DOI:10.1145/3386275

Article development led by acmqueue
queue.acm.org

Cryptography meets monetary policy.

BY JEREMY CLARK, DIDEM DEMIRAG, AND SEYEDEHMAHSA MOOSAVI

Demystifying Stablecoins

THE FIRST WAVE of cryptocurrencies, starting in the 1980s, attempted to digitize 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 hard-coded 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. Figure 1 shows a comparison of fiat currencies and bitcoin. The values were retrieved daily between Jan. 1, 2016 and Jan. 1, 2019. (Note that 1,000 mBTC = 1 BTC). Squint at the chart to notice how the GBP (British pound) drops around June 2016: This mild-looking pinch is actually the so-called "sharp decline" and "severe swing" that followed the Brexit referendum in the U.K. It is completely overshadowed, however, when placed beside BTC's large fluctuations.

A Third Wave?

Extreme volatility is not specific to BTC. It can also be seen in its contemporaries: ETH (ether) and XRP (Ripple). This instability is an issue of practical

IMAGE COMPOSITION BY ANDRIJ BORYS ASSOCIATES. USING PHOTO BY RUDMER ZWERVER

importance: Volatility encourages users to hoard (if the value 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 U.S. dollar. These designs are called *stablecoins*.

Stablecoins have garnered a lot of attention recently, both positive and negative. According to *CoinMarketCap*, a service that provides financial metrics for cryptocurrencies, more value in tether (a cryptocurrency issued by Tether Limited) changes hands across a given day than bitcoin—despite questions about tether's reserves and regulatory investigations into its affiliates. The announcement of Facebook's Libra stablecoin project made international headlines and has been remarked on by the Federal Reserve Board, U.S. legislators, and even the sitting U.S. president. Another project, Basis (*née* Basecoin) raised $133 million in venture capital but folded when it could not find a tenable path through U.S. financial regulations. Central banks, including those of Sweden and Denmark, have explored the idea of government-issued stable cryptocurrencies.

Stablecoins promise the functionality of Bitcoin without the roller-coaster ride of its exchange rate. But can this new breed of cryptocurrency really outsmart decades of central bank policy with algorithms and smart contracts?

Knowledge Gap

Understanding how stablecoins work should be easy. Most projects have white papers 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 white papers are obfuscated with jargon—terms left undefined and used inconsistently across other projects and the financial literature. In other cases, system components appear to be mislabeled. For example, a component that clearly 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. Maybe it is a play to make an unconventional protocol appear more conventional. Or maybe these are un-

Figure 1. Comparison among fiat currencies and Bitcoin.

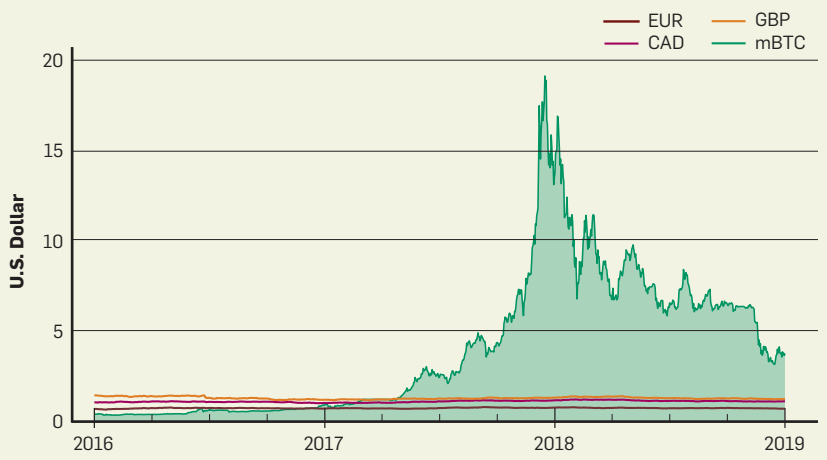


Figure 2. Stablecoin proposals as of Jan. 11, 2019.

Class	Mechanism	Resembles	Rank
Backed	Directly Backed and 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	⊥

conscious attempts at keeping any regulatory red flags at half-mast. In any case, here we make an effort to offer direct and simple explanations. In parallel to our work, other academics have produced their own taxonomies.[6,9]

How Do Stablecoins Work?

We started by finding stablecoin projects on CoinDesk, an online news source for cryptocurrencies, using search queries such as "stablecoins," "stability," and "price-stable." This resulted in 185 articles up to Jan. 11, 2019. (Given its high profile, Facebook's Libra coin, which was released after this date, is included.) The 25 projects for which there was sufficient documentation were classified as shown in Figure 2. Projects are classified according to what they assert (for example, there is no warranty that projects classified as "redeemable" provide actual redemption of the assets that back their coins). Projects are sorted according to their rank on *CoinMarketCap*, which evaluates cryptocurrencies that are actively traded on an exchange service. Unlisted projects are ranked ⊥.

