Demystifying Stablecoins

Didem Demirag Seyedehmahsa Moosavi Jeremy Clark

Gina Cody School of Engineering and Computer Science
Concordia University

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 the newly 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 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.

[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).

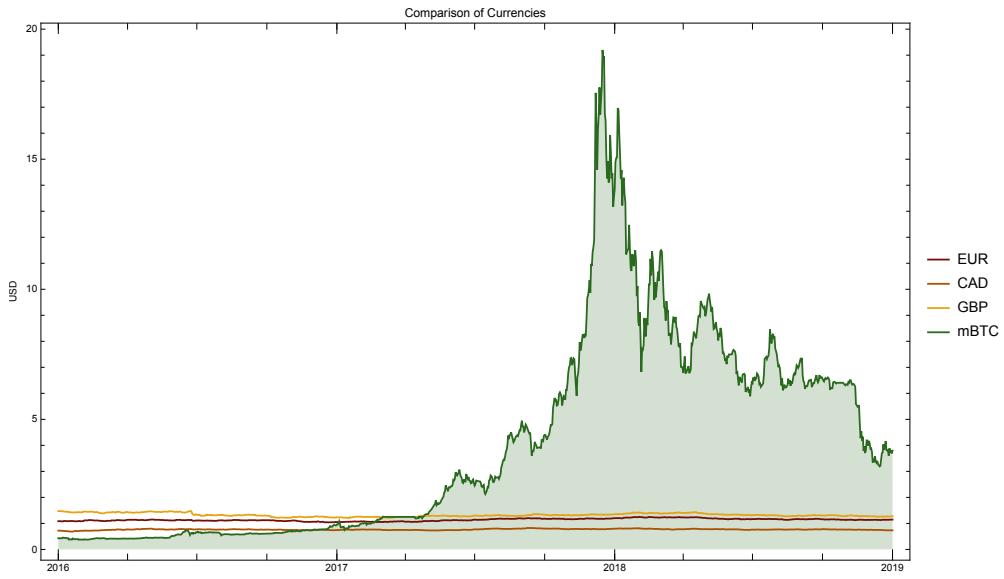


Figure 1: Comparison among fiat currencies and Bitcoin: The values are retrieved daily between 01 Jan 2016 and 01 Jan 2019. Note that 1000 mBTC = 1 BTC.

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 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. Next we distill stablecoin proposals down to a set of 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 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

there is a lot of different views, but we should include bank of england(explain that) In 2016, Ametrano introduces *Hayek Money*, a new monetary policy of elastic non-discretionary supply that can be used to achieve a price stable cryptocurrency [2]. There are currently many blog posts on the overview of stablecoins and how to design them. According to these resources, the main three approaches to design a stablecoin are (i) fiat-collateralized, (ii) crypto-collateralized and (iii) non-collateralized (also known as algorithmic)(*e.g.,* [6, 14, 17]) are the examples that give the overview of stablecoins based on these three approaches. Note that these resources uses various terms for these three categories interchangeably, **do we have to mention this? if yes (i) is it the best way of saying it? and (ii) should we mention each and every of these terms? (algorithmic, seignorage shares, elastic money supply)** 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 [5]. 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 from a crypto company called Blockchain [2] provides an extensive classification of 57 stablecoins together with discussions on issues related to governance (*e.g.,* legal structure, investors, partners *etc.*) [4]. In one of its blog posts, Consensys [3] describes stablecoins as "crypto-assets that maintain a stable value against a target price (e.g. USD)" and classify them according to the three main 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. Unlike other resources that define stablecoins within three categories (fiat-collateralized, crypto-collateralized, and non-collaterlaized), in this paper, we introduce new systemization of stablecoin projects and describe their fundamental primitives.

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[4]) 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

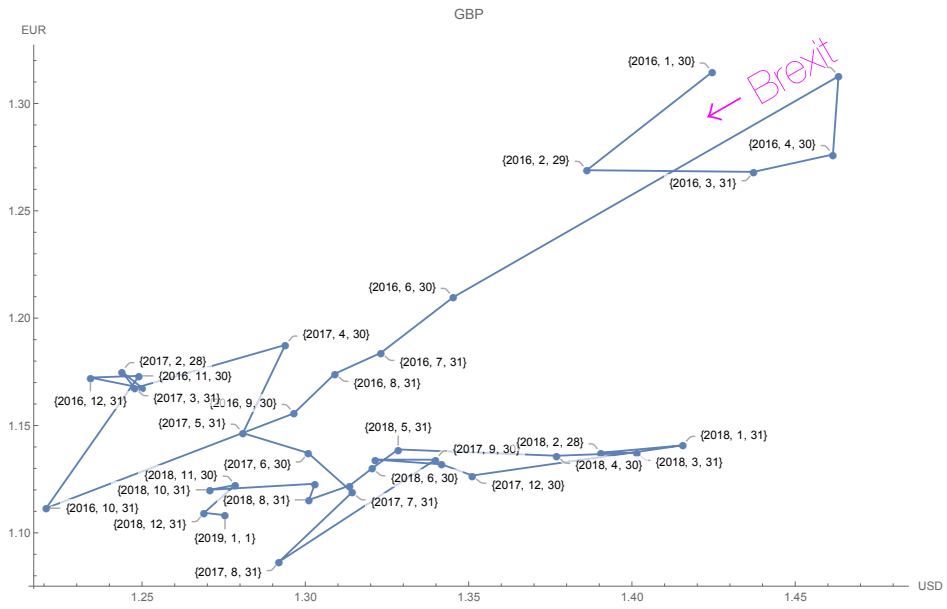
Consider that several hours after writing the previous section, 1 BTC is now priced at $3566.56 USD. In one sense, the price of BTC decreased by $32.20. However it is exactly equivalent to say the price of $1 USD increased by 0.002 mBTC. This raises a natural question: did BTC decrease in price or did 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 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.

