Demystifying Stablecoins

Abstract

TBD Bitcoin is volatile. People do not like this feature Bitcoin. People therefore try to tweak Bitcoin to make a less volatile version. Or they try to bring less volatile currencies onto Bitcoin or other blockchain systems. This paper is essentially a survey of work on stablecoins but we aim at making a number of subtle research contributions to ensure this survey is actually useful to the reader. First and foremost, we are very selective in the concepts from finance we bring into the survey and explain each from first principles, while attempting to minimize or eliminate jargon. We distill proposals done to their fundamental primitives and describe these concepts rather than enumerating the intricate details of how particular 'brands' of stablecoins work?details that could change tomorrow (that said, we do provide, as the reader probably expects, a chart mapping brands into our categorization). Additionally, we also consider the question and potential for the stability of index-cryptocurrencies (namely gas which is used in Ethereum), which are very pertinent to a discussion of stablecoins, yet not typically addressed. Last, we offer some novel visualizations of exchange rates we have not seen before.

1 Introduction

Many early cryptocurrency proposals designed secure digital representations of government-issued money (which cryptocurrency enthusiasts typically call 'fiat'). While Bitcoin was not the first proposal for a digital currency that is issued and operates independently of existing currencies and financial infrastructure, Bitcoin [10] is the first of this type to establish wide-scale deployment. Without government oversight, the exchange rate of Bitcoin is essentially subject to: (a) an algorithm which releases new BTC (Bitcoin's currency) on a fixed schedule, and (b) the market for exchanging Bitcoin for other things of value, namely fiat currencies such as the USD, and potentially (c) the market for participating in transaction validation which is integral into how new BTC comes into circulation.

From the inception of exchanges for buying and selling BTC for USD in 2010 to the time of writing, the exchange rate of BTC with the USD has been marked by extremely volatile with large fluctuations in its value that are atypical of a government-managed currency. Figure 1 illustrates this volatility by plotting the exchange rate of BTC (with the USD) alongside the same exchange rate for three economic zones—Europe, UK, and Canada—which all appear relatively stable. Note that Figure 1 deliberately includes the UK's referendum on exiting the EU ('Brexit') in June 2016, which was followed by a 'sharp decline' and 'volatility' in GBP's exchange rate.[1] Relative to BTC however, this 'severe swing' looks like a mild pinch of GBP's exchange rate with EUR in Figure 1.

In response to Bitcoin's extreme volatility, a flood of proposals have been made for alternative designs that would offer a more stable exchange rate (called 'stablecoins') between such a proposed stablecoin and a government-issued currency like the USD. Broadly, the proposals can be split into two categories: ones that essentially create a digital representation of a fiat currency that can be transacted like a cryptocurrency, and ones that propose separate currencies with some mechanism for stability and/or intervention built into the design.

Contributions. This paper is essentially a survey of work on stablecoins but we aim at making a number of subtle research contributions to ensure this survey is useful to the reader. First and foremost, we are very

[1] Descriptions from the following *BBC* articles: "The markets facing trading turmoil" (27 Jun 2016) and "How does Brexit affect the pound?" (15 Jan 2019).

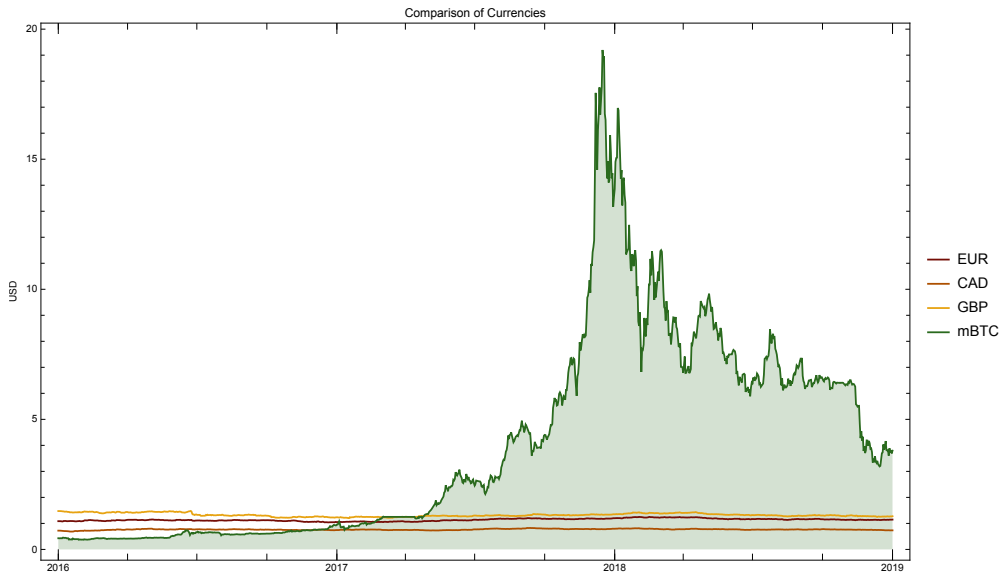


Figure 1: Comparison among fiat currencies and Bitcoin: The values are retrieved daily between 01 Jan 2016 and 01 Jan 2019. Note that 1000 mBTC = 1 BTC.

selective in the concepts from finance we bring into the survey and explain each from first principles, while attempting to minimize or eliminate jargon. Next we distill stablecoin proposals down to a set of fundamental primitives and describe how these concepts work, as opposed to enumerating the intricate details of how a particular 'brand' of stablecoins works today—details that could change tomorrow. We do provide, as the reader probably expects, a chart mapping existing stablecoin brands into our categorization. Additionally, we also consider the question and potential for the stability of index-cryptocurrencies (namely gas which is used in Ethereum), which are very pertinent to a discussion of stablecoins, yet not typically addressed. Last, we offer a novel visualization style for exchange rates we have not seen before used for exchange rates.