Next, each project was distilled into a core stability mechanism. Instead of enumerating the intricate details of how each "brand" of stablecoin works—details that could change tomorrow—we concentrated on the fundamentals. Broadly, the projects can be split into two categories: those that try to directly match the stability of a second asset such as the U.S. dollar and could not exist without this underlying asset; and those that propose independent currencies with algorithmic and/or human intervention mechanisms for providing stability.

Type 1: Backed Stablecoins

The first general type of stablecoin tries to match the stability of a second *target* asset, such as the U.S. dollar, either by making use of it (*directly backed*) or by making use of a third *reserve* asset like ETH (*indirectly backed*). These stablecoins could not exist without their underlying assets.

Directly backed and redeemable. For stablecoins in this category, the company operating the cryptocurrency obtains a reserve of some valuable asset—it might be the U.S. dollar or another sovereign currency, gold or another commodity, or a basket of multiple assets. It then issues digital tokens that represent a unit of the underlying asset, which can be exchanged online (to illustrate, assume a token is redeemable for $1).

Working Example: Alice is a trusted third party and uses Ethereum to instantiate a DApp (decentralized application), which issues 1,000 AliceCoins as standard tokens (for example, ERC20). She asks $1 USD for one 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. Whenever Alice receives a buy order for AliceCoins and does not have any left to sell, she creates new ones. If Carol wants to redeem five 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 U.S. dollars to redeem all coins in circulation (the number of AliceCoins can be checked any time on Ethereum. For more information, see the sidebar "Ethereum and DApp Primer.").

The idea of directly backed and redeemable currency predates Bitcoin: Liberty Reserve provided a similar digital currency, with some caveats about its redeemability (not to mention its legality). Liberty Reserve, e-gold, and similar pre-blockchain services, however, 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 (see sidebar "Bitcoin and Blockchain Primer."). In short, this type of stablecoin is more centralized than Bitcoin but less than Liberty Reserve. 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.

For finer-grained analysis, Figure 3 provides a comparative evaluation where a filled circle (●) indicates the properties (columns) are fulfilled by the corresponding mechanism (rows) within reason. A half circle (◒) means the property is fulfilled but the fulfillment is bounded. An open circle (○) means it is unfulfilled. A question mark (?) indicates a heuristic has been proposed for stability and the conditions under which it will work are not well enough established to evaluate. Finally, (×) indicates the property is not applicable.

Recall the mechanism for issuing AliceCoins. 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, those 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 necessarily happen; as we will discuss). 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 audit-

Bitcoin and Blockchain Primer

A public blockchain is a type of distributed database (or ledger) that is open to anyone who wants to maintain it, is robust against faulty and malicious participants, and runs without anyone in charge. When participants look at a local copy of the ledger, they are assured that everyone has the exact same records and that 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 of its currency (BTC) is held by each account, and to write "smart" transactions for 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 them 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.

Ethereum and 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 applications (DApps), which 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, a DApp can receive and store ETH and define functions for how ETH can 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.

Figure 3. Comparitive evaluation of mechanisms to design stablecoins.

	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	?	◒	●	×	●	◒

Prices

A cryptocurrency (like any asset) has two prices: the most someone is willing to pay; and 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 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 the bid price should never exceed $1 and that the offer price should never dip below $1. Note, conversely, that bids can dip below $1 (everyone prefers to pay less than something is worth) and asks can exceed $1 (everyone prefers to receive more than something is worth).

ing blockchain-based assets[10]).

Directly backed. What if a stablecoin operates exactly as in the previous section but does not offer a redemption process for the coin's underlying assets? If there is no clear assertion of redemption, the project is listed as directly backed in Figure 2.

Working Example: Alice is a trusted third party that issues 1,000 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. She offers no direct redemption of AliceCoins for U.S. dollars.

Here, bids will not exceed $1 for the same reason as mentioned previously. There is no longer a way to profit, however, if offers vary between $0 USD and $1 USD (that is, the mechanism does not prevent undervaluation). Generally, coins in this category are, in fact, redeemable by one user: the company 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 operating firm) to ensure reserves are intact. If every AliceCoin is 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, the firm is accused of issuing coins to manipulate markets,[5] and the firm has not always maintained full reserves of U.S. dollars 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) including Bitcoin. 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. Traders who want to divest their BTC for U.S. dollars have three options: (1) Hold the U.S. dollars in an exchange account, which can be used only on the same exchange and requires the exchange to be a trustworthy custodian; (2) withdraw the U.S. dollars 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; (3) exchange BTC into a stablecoin that can be withdrawn from the exchange (that is, moved from the exchange to Alice's private key) with little friction, delay, or regulatory oversight. This third option is a balanced alternative—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 U.S. dollars in an exchange account and less friction than withdrawing U.S. dollars.

