SoK: Demystifying Stablecoins[*]

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) [9]. The second wave, represented prominently by Bitcoin [8], 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.

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
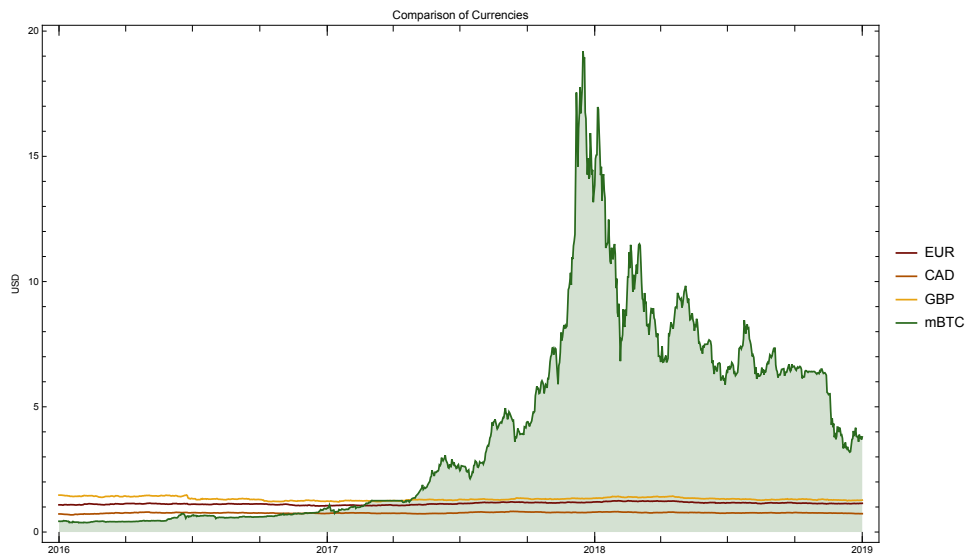

Fig. 1. Comparison among fiat currencies and Bitcoin: The values are retrieved daily between 01 Jan 2016 and 01 Jan 2019. Note that 1000 mBTC = 1 BTC.

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 [7, 11].

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 ⊥.

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.
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 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.
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.

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 [12]).

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.

	Corrects undervaluation	Corrects overvaluation	Decentralizes issuance	Decentralizes redemption	Decentralizes transfer	No trusted oracle	Any asset	Any price level	Any event
Mechanism	Price		Trust				Target		
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. Price and trust are explained in the main text and target is explained in Appendix B.1.

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 targeting 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
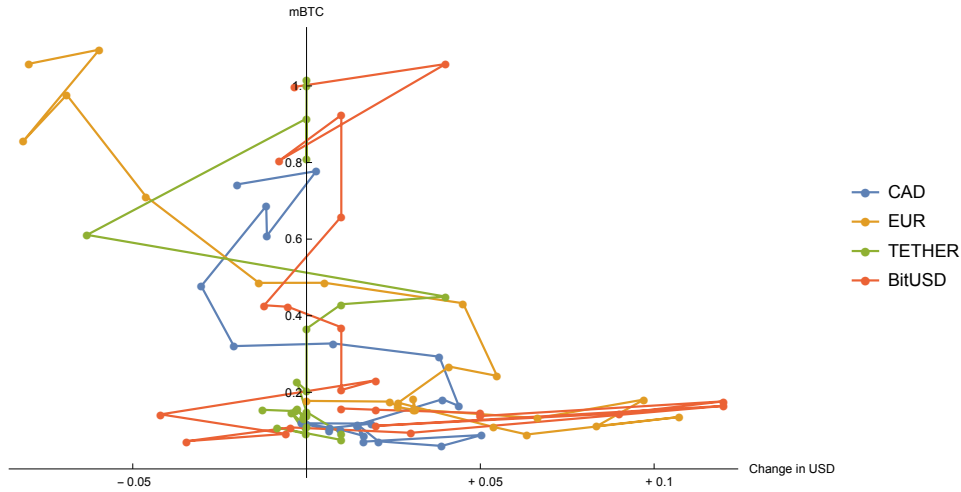
Fig. 2. Volatility in prices for two fiat currencies (CAD and EUR) and two stablecoins (Tether and BitUSD) against the USD and BTC. Vertical line segments demonstrate stability with the USD. Horizontal shows volatility in USD. For further interpretation, see Appendix A.2. While CAD and EUR are not pegged 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.

8

5 DISCUSSION AND CONCLUSION.

More details are available in the appendix. 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 [13]), a CBDC could reintroduce cash with technological advantages and efficient settlement while minimizing user fees.

ACKNOWLEDGMENTS

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. 2020. Demystifying Stablecoins. *Commun. ACM* (2020).

[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] Larry Harris. 2003. *Trading and exchanges: Market microstructure for practitioners*. Oxford University Press, USA. 410–419 pages.