2 Related Work

An early idea for a stable cryptocurrency was introduced by Ametrano in 2016 [2] which tweaked supply (see Section 6.3) In 2017, Robert Sams introduced a new dual token system that uses two coins to achieve price stability: (i) a stablecoin (*e.g.,* fiat currency) and (ii) a volatile coin (*e.g.,* equity shares) [15] (see Section 6.3). These informed the designs of stablecoins we discuss in the paper.

There are many blog posts and professional reports providing an overview of stablecoins with essentially the same goal as this paper. Most have the same general categorization: (i) fiat-collateralized, (ii) crypto-collateralized and (iii) non-collateralized, also known as algorithmic,*e.g.,* [7, 13, 17]. Buterin, in one of the earliest blog posts on stable cryptocurrencies, discussed different techniques to measure cryptocurrencies' price and how to make adjustments in the supply to achieve a fixed price accordingly [6]. Bitmex looked at the mechanics of the distributed stablecoins while focusing on two case studies (*i.e.,* BitShares (BitUSD) and MakerDAO (Dai)) [3]. Another report by crypto company Blockchain provides an extensive classification of 57 stablecoins together with discussions on issues related to governance (*e.g.,* legal structure, investors, partners *etc.*) [4]. They extend this research in a newly published report that reflects a significant update on their previous work [5]. In one of its blog posts, Consensys [2] describes stablecoins as "crypto-assets that maintain a stable value against a target price (*e.g.,* USD)" and classify them according to three main

[2]https://consensys.net

categories [16]. In [11], the authors use a slightly different categorization to group 13 stabelcoin projects into two broad categories: (i) centralized– which itself contains subcategories based on the type of the asset the coins are backed by (*e.g.,* fiat and gold), (ii) decentralized. Our survey can be differentiated from the related work in its focus: we strive for clear descriptions of the mechanics of stability within a coin, without glossing over details or substituting financial jargon for explanation. We focus less on any infrastructure around a stablecoin deployment (*e.g.,* it's code, interactions between contracts, governance, *etc.*).

3 Preliminaries

3.1 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[3]) 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).

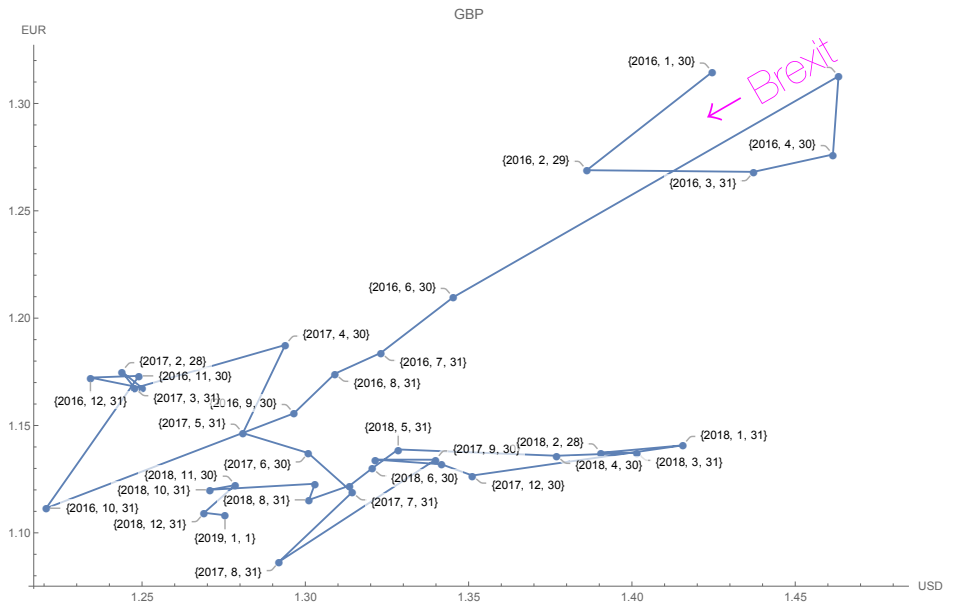
3.2 Exchange Rates

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.

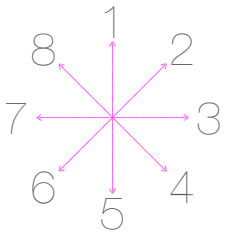
To determine which currency is moving, one might consider a third or forth currencies (*cf.* US Dollar Index) to try and triangulate if BTC is moving in price, or USD is moving in price, or both. For example, in Figure 1 it certainly appears that BTC is the currency that is moving because the rest of 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 2a. 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) forms a coordinate. For the last day of each month, a new coordinate is added and joined with a line from the previous value.

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



(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).

Figure 2: 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.

