|
| **Directly Backed and Redeemable.**<br>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.**<br>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.**<br>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 going 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 entire 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.**<br>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.**<br>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.

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 [10]).

### 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.

| *Mechanism* | Price | | Trust | | | |
|---|---|---|---|---|---|---|
| | Corrects undervaluation | Corrects overvaluation | Decentralizes issuance | Decentralizes redemption | Decentralizes transfer | No trusted oracle |
| 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.

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 [5], and it has not always maintained full reserves of USD to allow all Tether to be redeemed (for these reasons, we categorize it here). To many, it is a mystery 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 that it is too useful to fail.

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) withdraw 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, or regulatory oversight. The withdrawn stablecoin can be moved onto a different exchange, transferred to other users, or used for direct purchases without involving the original exchange. In short, it offers more flexibility than leaving USD in an exchange account and less friction than withdrawing USD.

### 3.3 Indirectly-Backed

Both of the previous mechanisms placed heavy trust assumptions on the firm operating the currency. Could a currency be managed autonomously by a DApp? The key idea of this mechanism is to offer a redeemable token that can be converted into $1 USD worth of ETH at the going USD/ETH exchange rate. Therefore the amount of ETH received ETH will grow or shrink depending on the exchange rate. Because a blockchain has no inherent knowledge of exchange rates, this mechanism still requires one trustworthy entity called an oracle to write the exchange rate into the blockchain (or consensus can be taken across a set of oracles).

Recall the mechanism in Table 2. Bids for an AliceCoin in excess of $1 USD will be fulfilled as long as there are individuals like Alice willing to lock up a deposit of ETH that is 1.5× the face-value of what they receive (this is called over-collateralization). An AliceCoin offered for less than $1 USD can be purchased and redeemed for a profit–assuming the DApp holds enough ETH. Otherwise, an AliceCoin will sell between $0 and $1 USD according to the value of the ETH held by the DApp.

Is it risky for Alice to offer such an AliceCoin? Holding the second place in line is more volatile than holding ETH itself—this stability mechanism does not (and cannot) eliminate volatility, it simply pushes it from the first place to the second place in line. However the second place in line is never more than $1 USD short of the full amount of ETH held in the DApp. So if Alice keeps the $1 USD she received for the AliceCoin, it offsets any losses from the second place in line. She has no more risk than holding ETH. The second place in line can also be sold to someone who is seeking risk: the token is a leveraged bet that ETH rises in value. Is it risky for Bob? In most conditions, holding an AliceCoin is purposefully the same as holding USD. However if the USD/ETH rate deteriorates quickly, the AliceCoin will use up its buffer and start to lose value (at the same rate as ETH).

Here are just a few of the design decisions to consider when deploying an indirectly-backed stablecoin: what should the overcollateralization ratio be (*e.g.,* 1.5x)? When can an AliceCoin be redeemed (*e.g.,* on-demand, after an elapsed time, after movements in USD/ETH, *etc.*)? How do you issue multiple AliceCoins (*e.g.,* collateral for each coin is held separately, or collateral for all coins are pooled together and coins are interchangeable)?

## 4 TYPE 2: INTERVENTION-BASED STABLECOINS

### 4.1 Money Supply Adjustments

A trusted oracle provides the going exchange rate between the cryptocurrency and a stable-valued asset, such as the USD. When the cryptocurrency gains value, the supply of the cryptocurrency is increased, and when it loses value, the supply is decreased. This mechanism is based on how central banks have historically controlled their economies, however the specifics of exchange rate targetting have been abandoned by modern central banks after past failures. That said, exchange rates are an illustrative example and other financial indicators could be used: oracle-provided interest rates (should lending markets emerge) or purchasing power; on-blockchain metrics like transaction volumes (should these prove robust against manipulation), or human discretion (such as central banks themselves [4]).