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

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

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

[10] Mildred Chidinma Okoye and Jeremy Clark. 2018. Toward Cryptocurrency Lending. In *International Conference on Financial Cryptography and Data Security*. Springer, 367–380.

[11] 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*.

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

[13] Kenneth S Rogoff. 2017. *The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy*. Princeton University Press.

[14] Gavin Wood. 2014. Ethereum yellow paper. *Internet: https://github. com/ethereum/yellowpaper,[Oct. 30, 2018]* (2014).

A   EXPANDED BACKGROUND

A.1   Prices

If 1 BTC is worth $3598.76 USD, as Google says it is at the time of writing, what does that actually mean? There are several subtleties here: (1) what that price actually represents, (2) the relationship between a quoted price and its actual price, (3) the concept that prices are really an exchange of one type of valuable good for another, and (4) the distinction between something's price and its value.

The quoted price means that two (hopefully different[2]) people recently exchanged BTC and USD at a valuation of 1 BTC for $3598.76 USD. First, note that it does not necessarily mean that exactly 1 BTC was exchanged — it could have been 1 mBTC for $3.60 or 1000 BTC for $36M USD. Further, this valuation on the previous trade does not mean you will necessarily be able to exchange 1 BTC for $3598.76 USD. Last sale price is an indicator of current price that becomes stale as time between subsequent exchanges increase (for example, for a house that last sold 30 years ago, last sale price on a house is not a good indicator of current price).

Instead, we will use the idea of that a cryptocurrency (or 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 ask (or offer) price respectively. Note that the best bid price should logically be less than the best ask price, otherwise an exchange would happen (such prices might occasionally 'cross' but this should be temporal and quickly resolved with an exchange). The spread between these prices is called the bid-ask spread.

To understand why this is relevant to stablecoins, consider an example. 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 dollar 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).

A.2   Exchange rates

Consider that several hours after writing the previous section, 1 BTC is now priced at $3566.56 USD. In one sense, the price of BTC decreased by $32.20. However it is exactly equivalent to say the price of $1 USD increased by 0.002 mBTC. This raises a natural question: did BTC decrease in price or did USD increase in price? With an exchange rate, it is impossible to tell. We only know that the price of BTC and USD became closer in price over this short period of time.

To determine which currency is moving, one might consider a third or forth currencies (*cf.* US Dollar Index) to try and triangulate if BTC is moving in price, or USD is moving in price, or both. For example, in Figure 1 it certainly appears that BTC is the currency that is moving because the rest of the currencies are stable relative to each other. The only alternative is that USD, EUR, GBP, and CAD are volatile currencies that move together as a cluster relative to the stability of BTC. But it is much simpler to conclude that BTC is moving.

In order to apply this same logic in a visual way, we have created a number of charts like the one provided in Figure 3a. Unlike most exchange rate graphs, these do not use a time axis. Instead each axis is a reference currency. In this case, the price of GBP (plotted value) in USD (x-axis) and EUR (y-axis) form a coordinate. For the last day of each month, a new coordinate is added and joined with a line from the previous value. This is inspired by similar charts on the website FiveThiryEight for things like kicking distance in football[3] and they have been called connected scatter plots.

Lines in a connected scatter plot can move in any direction. Figure 3b shows how we number the directions from 1 (upward or due north) clockwise to 8 (north-west). For each direction, we describe the simplest interpretation of what that price direction means. By simplest, we mean specifically that we keep an explanation that involves

---

[2]A trade between the same person is called a wash trade and is illegal in most regulated markets.

[3]"The 52 Best—And Weirdest—Charts We Made In 2016," *FiveThirtyEight*, 30 Dec 2016.

(a) GBP with respect to EUR and USD.

(b) Direction labels.
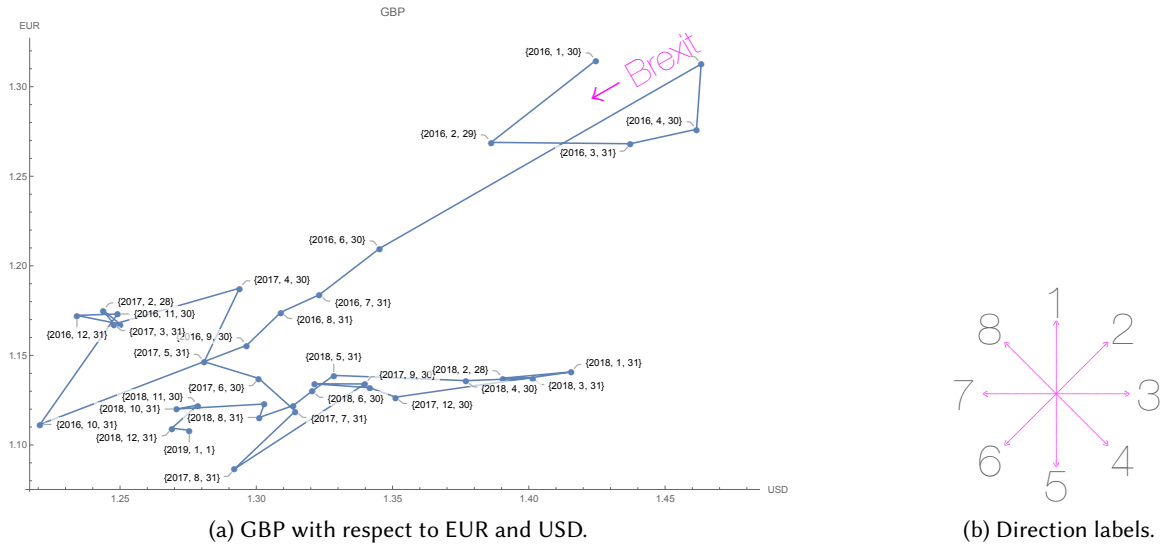
Direction	Interpretation
1/5	Y is losing (1) / gaining (5) value
2/6	Plotted asset is gaining (2) / losing (6) value
3/7	X is losing (3) / gaining (7) value
4/8	Plotted asset is gaining (4) / losing (8) value against X, while losing (4) / gaining (8) value against Y