This is inspired by similar charts on the website FiveThiryEight for things like kicking distance in football[4] and they have been called connected scatter plots.

Lines in a connected scatter plot can move in any direction. Figure 2b 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 a single currency moving rather than an explanation that involves a pair of currencies moving in tandem. For example, in Figure 2a, 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. [5]

We will return to these charts later in Section 6.3 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.

[4] "The 52 Best—And Weirdest—Charts We Made In 2016," *FiveThirtyEight*, 30 Dec 2016.
[5] https://github.com/ Removed for anonymity.

3.3 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 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, which 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.

3.4 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 [9]. 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 [9]. 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.

3.5 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 it should fulfill for its 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. [14]

3.6 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. [12]"

4 Type 1: Backed Stablecoins

In this section, we discuss the first type of stablecoin. These coins try to directly match the stability of a second asset, such as the USD. These coins could not exist without their target asset. In Section 5, we consider the second type of coin which is a standalone currency that use intervention (algorithmic and/or human) to reduce volatility.

In Table 1, we show the taxonomy we use to classify stablecoins. As mentioned earlier in related work (see Section 2), taxonomies for stablecoins have been proposed many times. The focus of our taxonomy is a bit different. We do not care about classification *per se*—we view our work as a tutorial on how to build a stablecoin, and the taxonomy are simply is a set of directions a designer can choose between or combine. They are based on proposals for stablecons, as well as insights from monetary policy for governmental currencies.

To find stablecoin projects, we performed a number of search queries on *CoinDesk*, an online news source for cryptocurrencies and blockchain technology.[6] Our search terms included "stablecoins," "stability," and "price-stable." We read 185 articles up to January 11, 2019 and extracted the names of projects. 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. Finally, within each category, we sort projects according to their rank on *CoinMarketCap* which ranks cryptocurrencies that are actively traded on an exchange service.[7] Unlisted projects are ranked $\perp$.

[6] https://www.coindesk.com/
[7] https://coinmarketcap.com

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
		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 corrosponds to *CoinMarketCap*.

4.1 Directly-Backed and Redeemable

The first direction one might take in producing a stablecoin is the creation of a digital representation (or tokenization) of a fiat currency, commodity, or portfolio of assets. Tokens are designed to have the same price (and thus volatility) as the underlying portfolio. To further enable an equivalence of value (we will explain how shortly), the digital token can be redeemed on-demand for the underlying asset. For simplicity, we will consider a cryptocurrency designed to digitally represent the USD.

The idea of tokenizing USD (or EUR or gold) for use on the internet is not new. Liberty Reserve and e-gold provided a similar service. Liberty Reserve dollars were redeemable in principle, but only indirectly through an intermediary and redemption could be refused. Meanwhile, e-gold was not redeemable (see next section of a discussion of the consequences of this). What is novel about a stable cryptocurrency is that transactions are not done on a centralized server, but rather finalized and settled on a decentralized blockchain. However since directly-backed stablecoins reintroduce centralization to create the digital tokens, maintain reserves of the underlying asset, and process redemption requests, the benefit of a decentralized transaction platform is marginal.

Process. Alice is a trusted third party and uses Ethereum to generate a contract to issue 1000 AliceCoins as standard (*e.g.,* ERC20) tokens. She lists asks $1 USD for 1 AliceCoin and promises to redeem the tokens 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 request for AliceCoins but does not have any left to sell, she creates new ones and deposits the payment. If Carol wants to redeem 5 AliceCoins, Alice withdraws $5 USD and exchanges it with Carol and takes the AliceCoins out of circulation. Alice frequently obtains bank statements showing that her account holds USD equivalent to the number of coins in circulation (the number of AliceCoins can

be checked anytime on Ethereum).

Price Stability. For simplicity, assume all transactions are free and frictionless. Consider a bid for 1 AliceCoin that is greater than $1 USD. Bob will sell an AliceCoin immediately for this price and will ask Alice to generate a new AliceCoin, deposit only $1 USD for this, and keep the rest of the bid value as profit. Therefore bids in excess of $1 USD will be temporal assuming Alice is quick to generate new coins on demand. Next, consider an ask for 1 AliceCoin for less than $1 USD. Bob will immediately purchase this AliceCoin for its asking price, try to redeem it for $1 USD from Alice, and if successful, keep the difference as profit. Bob's willingness is proportional to the expectation that it can actually be redeemed for $1 USD. For an example, if he only buys at $ 0.60 USD, it might reveal that Bob believes there is only a 60% chance of redeeming the coin or that he can only redeem 60% of its redemption value (the asker thinks it must be less, otherwise she'd rather redeem it than sell it).

Conclusion: the bid-ask spread will saddle $1 USD and trades should execute close to $1 USD assuming the market is close to 100% confident in a frictionless creation and redemption process for of coins. In reality, fees and time delays for moving stablecoins and fiat payments will cause distortions.

Discussion. Blockchain-based cryptocurrencies are designed to minimize trust in third parties. The trust assumption on stablecoins in this category are close to pre-blockchain currencies like Liberty Reserve and e-gold, who would maintain transaction details and account balances on a private server. Blockchain enables decentralized trust for the transactions, although it also makes them transparent—at least, as transparent as token movements are for the underlying contract and/or blockchain. This includes transactions with other decentralized applications. However the coin creation and redemption processes rely on trust.