Indirectly backed. Both of the previous mechanisms—directly backed and redeemable, and directly backed—place heavy trust assumptions on the company operating the currency (recall Figure 3). 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 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).

Working Example: 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 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 stablecoin called AliceCoin) to Bob for $1 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.

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 times 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 the ETH itself. This stability mechanism does not (and cannot) eliminate volatility; it simply pushes it from first place to second place in line. The second place in line, however, is never more than $1 USD short of the full amount of ETH held in the DApp. By keeping the $1 USD she received for the AliceCoin, Alice 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 U.S. dollars. If the USD/ETH rate deteriorates quickly, however, the AliceCoin will use up its buffer and start to lose value (at the same rate as ETH).

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

Type 2: Intervention-based Stablecoins

The second broad category of stablecoins encompasses those that propose independent currencies with algorithmic and/or human intervention mechanisms for providing stability.

Money supply adjustments. A trusted oracle provides the going exchange rate between the cryptocurrency and a stable-valued asset, such as the U.S. dollar. When the cryptocurrency gains value, the supply of the cryptocurrency is increased; 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 targeting have been abandoned by modern central banks after past failures.

That said, exchange rates are an example, and other financial indicators could be used: oracle-provided interest rates (should lending markets emerge) or purchasing power; on-blockchain metrics such as transaction volumes (should these prove robust against manipulation); or human discretion (such as central banks themselves[4]).

Allowing a cryptocurrency to expand is not difficult. Who receives the new currency is a design decision with options including: existing holders of the currency in proportion to their holdings;existing holders through a random lottery; miners; or a specific entity such as a central bank. Determining who loses when the currency contracts is the primary challenge.

Working Example: Alice forks Bitcoin to create a new altcoin called AliceCoin. She tweaks the schedule for releasing new AliceCoins (called the *coinbase* amount) according to the rules outlined here. She sets up a trusted oracle for the latest exchange rate of AliceCoins to U.S. dollars. 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 (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.

If many bids for AliceCoin exceed $1.02 USD, some of the newly injected currency could be spent on obtaining U.S. dollars 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 U.S. dollars, especially if demand for the dollar is falling. The justification for offers below $0.98 is symmetric: The currency contractions could make holders less willing to spend it on U.S. dollars. If the price drop is caused by a lack of demand for AliceCoins rather than an oversupply, however, then removing supply will only thin out the market but not actually give traders incentive to trade and correct the undervaluation.

When the coinbase is increased or decreased dynamically (this is 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 still have incentive 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 debatable1).

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, users are effectively burning their transaction fees to contract the money supply.

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, as shown in the following example.

Working Example: Alice instantiates a DApp with an ERC20 token called an 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 a new set of AliceCoins (as before, 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.

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 U.S. dollars will be purchased. Offers below $0.98 are justified on the premise that individuals will buy 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 falls, and the speculative market thins out to traders wanting a higher and higher risk/reward ratio. These trends do not guarantee, or even point toward, a recovery in price.

Discussion and Conclusion

In summary, some stablecoins tokenize a low-volatility coin and bring it onto the blockchain. Others generally play one of two tricks: The first is to expand and contract the amount of currency to stabilize the value; the second is to turn two high-volatility coins (for example, of the underlying cryptocurrency) into one stablecoin and one extremely volatile coin. This last trick is similar to other financial assets that do not reduce overall risk but instead push it from one tranche of the asset to another.

A more detailed version of this article is available as a white paper.[3] It includes more details and discussion about the categories, some empirical studies of how stable these coins are, reasons stablecoins are never perfectly stable, and an evaluation of whether Ethereum's mechanism for paying for computation (gas) is stable or not (the answer: it does not seem to be, for now).

Figure 4 is taken from the white paper and shows volatility in prices for two fiat currencies (Canadian dollar [CAD] and Euro [EUR]) and two stablecoins (Tether and BitUSD) against USD and BTC (prices from January 2017 to November 2018; 1000 mBTC = 1 BTC). A vertical line segment indicates the currency correlates with USD, while horizontal correlates with BTC. While CAD and EUR are free-floating currencies, they demonstrate a degree of stability not that different from the stablecoins, which demonstrates the stability of similar central banking operations in these economic zones. (See the sidebar entitled "Prices.")