(c) The simpliest interpretation of the plots where X refers to the currency on the x-axis (likewise Y).

Fig. 3. A connected scatter plot of GBP's exchange rate with EUR and USD demonstrating the effect of Brexit on GBP. Supporting documentation helps interpret the line movements in the plot.

a single currency moving rather than an explanation that involves a pair of currencies moving in tandem. For example, in Figure 3a, GBP shows a drastic movement along direction 6 starting at the time period marked Brexit. This means that GBP is losing value against both EUR and USD. The simplest explanation is that the movements are originating from GBP which is consistent with it losing value after Brexit. Later, GBP shows a lot of horizontal movements along the 7/3 line. The simplest explanation for this segment is volatility in USD rather than GBP. A copy of the datasets and codes of all the charts can be found on our GitHub repository.[4]

We will return to these charts later in Section B.4 where we will use a government currency as one reference (USD on the x-axis) and a cryptocurrency as the other reference (BTC on the y-axis). A stablecoin should exhibit mostly vertical movements along the 1/5 direction.

A.3 Valuation

Recall that in the previous section, 1 BTC was priced at $3566.56 USD. This means that two people recently swapped some amount of BTC and USD for the stated valuation. Does this mean 1 BTC is worth $3566.56 USD? Value can mean different things in different contexts. The market value of a currency does present one type of

---

[4]https://github.com/mahsamoosavi/Stablecoins

value — its replacement value, or the cost in USD to replace it. Note that more technically, one should determine replacement value from the set of best offer prices sufficient to cover the volume of BTC being valued.

But does this mean that BTC is fundamentally worth $3566.56 USD. This is unlikely because by the time you read this paper, the price of BTC in USD is probably quite different from this quoted value (perhaps humorously so). So what constitutes fundamental value? And why do prices change over time?

Stocks represent ownership in a firm, and thus a stake in the firm's equity. Therefore shares (called equities) have a fundamental value called its book value: simplified, it is the firm's capital or equity (the value of its assets minus the value of its liabilities, as reported on its annual audited financial statement) divided by the number of outstanding shares. Working in reverse, the price of a single share multiplied by the number of shares represents the market capitalization of the firm. In theory, these numbers should be the same but often are not. When the market capitalization exceeds the reported capital, the market believes the firm's capital will increase over time. If the market capitalization is less than the reported capital, it demonstrates a lack of confidence in the soundness of the firm's financial statements. Floating currencies like the USD, EUR, GBP, and CAD do not have the equivalent of a book value.

To explain Bitcoin's exchange rate with fiat currencies, an oft-repeated theory has emerged that attributes Bitcoin's value to the hydro consumed by blockchain mining. While imprecise, the theory suggests that if a valuable resource x is consumed to produce y, the value of x is imparted into y. Setting aside the nuance that the hydro contributed to the Bitcoin system only indirectly produces new coins (it produces blocks, and blocks produce coins only for now), there is no economic principle underlying this transfer of value.

A.4 Stability and volatility

When the price of a currency changes over time, it is due to one of two reasons: new information about the currency's fundamental value (even if we cannot concretely say what it is) or transitory volatility due to the trading activites of uninformed traders [6]. For a government issued currencies, information like national inflation rates, macro-economic policies, changes in trade flows, and changes in capital flows seem predictive of changes in the value of the country's currency [6]. Note that a cryptocurrency, like Bitcoin, has none of these indicators. While volatility can be measured mathematically (using variances or deviations), most stablecoins do not offer a concrete, positive definition of what stability means. They tend to be defined by a negative sentiment of what they do not want (the volatility of Bitcoin) rather than a positive sentiment of what they do want.

A.5 Functions of money

There is controversy over whether Bitcoin, and other cryptocurrencies, can even be classified as currencies. The original intent from Bitcoin's creator was for it to be a currency, however it has been assigned many different classifications: from a digitally scarce commodity, to a speculative instrument, to an entirely new asset class.