A financial audit is an important step than can establish confidence in the redemption process, which in turns provides stable prices on coins being offered for sale. The auditor becomes a further trusted entity, and ties its reputation to the firm operating the stablecoin. For regulatory reasons, reputable auditing firms will want a clear indication of the coin's legality, as well as confidence in the firm's internal controls over the issuance and redemption of tokens and the custodianship of the backing assets. A sensible template for a stablecoins of this type will consist of three trusted entities: the firm operating the coin, a reputable auditor, and a reputable custodian of the assets.

If the firm operates in a jurisdiction with modern securities laws, the issuance of the stablecoins is likely subject to regulatory approval. Further, the redemption of the coins will serve as a main point of regulation, requiring financial reporting to prevent the kind of crime that was prevalent on pre-blockchain coins like Liberty Reserve and e-gold. A number of existing coins with operations in the United States have been reported as disallowing redemption for some holders.

A variety of firms and projects providing stablecoins in this category exist. Why so many? 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.*) [1]; and (3) the degree of regulatory compliance: paving forward in a highly regulated environment to bootstrap trust, or seeking under-regulated environments to move to market quickly and avoid government surveillance for participants.

4.2 Directly-Backed

Next we consider stablecoins that are directly-backed—exactly as in the previous section but they do not offer a redemption process for the coin's underlying assets. Redemption is logistically complicated. Consider a USD-backed dollar—it is usually easier for a firm to receive USD payments from users than it is for it to send payments back, and sending payments opens up new exposure to regulation. Instead the firms behind these coins pledge to keep the backing assets in trust for the duration of the circulating coins. We will shortly explain what impact there is on the exchange rate if it does not provide redemption—obviously, if redemption was inconsequential than no one would offer it as it increases costs and complexity. For our

ranking in Table 1, if we could not find a clear assertion of redemption, we listed the project under this category.

Process. As previously, Alice is a trusted third party and uses Ethereum to generate a contract to issue 1000 AliceCoins as ERC20 tokens. She asks $1 USD for 1 AliceCoin and promises to deposit the payment. If Bob buys 10 AliceCoins for $10 USD, Alice deposits the $10 USD in a bank account. Any time Alice receives a request for AliceCoins but does not have any left to sell, she creates new ones and deposits the payment. Alice frequently obtains bank statements showing that her account holds USD equivalent to the number of coins in circulation (the number of AliceCoins can be checked anytime on Ethereum).

Price Stability. Again, assume all transactions are free and frictionless. Bids will not exceed $1 for the same reason the coins in the previous section (Section 4.1). Consider an ask for 1 AliceCoin for less than $1 USD. Bob will only immediately purchase this AliceCoin for its asking price if he has some assurance it will return to $1 USD. Because it is not redeemable, the only mechanism that will push the value up is psychological: others in the market will ask $1 USD because they believe it is valued at $ USD because it is backed by $1 USD.

Conclusion: bids will not exceed $1 USD but the best ask could vary from $0 USD to $1 USD without being immediately traded.

Discussion. The idea of tokenizing assets and re-selling them in a useful format (*e.g.,* as a portfolio or in a way that is digitally compliant with standard trading software and automated accounting systems) is commonplace for standard financial assets, however most tokenizations of this type have some direct or indirect redeemable value. 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 ($\pm 1\%$) to the value of its underlying assets—it is most like the stablecoins in Section 4.1. 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 ($\pm 5\%$).

A coin that has no redemption, direct or indirect, will not clearly trade for a particular amount. An informal argument in favour of it being stable is that minting the coin is costly—it requires obtaining USD to hold in reserve. This feature serves an important function, albeit a different one. This bounds the firm from over-issuing tokens, which would cause the coin to loose value, however it does not ensure asks do not drop below $1 USD.

The difference between the market value of a newly minted coin and the cost to produce it is called seignorage. A backed stablecoin has no seignorage: it sells for $1 USD and requires holding $1 USD to 'produce' it. There appears to be a folk theorem that if minting asset X requires consuming asset Y, asset X will take on the value of asset Y (otherwise, who would produce X?). In reality, resources can be consumed to produce something of no value—that value is simply lost. A canvas that has been applied with acrylic paint might cost $100 USD in raw materials; its value could none-the-less be much less than $100 USD. . . or much more.

Even if the market does not accept the psychology that a coin backed by $1 USD should be priced at $1 USD, it is still important to establish that the coin is actually backed as a guard against over-issuance. As in the previous section, holders of the coin will want assurance that the custodianship of the backing asset is sound. A financial audit by reputable firm is one method to provide this assurance. Recap: Is bitcoin really un-tethered?.

4.3 Indirectly-Backed

The previous two sections describe coins that require a trusted firm to hold assets. The difference between these coins and traditional digital currencies like Liberty Reserve and e-gold is marginal—it is only that

transactions are now decentralized. By contrasts, coins in this class prioritize decentralization and offer stablecoins that are issued, transacted, and redeemed in an autonomous fashion, while still being redeemable for USD. However these requirements are in conflict as there are no USD on a blockchain like Ethereum.