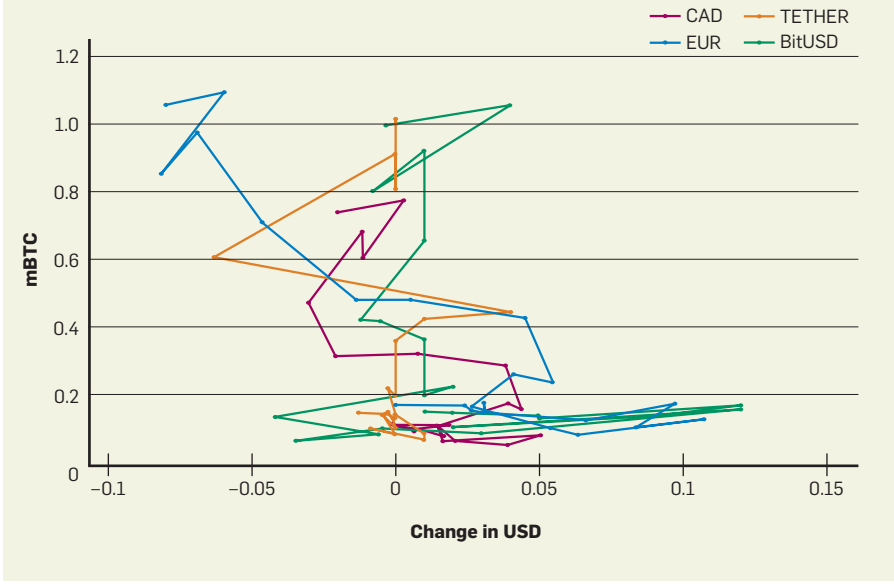
Why are there so many stablecoin projects? The differentiation among coins is along a few parameters: the type of asset that can be redeemed for the coin: USD, EUR, gold, and so on; the underlying blockchain (for example, Bitcoin, Ethereum, among others) and the low-level technical design (updatable contracts, governance, among others); and the country it operates from, which determines the degree of regulatory compliance that is 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 AMF (Autorité des Marchés Financiers) and the National Sciences and Engineering Research Council (NSERC)/Raymond Chabot Grant Thornton/Catallaxy Industrial Research Chair in Blockchain Technologies. S. Moosavi acknowledges support from Fonds de Recherche du Québec – Nature et Technologies (FRQNT).

Figure 4. Volatility in prices for fiat currencies and stablecoins.



Related articles on queue.acm.org

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

Blockchain Technology: What Is It Good For?
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
Jim Waldo
https://queue.acm.org/detail.cfm?id=3305265

References

1. Carlsten, M., Kalodner, H., Weinberg, S.M., Narayanan, A. On the instability of bitcoin without the block reward. In *Proceedings of the ACM SIGSAC Conf. Computer and Communications Security*, 2016, 154–167.
2. Champagne, P. *The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto.* e53 Publishing, 2014.
3. Clark, J., Demirag, D., Moosavi, S. SoK: Demystifying Stablecoins. Social Sciences Research Network, 2019; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3466371.
4. Danezis, G., Meiklejohn, S. Centrally banked cryptocurrencies. In *Proceedings of the Network and Distributed System Security Symp*, 2016.
5. Griffin, J.M., Shams, A. Is Bitcoin really un-tethered? Social Sciences Research Network, 2018; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066.
6. Moin, A., Sekniqi, K., Sirer, E.G. SoK: A classification framework for stablecoin designs. *Financial Cryptography*, 2020
7. Nakamoto, S. Bitcoin: a peer-to-peer electronic cash system, 2008; https://bitcoin.org/bitcoin.pdf.
8. Narayanan, A., et al. *Bitcoin and Cryptocurrency Technologies.* Princeton University Press, Princeton, NJ, 2016.
9. Pernice, I.G.A., et al. Monetary stabilization in cryptocurrencies: design approaches and open questions. In *Proceeding of the IEEE Crypto Valley Conf. Blockchain Technology*, 2019.
10. Pimentel, E., Boulianne, E., Eskandari, S., Clark, J. Systemizing the challenges of auditing blockchain-based assets. *Social Sciences Research Network Electronic J.*, 2019.
11. Rogoff, K.S. *The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy.* Princeton University Press, Princeton, NJ, 2017.

Jeremy Clark is an associate professor at the Concordia Institute for Information Systems Engineering in Montreal, Canada, where he holds the NSERC/Raymond Chabot Grant Thornton/Catallaxy Industrial Research Chair in Blockchain Technologies.

Didem Demirag is a Ph.D. student at the Concordia Institute for Information Systems Engineering in Montreal, Canada. She is 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, focusing on understanding the future of financial technologies using blockchains.