Most introductory finance textbooks classify currencies according to a set of three core properties they should fulfill for their users. it should operate as a medium of exchange, which roughly means that Alice will accept the currency from Bob because she is confident Carol will later accept it from her. Given the existence of exchange services, Bitcoin is generally considered an acceptable medium of exchange (albeit with some friction). Next, a currency is useful when it serves as the unit of account for pricing other assets. Bitcoin is almost never used as a unit of account and if goods are sold for Bitcoin, it is often priced in, say, USD with a short-lived (*e.g.*, 2 minute) spot conversion of the price to BTC for Bitcoin purchases. Finally, currencies should represent a stable store of value. Alice will not accept a currency that depreciates quickly in value from Bob because even though Carol might accept it, what she can obtain from Carol in exchange will be worth less. Less intuitively, currencies that appreciate quickly in value are equally problematic. Alice might gladly accept it from Bob but Bob is unlikely to part with it, and so currencies like this tend to be hoarded. They also hamper lending (see next section).

The goal of a stablecoin is to add the store of value feature to cryptocurrencies, which are already a somewhat adequate medium of exchange. Further, if the currency is stable, it may become a more prominent to use it as a unit of account. Thus stablecoins are intended to make cryptocurrencies more currency-like.

A.6 Lending

Lending a volatile currency poses a risk for both the cash provider and cash taker. Currency depreciation results in the cash provider being repaid less than what they initially provided, and currency appreciation results in the cash taker having to repay a great amount than what was borrowed. Thus a stable currency enables low-risk lending which is beneficial to all participants and is the cornerstone of a modern economy. Okoye *et al.* put it in a way that is hard to improve on:

> "It is difficult to overstate the role of lending in a modern economy. Take, as an illustrative example, the role of a central bank; one of the main national institutes (along with the treasury) that cryptocurrencies aim to displace. First and foremost, a central bank is an actual bank, providing accounts for its member banks to deposit money and earn interest. Member banks provide interest-earning accounts to the public. Interest is paid to the public because banks use the deposited money to form loans. Because central bank interest rates are low, banks prefer to lend to other banks any excess cash they hold at day's end instead of depositing them (other banks borrow to meet liquidity requirements). These loans earn interest, and central banks target this specific lending rate when they intervene in the economy. The most common intervention is the buying (circulating new money) or selling (removing circulating money) of government bonds, which are interest-earning loans from investors to the government. Central banks will also provide loans (of 'last resort') to banks unable to secure loans from other banks, typically during some sort of liquidity crisis. An economy without loans would have no interest rates, no bonds, and essentially nothing for a modern central bank to do. [10]"

A.7 Foundations of Bitcoin's exchange rate

Without government oversight, the exchange rate of Bitcoin is dependent on: (a) the supply and demand for exchanging Bitcoin and other things of value, namely fiat currencies such as the USD; (b) it's internal algorithm for releasing new BTC (Bitcoin's currency) on a fixed schedule; and (c) the market for participating in transaction validation which is integral into how new BTC comes into circulation.

B DISCUSSION POINTS

B.1 Which stability mechanism is best?

Recall the evaluation in Figure 3. The main takeaway of this table is that no stability mechanism is strictly better than any other. Each mechanism represents a unique configuration of trust and financial features.

Valuation. A directly backed and redeemable mechanism provides the strongest method to correct under- and overvaluation (*e.g.,* a USD-backed coin trading for less or more than 1 USD). If redemption is not allowed, arbitrary traders have no method to profit from undervalued coins (however the issuer could purchase and redeem them if active in the market). Indirectly backed coins allow redemption except when the currency backing the coin loses enough value against the pegged coin.

Intervention-based approaches argue that they correct under- and overvaluation, however there is no mechanism reasonably guarantees that the trader's corrective actions will yield them profit. We refer to the proposed stability mechanisms as *heuristics* because their validity can only be shown within models that may or may not actually model human (and trader) behaviour. In fact, this is the best case scenario. Most of these heuristics do not

even have models or simulations showing the conditions under which they work, however there is interesting future work to be done here.

Trust. All stability mechanisms requires at least one trusted party. For directly backed coins, this entity issues and redeems digital coins, while maintaining the reserve of backing coins. This is a heavy reliance on a trusted third party.

Indirectly backed coins require an oracle for price target information, but otherwise could be operated autonomously. While a corrupt oracle could damage the coin to a great extent, the reduction in trust is still significant because the role of an oracle is much smaller than operating a fully backed coin. Because the barrier to entry is lower for an oracle, reputable firms may be more willing to participate in this role. In practice, information from oracles is taken through the consensus of a set of individual oracles to improve trustworthiness.