Coins in this section try to find a middle-ground. They introduce a single trusted element: an exchange rate of the underlying (non-stable) cryptocurrency on the blockchain (*e.g.,* ether) and a stable fiat currency (*e.g.,* USD). Since the blockchain has no inherent knowledge of the USD/ETH exchange rate, the rate is stored and periodically updated by a trusted entity called an oracle (the consensus of multiple oracles can also be referenced), and such a service could have useful applications beyond stablecoins.

Tokens then created when the equivalent of $1 USD in ETH is collected, and redeemable for the equivalent of $1 USD in ETH. Thus the amount of redeemable ETH can grow or shrink as the exchange rate with the USD changes. If it shrinks, the contract that issued the coin holds the difference and returns it to creator of the coin. If it grows, it is problematic because the contract cannot hold an unbounded amount of ETH. Thus the contract collects more than $1 USD (say $1.5 USD) when it mints a new coin to provide a buffer against falling ETH prices.

Process. Alice sets up a DApp that can hold ETH and issue ERC20 tokens called AliceCoins. The DApp determines how much ETH is equivalent to $1.50 USD using the current exchange rate, provided to the DApp by a trusted oracle. Alice deposits this amount into the DApp and it issues 1 AliceCoin to Alice. Bob purchases 1 AliceCoin from Alice for $1 USD. Bob transfer the AliceCoin to Carol and Carol returns to the DApp to redeem the coin. The DApp determines how much amount ETH is equivalent to $1 USD (call this the strike price). If the deposit of ETH in the DApp is greater than the strike price, the DApp pays Carol the strike price and it returns the remainder of the deposited ETH to Alice. If the strike price is less than or equal to the deposit, Carol is paid the entire deposit and Alice is paid nothing (she does however have $1 USD from Bob). In this scenario, Carol may not recover a full $1 USD and therefore is incentivized to monitor the deposit value, and redeem quickly if the deposit value in USD drops close to the face value of her AliceCoins.

Price Stability. Consider a bid for 1 AliceCoin that is greater than $1 USD. Bob will sell an AliceCoin immediately for this price and will ask Alice to generate a new AliceCoin, pay her only $1 USD for this, and keep the rest of the bid value as profit. (More generally, Bob could issue a BobCoin assuming the bid is for any coin backed by this type of contract). Therefore bids in excess of $1 USD will be fulfilled as long as there are individuals willing to lock up a deposit of ETH that is 1.5x the face-value of what they receive. If there is a shortage of ETH for this purpose, AliceCoins might trade in excess of $1 USD. It is important to note if Alice underwrites one of these contracts, retains the USD she sells the AliceCoin for, and the ETH/USD exchange rate changes, she will make or lose exactly the same amount of money as she would by simply holding the same amount of ETH she deposited. The exception is if the contract's deposit becomes worth less than the amount that can be redeemed from it — in this case, Alice loses less money by underwriting the contract (the holder of the coin bears the loss) than if she held ETH.

Next, consider an ask for 1 AliceCoin less than $1 USD. If the contract backing the coin has an ETH deposit valued at the bid price or more, Bob will immediately purchase the AliceCoin, redeem it for $1 USD, and keep the difference as profit. If the contract's deposit is worth less than the bid price, the ask will not necessarily be filled. Therefore AliceCoins will trade for less $1 USD when contracts have insufficient deposits, as might happen following a fast deterioration in the value of ETH relative to USD.

Conclusion: Indirectly-backed coins will fulfill bids greater than $1 USD assuming there is a willingness for ETH holders to lock up their ETH. Asks less than $1 USD for an indirectly-backed coin will also be quickly fulfilled when the exchange rate of ETH is favourable (by any amount) or when it decreases by a moderate amount. Asks less than $1 USD will persist if ETH decreases substantially.

Discussion. In standard finance, brokerages will lend money to investors but are concerned about getting it back in the case that the investors lose their borrowed money. They generally will require a deposit from the investor, monitor the investor's profits and losses, and liquidate the investor's position if their losses

approach the deposited amount (or ask the investor to deposit more). This is premised on the assumption that prices do not fall too quickly to react and that the position can be sold quickly at a good price. Therefore it is a precedented premise that an indirectly-backed stablecoin can be redeemed quickly before the deposit is worth less than the coins, however ETH may be far more volatile than other financial instruments.

There are many design decisions to consider when deploying an indirectly-backed stablecoin: the ratio by which the initial deposit exceeds the redemption value (*e.g.,* 1.5x), if coins can be redeemed any time, if a third-party can trigger a redemption (*e.g.,* for a fee) if they notice a deposit is close to losing more value than the face value of the coins (before the coin holder does), how close the deposit can get to losing value before such a trigger, and if all deposits backing all such coins should be pooled together, so all coins are interchangeable ('fungible'), or each coin is tied to a specific deposit. Note that while allowing third parties to trigger a redemption seems like a sensible service, if the coin holder is not monitoring the situation, they will end up holding ETH, instead of an AliceCoin, which is still losing value. This mechanism is really only about maintaining the reputation of the stablecoin.

5 Type 2: Intervention-based Stablecoins

The second main class of stablecoins are not backed by a separate asset, like the USD. Instead they allow for interventions that are meant to increase or decrease the value of the currency. Deciding when to intervene is the first design decision, and the decision central banks use. A modern central bank might look at how much one bank charges another bank, in interest, for a short-term loan.[8] In a cryptocurrency, none of this infrastructure exists: there are no banks, no central banks, no interest rates without lending, and no lending without a stable currency.