Allowing a crypto-currency to expand is not difficult. Who receives the new currency is a design decision with options including: (1) existing holders of the currency in proportion to their holdings, (2) existing holders through a random lottery, (3) miners, or (4) a specific entity like a central bank. Who loses when the currency contracts is the primary challenge.

The mechanism in Table 2 gives one illustration. Here if many bids for AliceCoin exceed $1.02 USD, some of the newly injected currency could be spent on obtaining USD until all buyers willing to pay more than $1.02 USD have purchased AliceCoins. This is merely a heuristical argument because there is no guarantee the recipients will spend the new currency on USD, especially if demand for USD is falling. The justification for offers below $0.98 is symmetric: the currency contractions could make holders less willing to spend it on USD. However if the

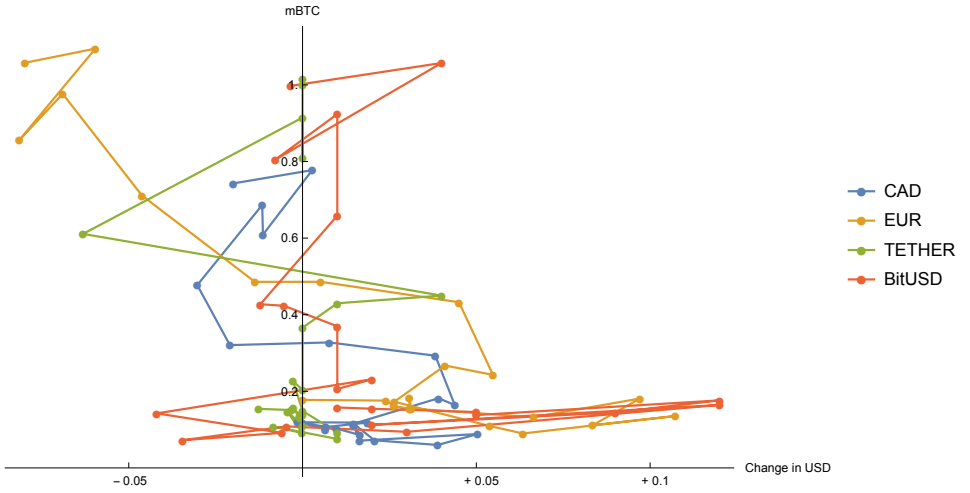


Fig. 2. Volatility in prices for two fiat currencies (CAD and EUR) and two stablecoins (Tether and BitUSD) against the USD and BTC. Vertical line segments demonstrate USD stability. Horizontal show the currency tracking BTC. For further interpretation, see [3]. While CAD and EUR are not pegged to USD, they demonstrate a degree of stability not that different from the stablecoins. Prices from Jan 2017 to Nov 2018; 1000 mBTC = 1 BTC.

price drop is caused by a lack of demand for AliceCoins rather than an oversupply, then removing supply will only thin out the market but not actually incentivize traders to trade and correct the undervaluation.

When the coinbase is increased or decreased dynamically (called an elastic coinbase), increases can be by any amount but decreases cannot appear to go past zero. When the coinbase is exactly zero, miners are still incentivized to mine because of the fees provided in the transactions. In fact this is how Bitcoin will eventually (projected to happen in 2140) function once all BTC is created (how well it will work is debatable [1]). Could the coinbase go negative? Since miners are rewarded the sum of the coinbase and the transaction fees, a coinbase can indeed be moderately negative if the transaction fees are greater than the negative coinbase. Under this deployment, the users are effectively burning their transaction fees to contract the money supply.

### 4.2 Asset Transfer

The second subtype of intervention-based stability mechanism expands and contracts the supply of currency to influence its value, however it uses a less direct contraction method. Recall the mechanism in Table 2. If many bids in excess of $1.02 USD remain unexecuted, the logic follows the previous section: the currency is handed out in hopes that more USD will be bought. The justification for offers below $0.98 is premised on individuals buying places in line, and if this premise is true, the resulting contraction of the currency follows the same logic as the previous section. The purchase of a spot in line is highly speculative — the currency might not return to stability and the spot might never be reached. As the line gets longer, the price of a place in line will fall, and the speculative market will thin out to traders wanting a higher and higher risk/reward ratio. These trends do not guarantee, or even point toward, a recovery in price.