The degree to which an indirectly backed coin operates autonomously can differ between theory and practice. For example, the prominent example, dai/sai, includes a complex infrastructure of additional stability mechanisms beyond the core mechanism in Table 2. At the time of writing, this includes constant adjustment of certain frees and rates that makes the whole system resemble the operations of a central bank. While adjustments are made by a shareholder's vote and thus decentralized, guidance is provided by the foundation overseeing the coin through a conference call. This is illustrates that there are pragmatic challenges to operating a truly 'decentralized' and 'autonomous' stablecoin.

Intervention-based stablecoins provide the most promise for a minimal trust base. Bitcoin, Ethereum, and other cryptocurrencies already operate a fully autonomous, albeit not stable, mechanism for creating value. In theory, achieving this with less volatility seems possible. Such coins might rely on a trusted oracle if the price target is external to the blockchain (we illustrated the coins as targeting USD which requires an oracle). Alternatively, intervention-based stablecoins might fully embrace a trusted third party to offer intervention based on human expert discretion.

Stability targets. Depending on its design, a stablecoin potentially involves up to two additional components: the reserve asset and the target. For example, a directly backed stablecoin with a USD reserve is intended to match the price of USD. We say its reserve asset is USD and its price target is also the USD. Directly backed stablecoins always have the same reserve and target. Because the reserve has to be an asset that can be held in custody, the target has to also be an asset that can be held. This includes (but it not limited to) currencies, commodities, securities, and baskets of assets.

An indirectly backed asset uses a reserve asset that is different from the price target. For example, ETH might be held in reserve for a stablecoin that targets the USD. On redemption, the holder of the stablecoin receives a variable amount on ETH according to its price in USD. Because no actual USD is involved in the deployment of the coin, the target is only a number; one that scales up or down the amount of the reserve asset that is redeemed. Thus price targets for indirectly backed stablecoins are more versatile than directly backed: targets not only include assets that can be held, but any synthetic price, even if the price does not represent a real asset. For example, an indirectly-backed stablecoin could target a currency index which measures the value of a currency relative to a basket of other currencies, or the purchasing power of the currency, or the issuing country's GDP. If it uses an asset as the price target, like any derivative, the value of all issued indirectly-backed stablecoins can exceed the total value of the asset being targeted (however it cannot exceed the total value of the asset held in reserve).

For intervention-based stablecoins, there is no reserve asset. While we always illustrated the price target as the price of the stablecoin in USD, the target can be anything that can be determined, whether it is a number or an event. Thus these coins offer the most flexibility. For example, intervention could be decided on the level of inflation or a particular interest rate. The importance of this that these coins can be truly independent of any other currency. Backed (directly and indirectly) stablecoins require the reserve asset and cannot continue to

function if the reserve asset disappears or becomes worthless. Hypothetically, if an intervention-based stablecoin could target on-blockchain events (thus not requiring an oracle) and demonstrate reliable price corrections to under and overvalued coins, it would represent the best possible stablecoin along all the properties we use in our evaluation.

B.2   Why are there so many?

Stablecoins can choose from a variety of price targets, reserve assets, and blockchain platforms to deploy on. This by itself results in a large number of projects. Additionally, how contracts are set-up, what the governance over the system looks like, to what extent the system can change, how compliant the coin aims to be with regulations, and other design decisions differentiate the projects.

B.3   Why aren't stablecoins perfectly stable?

A stablecoin that the USD will still experience some volatility. If it trades above or below 1 USD, there are three basic explanations to consider. First, is there a mechanism to correct the under/overvaluation? If not, there is no guarantee of stability. If there is, how much friction is there in using the mechanism? For example, if offers are below 1 USD, can the coins be purchased and redeemed at all, and if so, what are the fees and time delays associated with redemption? The more friction there is, the higher the volatility.

This is seen in other financial instruments as well. Consider two contrasting examples: a typical ETF and a typical trust fund. An electronically traded fund (ETF) will typically sell shares of a portfolio of assets, be redeemable for the assets on-demand, and will be priced closely (±1%) to the value of its underlying assets—it is most like a directly backed and redeemable stablecoin. A simplification of a (close-ended) trust fund is as follows: a firm will set up a special corporation to hold the assets, the tokens are not directly redeemable, however the tokens are ownership shares in the special corporation—by owning the corporation, you effectively own its assets. Such a fund will trade with greater deviation from the value of its assets (±5%).

A second explanation for volatility in a stablecoin is some catastrophic failure in the coin; for example, around its security. If coins or their direct/indirect reserves are stolen or the coin issuing process is hijacked, a collapse in price could occur. Technically this is a special case of the first explanation—a hack of the coin makes redemption (the primary undervalue correction mechanism) impossible.

The final explanation is also seen in all financial markets. Generally, traders of financial instruments must choose between executing trades at a good price and executing trades fast. Depending on the circumstances for why they are trading, they might prioritize price over time, or time over price.