Instead, most stablecoin projects use the exchange rate with a fiat currency (*e.g.,* the USD) as input to the intervention mechanism. This makes these coins look more similar to coins that are backed by USD (in Section 5). This is good for cross-comparison in a paper like this, but the reader should bear in mind that any economic metric could be used instead with these coins, including ones not based on an exchange rate. Second, we remark that central banks in the past have used exchange rates to decide when to intervene, but this approach was not found inadequate for stablising an economy. Alternatives to the exchange rate might include interest rates (if lending markets emerge), purchasing power, or measurements on the amount, volume, and/or velocity of transactions. The challenge for these is ensuring the metrics cannot be easily manipulated in the blockchain environment, where single entities can created unlimited identities and wash transactions, trades, loans, *etc.* with themselves.

The second design decision is what intervention to make. All the stablecoin projects in this category make the same fundamental intervention: the supply of the stablecoin is increased to curb the value of the currency, and the supply is contracted to boost its value. The final design decision is how exactly the supply is manipulated. Some coins very directly influence the money supply, while other coins try to turn currency into assets to contract, and turn assets into currency to expand. This is obviously inspired by how modern central banks influence interest rates.[9] The final design decision is deciding who participates in these mechanisms.

In this section, 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.

[8]This value is readably available to the central bank, as these loans tend to be arranged daily by a payments system the bank maintains, and influencing this interest rate trickles out over time to other interest rates in the economy, and interest rates are seem as a force for influencing other metrics like the stability of the exchange rate, inflation, imports and exports, and the general health of the economy.

[9]Central banks will purchase assets, like government bonds, from banks at competitive prices to increase the bank's cash and lower the interest rate at which the bank will lend. Conversely, they will sell assets to the banks at competitive prices to remove cash from the banks, causing a greater demand for cash loans, which tends to increase inter-bank interest rates.

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

Table 2: 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 rank, and × indicates the property is not applicable.

5.1 Money Supply Adjustments

Intro

Process. Alice forks Bitcoin to create a new altcoin called AliceCoin. She sets Bitcoin's fixed schedule for releasing new Bitcoin as the default behaviour but allows this value (called the coinbase amount) to be tweaked according to the rules outlined below. She setups 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 (again, based on some mathematical 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.

Variant Process. Similar to above, Alice forks Bitcoin, preserves its coinbase schedule, and adds a trusted exchange rate oracle. When the price exceeds $1.02 USD, the coin increases the balance of every AliceCoin holder; when it dips below $0.98 USD, the coin decreases the balance of every AliceCoin holder.

Price Stability. Justification that bids will never exceed $1. Justification that offers will be less than $1. Conclusion: recap.

Discussion. Can actionally do this. No zero bound.

5.2 Asset Transfer

Process. Alice creates an ERC20 token called AliceCoin and setups up a trusted oracle for the latest exchange rate of AliceCoins to USD. A smart contract 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 contract creates new a set of AliceCoins (the size is determined by some mathematical relationship with how much the price exceeds $1.02 USD) 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 contract 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 contract and the contract destroys the payment. The place in line is a transferrable token. An additional transferrable token can be auctioned off which receives AliceCoins when the line is empty.

Price Stability.

Discussion.

6 Discussion Points

6.1 Summary of mechanisms

We have considered various issues with different mechanisms of designing a stablecoin (discussed in Sections 4 and 5) . We provide a summary of these results in Table 2 that evaluates each mechanism's core ideas and trust model. The columns and rows of the table are the evaluation criteria and mechanisms respectively. This framework provides a summary of the advantages and disadvantages of the different mechanisms for creating stablecoins.

6.2 Oracles everywhere

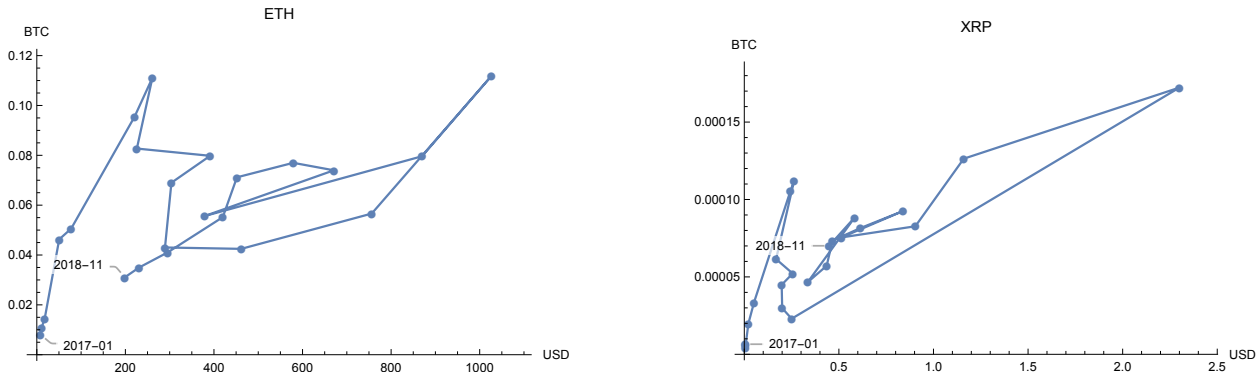
A number of stablecoin proposals feature oracles which feed information about the stablecoin's exchange rate onto the blockchain. This is essential for indirectly-backed stablecoins, and incidental to intervention-based coins. This raises an important design question. A stablecoin exists so that a digital (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 elaborate 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 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.