## 5 DISCUSSION AND CONCLUSION.

A more detailed version of this article is available as a whitepaper [3]. It includes more detail about each coin, some empirical studies of how stable these coins are (see Figure 2 for a preview), and an evaluation of whether of

Ethereum's mechanism for paying for computation (gas) is stable or not (the answer: it does not seem to be, for now).

In short, stablecoins might tokenize a low volatility coin and bring it onto the blockchain. Or they generally play one of two tricks. The first trick is to expand and contract the amount of currency to stabilize the value. The second trick is to turn two high volatility coins (*e.g.,* of the underlying cryptocurrency) into one stablecoin and one extremely volatile coin. This last trick is similar to other financial assets which do not reduce overall risk, but instead push it from one tranche of the asset to another.

Why are there so many projects? The differentiation between coins is along a few parameters: (1) the type of asset that can be redeemed for the coin: USD, EUR, gold, *etc.*; (2) the underlying blockchain (*e.g.,* Bitcoin, Ethereum, *etc.*) and the low-level technical design (updatable contracts, governance, *etc.*); and (3) the country it operates from which determines the degree of regulatory compliance that's required.

What's next? Self-sovereign stablecoins are interesting and probably here to stay, however they face numerous regulatory hurdles from banking, financial tracking, and (likely) securities laws. For stablecoins backed by a governmental currency, the ultimate expression would be a centrally banked digital currency (CBDC). Since paper currency has been in steady decline (and disproportionately for legitimate transactions [11]), a CBDC could reintroduce cash with technological advantages and efficient settlement while minimizing user fees.

## 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] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. 2016. On the instability of bitcoin without the block reward. In *ACM CCS*. ACM, 154–167.
[2] Phil Champagne. 2014. *The book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto*. e53.
[3] Jeremy Clark, Didem Demirag, and Seyedehmahsa Moosavi. 2019. SoK: Demystifying Stablecoins. SSRN 3466371.
[4] George Danezis and Sarah Meiklejohn. 2016. Centrally banked cryptocurrencies. In *NDSS*.
[5] John M Griffin and Amin Shams. 2018. Is bitcoin really un-tethered? *Available at SSRN 3195066* (2018).
[6] Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. 2020. SoK: A Classification Framework for Stablecoin Designs. In *Financial Cryptography*.
[7] Satoshi Nakamoto et al. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).
[8] A Narayanan, J Bonneau, Edward W. Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies*. Princeton.
[9] 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*.
[10] Erica Pimentel, Emilio Boulianne, Shayan Eskandari, and Jeremy Clark. 2019. Systemizing the Challenges of Auditing Blockchain-Based Assets. SSRN.
[11] Kenneth S Rogoff. 2017. *The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy*. Princeton University Press.

**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

**Authors.**

**Jeremy Clark** is an associate professor at the Concordia Institute for Information Systems Engineering in Montreal, Canada, where he holds the NSERC/RCGT/Catallaxy Industrial Research Chair in Blockchain Technologies. He collaborates regularly with government agencies on voting and blockchain technologies.

**Didem Demirag** is a PhD student at the Concordia Institute for Information Systems Engineering in Montreal, Canada. She is interested in applied cryptography, genomic privacy, blockchain applications. She is currently working on realizing secure function evaluation using blockchain and is an intern at Autorité des Marchés Financiers, Montreal.

**Seyedehmahsa Moosavi** is a Ph.D. student at the Concordia Institute for Information Systems Engineering in Montreal, Canada. She previously worked as a research intern at the Autorité des Marchés Financiers, Québec, and now focuses on understanding the future of financial technologies (FinTech) using blockchains.