Consider a USD-backed and redeemable stablecoin where coins can be issued and redeemed with minimal friction. A good price for such a coin is 1 USD (with some variance, perhaps similar to the ±1% band of an ETF). However if traders want to quickly buy or sell the stablecoin, they might forgo obtaining a good price for fast execution of their trades. One of the quickest to execute trades that are possible with a stablecoin is an exchange for another cryptocurrency, such as Bitcoin (and vice versa). If traders want to buy/sell BTC quickly and prices are not ideal (*i.e.,* close to 1 USD), the time-sensitive traders may prioritize time over price and execute the trade anyways. Meanwhile, price-sensitive traders will avoid the poorly priced stablecoin and trade BTC and actual USD, even though this involves more risk and time to actually withdrawal the USD. The result is greater volatility in the stablecoin's exchange rate with the USD, at least temporarily. Once the time-sensitive trading subsides, price-sensitive traders drive the price back to stability.

B.4   How do stablecoins compare to governmental currencies?

We show a connected scatter plot in Figure 4 that shows two cryptocurrencies, ETH and XRP (from Ripple) plotted against two reference currencies: the USD on the x-axis as a currency with government-managed stability,
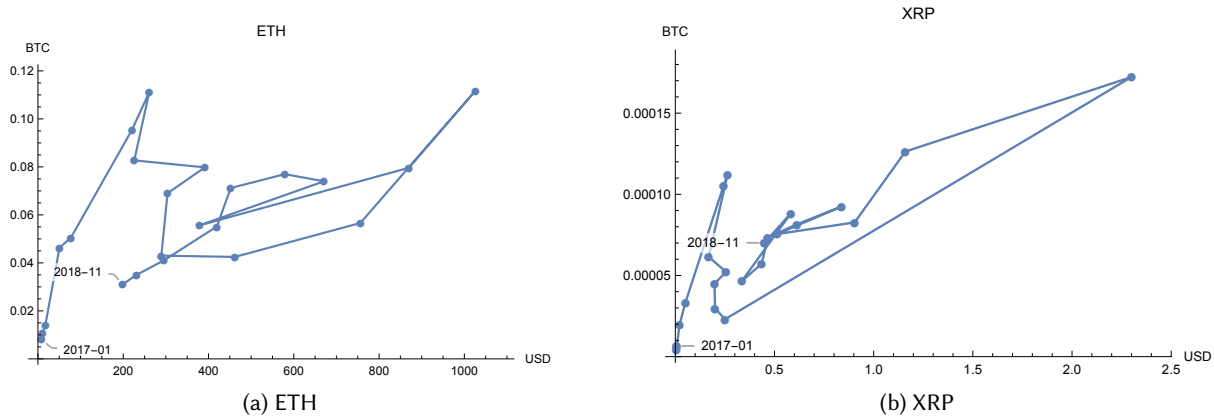
Fig. 4. Volatility in cryptocurrencies

and Bitcoin which has no stability mechanism. Like Bitcoin, neither ETH nor XRP have a stability mechanism. The reader might anticipate one of two things: either (i) they move independently from the reference currencies (diagonal movements along the 2/6 direction) or (ii) they move in a way that is correlated to Bitcoin (3/7 movements) because the market prices all cryptocurrencies like a sector. From Figure 4, it is fairly apparent that (i) is correct. The graph displays XRP's strong price surge in December 2017.

Next we plot a number of stablecoins in Figure 5. The top two plots are governmental currencies, the Canadian dollar and the Euro, which have no formal relationship to the USD but are managed by their central banks using similar policies and have intertwined economies. The bottom two currencies are two stablecoins, Tether (directly backed with USD) and BitUSD (indirectly backed with USD). All four currencies exhibit movements in 1/5 direction which indicate that most price movements are due to Bitcoin's volatility and not the volatility of either the plotted currency or USD. Note also that the spread of the x-axis is consistent across all four plots to allow cross-comparison. Both Tether and BitUSD exhibit some volatility. When Tether breaks from its stability with the USD, it moves in diagonal movements that are not correlated with either Bitcoin or USD. When BitUSD loses its stability relative to the USD, it moves in a horizontal 3/7 direction which is correlated with BTC.

B.5 Oracles everywhere

A number of stablecoin proposals feature oracles which feed information about the stablecoin's exchange rate onto the blockchain. This is essential for indirectly-backed stablecoins, and incidental to intervention-based coins. This raises an important design question. One use of a stablecoin is as a unit of account (recall the function of money in Section A.5)—so that a digital (or material) good or service can be effectively priced in, say, USD instead of in ETH. To be clear, it is priced in the stablecoin, which maintains a stable exchange rate with USD. To accomplish this, an oracle provides a reliable exchange rate and somewhat elaborates contracts issue stablecoins with an unusual risk profile (*e.g.,* full redemption might not be possible under certain market conditions) that could be difficult for non-experts to understand.