6.3 Visualizing stability

We show a connected scatter plot in Figure 3 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, 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 3, 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 4. 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



(a) ETH (b) XRP

Figure 3: Volatility in cryptocurrencies

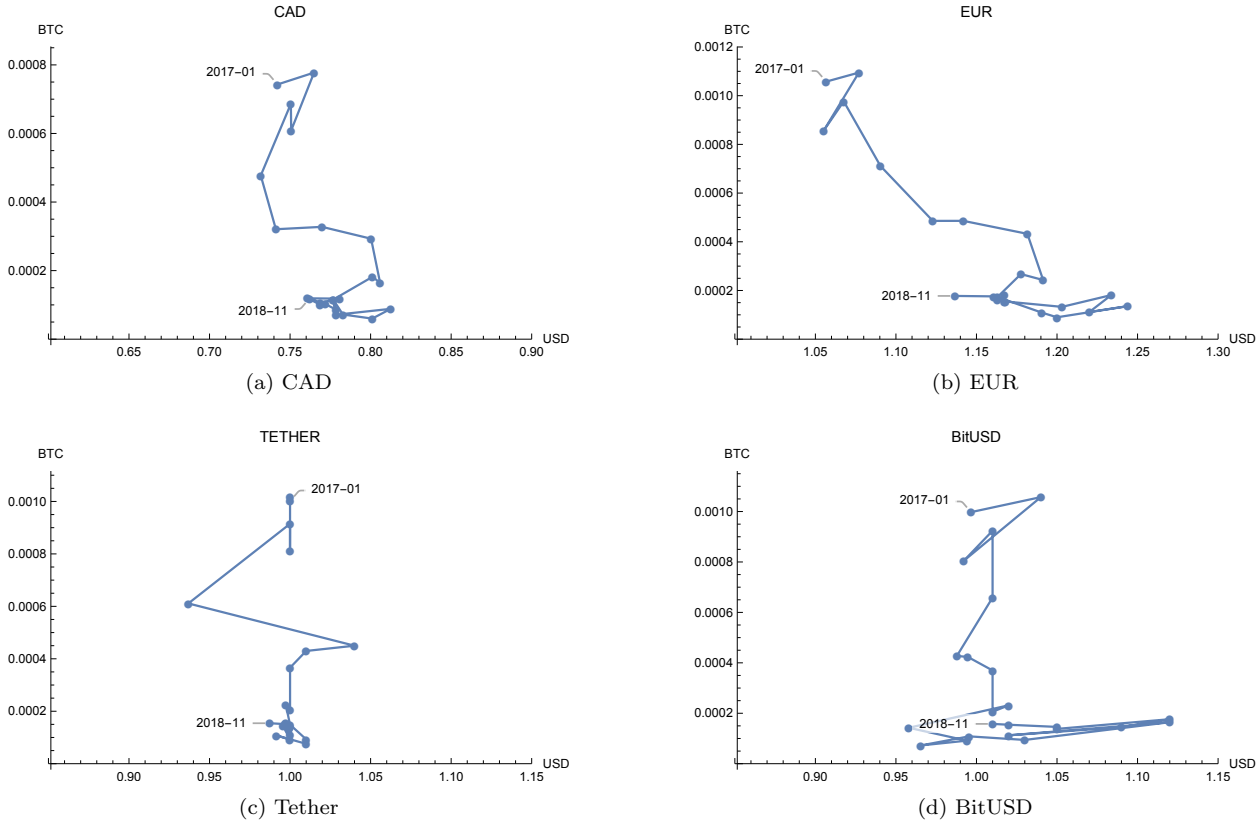
across all four plots to allow cross-comparison. Both Tether and BitUSD exhibit some volatility. When Tether breaks from its stability with the USD, it moves in diagonal movements that are not correlated with either Bitcoin or USD. When BitUSD loses its stability relative to the USD, it moves in a horizontal 3/7 direction which is correlated with BTC.

7 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 has a fixed price. Naturally the operations might be priced in ETH, since this 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.[10] Each instructions 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 3a). We first investigate how successful gas has been with the charts in Figure 5, 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 US-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 popuar Ethereum game Cryptokitties [11] was first launched (January 2018) and, (ii) when the China-based crypto exchange FCOIN [12] 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

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



(a) CAD (b) EUR

(c) Tether (d) BitUSD

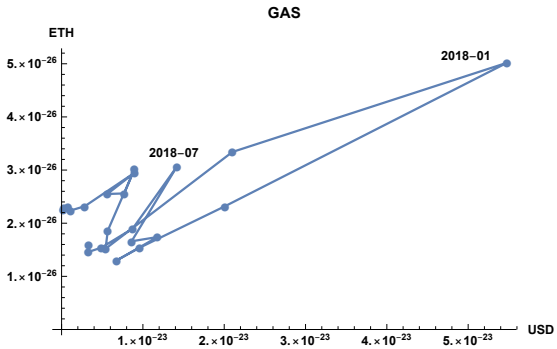
Figure 4: Stability in two government-issued fiat currencies (CAD and EUR) and two stablecoin projects (Tether and BitUSD). Note that the x-axis is sized consistently across all four plots, with a $0.30 USD spread.

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.

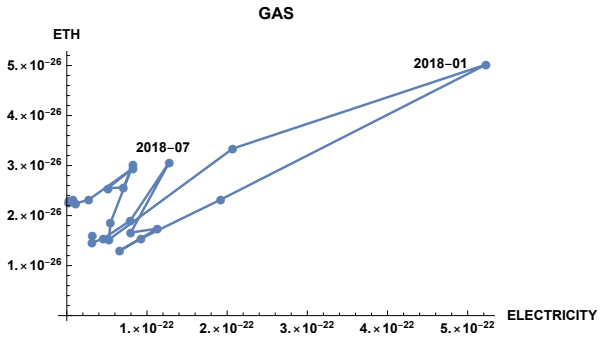
Although gas might become a stable unit of account, it is not a store of value because it cannot be held or transacted. However gas could be used to back a stablecoin, much like the coins in the directly-backed category. Amazingly, such a gas-backed coin could even be made redeemable.Ethereum is designed in such a way that it allows users to create a smart contract which stockpile and swaps gas with other tokens. Operations that store 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 [18].

GasToken is the directly-backed and redeemable tokenization of gas.[13] When the gas price is low (*e.g.,* 1 Gwei), users can store some data on the GasToken contract and create GasTokens, as mentioned, such transaction costs a lot of gas but it does not cost much in ETH or USD as the gas is cheap. Later when the gas price increases (*e.g.,* 50 Gwei), users can spend their GasTokens to pay for transactions. Thus, users benefit from paying for less gas and bidding for higher gasPrice in their transactions.

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



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



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

Figure 5: Ethereum average gas price variations with respect to Ether, USD, and Electricity. As mentioned in the Section 7, the drastic movement in the chart represents a specific event. Data is from January 2017 to November 2018.

8 Conclusion

In this paper, we provide a survey of active stablecoin projects. Unlike previous research studies performed on this topic, we selectively use the concepts from finance while eliminating the jargons. In addition, rather than focusing on the details of how particular 'brands' of stablecoins work, we thoroughly describe the fundamental mechanics and concepts to achieve price stability. Respectively, we show the taxonomy we use to classify stablecoins which represents the techniques to build a stablecoin. Additionally, we evaluate different price stability achieving mechanics based on their fundamental design decisions and trust models. The comparative evaluation framework highlights the advantages and disadvantages of each techniques more precisely. Eventually, we explore the potential stable index-cryptocurrencies (namely Ethereum gas) in the context of stablecoins.

References

[1] gemini-dollar-trailofbits-audit.pdf. `https://gemini.com/wp-content/themes/gemini/assets/img/dollar/gemini-dollar-trailofbits-audit.pdf`. (Accessed on 02/23/2019).

[2] F. M. Ametrano. Hayek money: The cryptocurrency price stability solution. 2016.

[3] Bitmex. A brief history of stablecoins (part 1). `https://blog.bitmex.com/a-brief-history-of-stablecoins-part-1/`, 2018. Accessed: 2018-09-02.

[4] Blockchain. The state of stablecoins. 2018.

[5] Blockchain. 2019 state of stablecoin. 2019.

[6] V. Buterin. The search for a stable cryptocurrency. `https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/`, November4 2014. (Accessed on 02/11/2019).

[7] S. Dhillon. Stablecoins vs. govtcoins: The race to solve cryptocurrencies price volatility problems. `https://www.linkedin.com/pulse/stablecoins-vs-govtcoins-race-solve-cryptocurrencies-price-dhillon`, 2018. Accessed: 2018-10-29.

[8] S. Eskandari, S. Moosavi, and J. Clark. Sok: Transparent dishonesty: front-running attacks on blockchain. In *International Conference on Financial Cryptography and Data Security*. Springer, 2019.

[9] L. Harris. *Trading and exchanges: Market microstructure for practitioners*. Oxford University Press, USA, 2003.

[10] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[11] C. O'Higgins. Stablecoins - everything you need to know. `https://cryptoinsider.21mil.com/stablecoins-everything-need-know/`, 2018. Accessed: 2018-07-09.

[12] M. C. Okoye and J. Clark. Toward cryptocurrency lending.

[13] H. Qureshi. Stablecoins: designing a price-stable cryptocurrency. `https://hackernoon.com/stablecoins-designing-a-price-stable-cryptocurrency-6bf24e2689e5`, 2018. Accessed: 2018-09-03.

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

[15] R. Sams. A note on cryptocurrency stabilisation: Seigniorage shares. *Brave New Coin*, pages 1–8, 2015.

[16] N. Sexer. State of stablecoins, 2018 consensys media. `https://media.consensys.net/the-state-of-stablecoins-2018-79ccb9988e63`, July24 2018. (Accessed on 02/12/2019).

[17] C. P. TEAM. Comprehensive overview of stablecoins. `https://medium.com/cp-processor/comprehensive-overview-of-stablecoins-819d183f6ac7`, 2018. Accessed: 2018-01-15.

[18] G. Wood. Ethereum yellow paper. *Internet: https://github. com/ethereum/yellowpaper,[Oct. 30, 2018]*, 2014.