Let us take a step back and think about the larger picture. If we have trustworthy oracles providing reliable exchange rates, is it not a simpler design to just have transacting parties use the oracle directly? Anyone wanting to do business in a stable currency can determine at transaction time how much their good or service, priced in USD, is in ETH and charge the correct amount in ETH (which can then be immediately liquidated for USD, if
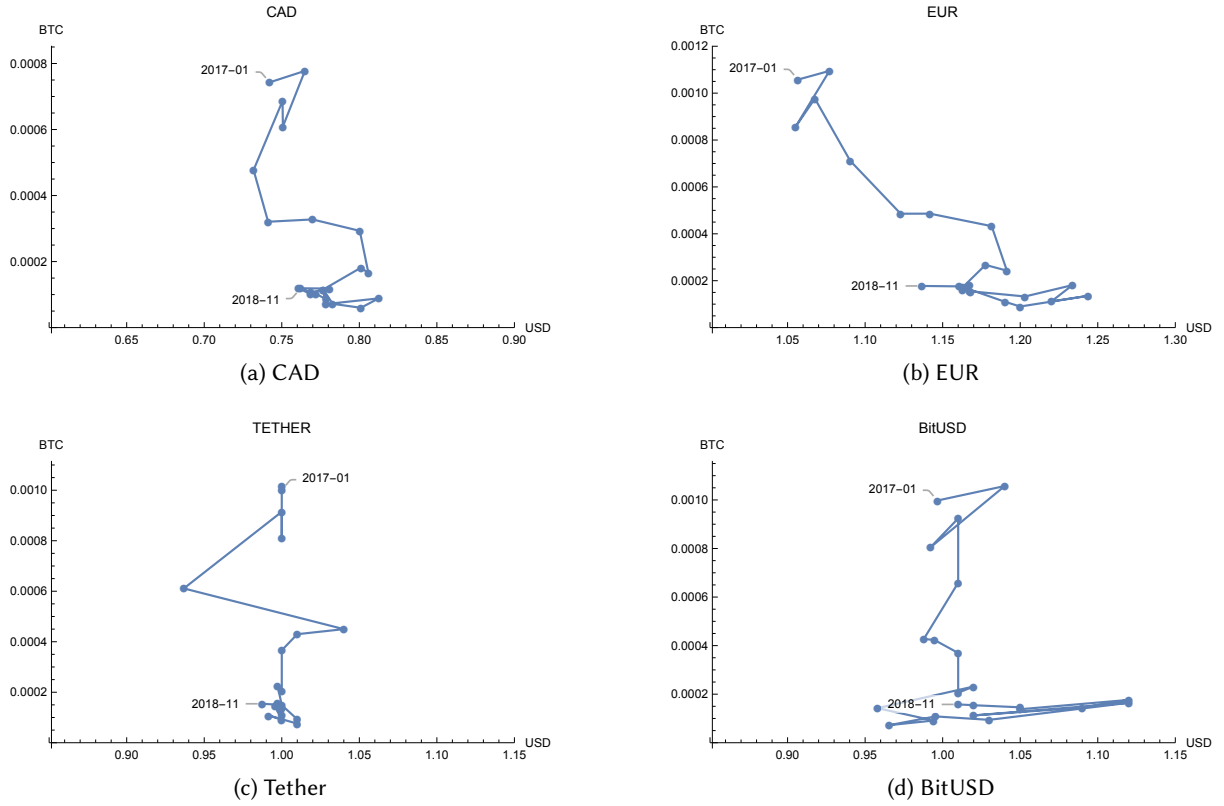
Fig. 5. Stability in two government-issued fiat currencies (CAD and EUR) and two stablecoin projects (Tether and BitUSD). Note that the x-axis is sized consistently across all four plots, with a $0.30 USD spread.

desired). In summary, the oracle assumption that underlies many stablecoins is itself sufficient to side-step the need for stablecoins. This is applicable to lending as well: loans, interest rates, and repayment amounts can be denominated in USD but paid in ETH using a spot conversion via an oracle.

The one remaining issue is that oracle-denominated transaction do not offer a stable store of value. So if Alice is paid in ETH at a rate set in USD, an oracle is sufficient. However if the value of ETH relative to USD changes before she does something with her ETH, she gains/loses. Alternatively if she was paid in a USD-targeting stablecoin, she can leave her pay untouched indefinetely without it gaining/losing value relative to the USD. Thus oracles alone provide a unit of account, while stablecoins provide both a unit of account and a store of value.

B.6 Is Ethereum's gas a stable 'coin'?

DApps on Ethereum execute arbitrary code provided by the owner of the DApp. While this code might be written in a high-level programming language like Solidity, it is compiled to a compact representation (called 'bytecode') that is a set of low-level instructions to the environment (Ethereum virtual machine or EVM). Because different functions will have different complexities, the user running the function pays in proportion to the number of instructions, the complexity of the instructions, and the storage requirements. This means that each operation

(a) Ethereum gas with respect to ETH and USD.

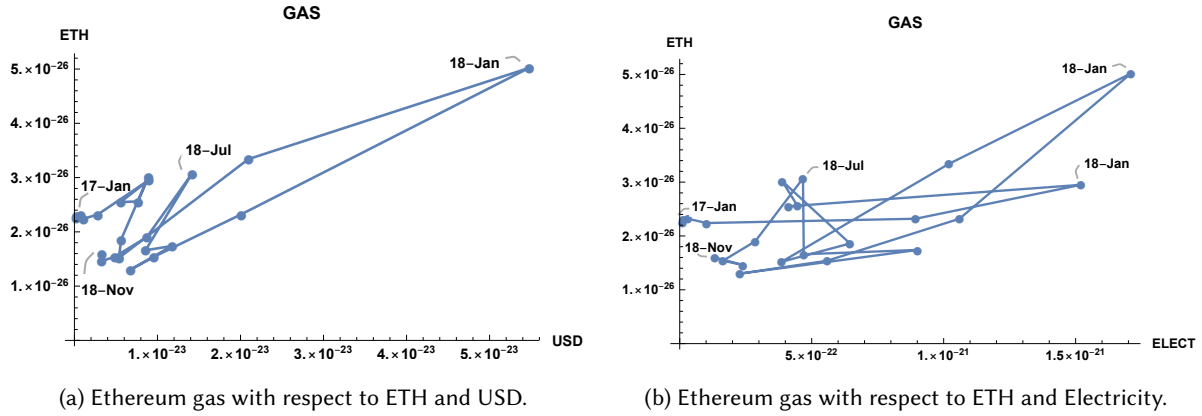(b) Ethereum gas with respect to ETH and Electricity.

Fig. 6. Ethereum average gas price variations with respect to Ether, USD, and Electricity. As mentioned in the Section B.6, the drastic movements in the charts represent specific events. Data is from January 2017 to November 2018.

has a fixed price. Naturally the operations might be priced in ETH, since it is the on-board currency, however this would cause the price of computation to be as volatile as Ether itself. Instead, Ethereum uses a pseudo-currency called gas.[5] Each instruction has a fixed price in gas. A user who wants to run a function will offer to pay a certain amount of ETH per unit of gas to the miner who finalizes the function. Miners will generally choose which functions to run first based on how much ETH/gas they offer, and they might ignore functions that offer too little ETH/gas. We describe gas as a pseudo-currency because it cannot be directly stored or transacted, however we will revisit this below.

Gas was envisioned as maintaining a relatively stable value where a particular function should cost the same amount (say in USD) over time, even as the price of ETH changes dramatically (as seen in Figure 4a). We first investigate how successful gas has been with the charts in Figure 6, which show the monthly average gas price variations with respect to USD and ETH in the first chart; and electricity and USD in the other. Electricity data is from a Canada-based average index which does not necessarily reflect the costs of mining on a global blockchain, like Ethereum, but if gas were correlated to electricity generally, it should be evident from a representative energy index. Gas demonstrates diagonal movements along the 2/6 direction meaning that it actually moves independently of ETH, USD and electricity. There is no strong evidence of stability. This could be due to a few factors. First, the graph is dominated by one large spike and one moderate spike which correspond to (i) when the popular Ethereum game Cryptokitties [6] was first launched (January 2018) and, (ii) when the China-based crypto exchange FCOIN [7] was launched (July 2018) and required a lot of on-chain voting. Both these events clogged up the Ethereum network and increased the gas price as users had to pay more gas for their transactions to go through. Second, it is probably true that users do not have a strong mental model of how much gas to stake for a computation and rely heavily on the user interface for prompts about gas.

Although gas might become a stable unit of account, it is not a store of value because it cannot be held or transacted. However gas could be used to back a stablecoin, much like the coins in the directly-backed category. Amazingly, such a gas-backed coin could even be made redeemable. Ethereum is designed in such a way that it allows users to create a smart contract which stockpiles and swaps gas with other tokens. Operations that store

---

[5]http://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html#what-is-gas
[6]Cryptokitties website https://www.cryptokitties.co/
[7]Fcoin website https://www.fcoin.com

data on Ethereum blockchain modify its global state hence they are very expensive. So in order to incentivize users to free up space on the blockchain, Ethereum refunds the amount of gas users paid if they delete their smart contracts or stored data [14]. GasToken is a directly-backed and redeemable tokenization of gas.[8] When the gas price is low (*e.g.,* 1 Gwei), users can store some data on the GasToken contract and create GasTokens. Later when the gas price increases (*e.g.,* 50 Gwei), users can redeem their GasTokens. However they do not receive ETH back; rather, they use the tokens to pay the transaction fees for other computations.

As users' mental model of gas improves over time, the volatility of gas has the potential to reduce. Gas-backed tokens represent a new class of stablecoin that float in value without any direct ties to USD, references to exchange rates, or explicit intervention mechanisms. It is an interesting subject worthy of further research.

---

[8]https://github.com/projectchicago/gastoken

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/Raymond Chabot Grant Thornton/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, and blockchain applications. She is currently working on realizing secure function evaluation using blockchain and is an intern at the 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.