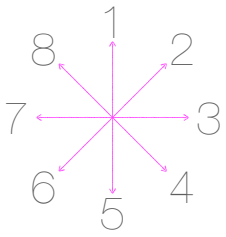
[2] https://www.blockchain.com

[3] https://consensys.net

[4] 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.

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. This is inspired by similar charts on the website FiveThiryEight for things like kicking distance in football[5] and they appear to be 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.

We will return to these charts later in Section 6.2 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

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

exhibit mostly vertical movements along the 1/5 direction.

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 [7]. 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 [7]. 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.

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

[6] https://www.coindesk.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	Market Manipulation	NuBits*	892
	Money Supply Adjustments	Ampleforth	⊥
		RSCoin	⊥
	Asset Transfer	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*.

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 ⊥.

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

[7] https://coinmarketcap.com

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-bockchain 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.*) cite that talk on gemini from michael's company's conference; 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, it pledges to keep the backing assets in trust for the duration of the circulating coins. We will shortly explain what impact there is on the coin if it does not provide redemption—obviously, if redemption were 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.

Discussion. The idea of tokenizing assets and re-selling them in a useful format (*e.g.,* as a portofolio 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. An electronically traded fund (ETF) will typically sell shares of a portfolio of assets, be redeemable for the assets, and will be priced closely ($\pm 1\%$) to the value of its underlying assets—it is most like the stablecoins in the previous section. A simplification of a trust fund, such as a closed end 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 be more moderately priced ($\pm 5\%$) to the value of its assets. Need to distinguish out three cases: directly redeemable, redeemable for ownership, not redeemable at all.

4.3 Indirectly-Backed.

5 Type 2: Intervention-based Stablecoins

5.1 Market manipulation

5.2 Discretionary input; money expansion/contraction output

5.3 Money expansion/contraction

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. 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.

5.4 Indirect money expansion/contraction

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.

5.5 Blockchian metrics input; with only internal information

6 Evaluation Framework

In this Section, we review various issues with different mechanisms of designing a stablecoin (discussed in Sections 4 and 5) . We provide an evaluation framework based on x (to be filled) criteria (see Table **??**) 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 advantages and disadvantages of different mechanisms for creating stablecoins.

Mechanism	Price Stability		Trust				Risks
	Stable to undervaluation	Stable to overvaluation	No issuance violation	Redemption guaranteed	No intermediaries for transfer	No trusted oracle	No collateral termination
Directly Backed and Redeemable	•	•					
Directly Backed							
Indirectly Backed							
Market Manipulation							
Money Supply Adjustments							
Asset Transfer							

Table 2: Evaluation Framework.

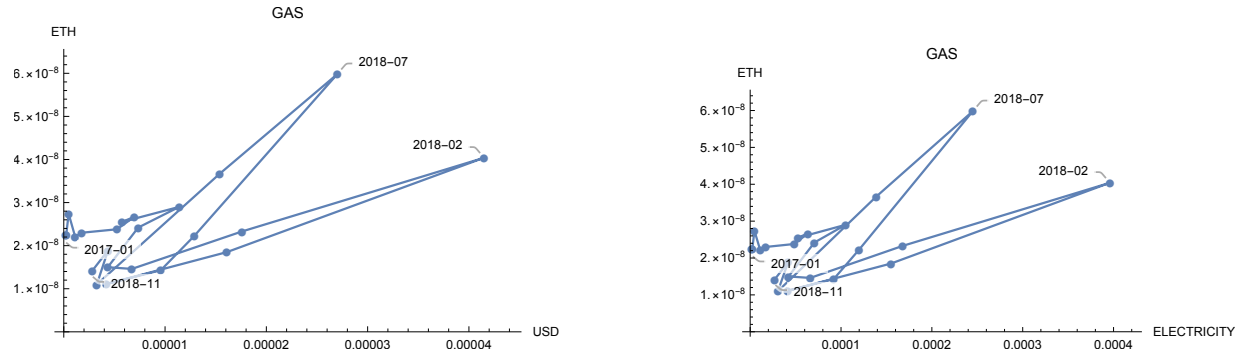
7 Discussion

7.1 Why so many?

7.2 What Stability looks like

7.3 Ethereum's Gas

The two spikes in the Fig **??** correspond to (i) January 2018 when Cryptokitties [8] was launched for the first time and (ii) when the FCOIN [9] was launched and required a lot of on-chain voting. Both these events have caused the GasPrice to go up as Ethereum users had to pay more Gas for their transactions to go through.

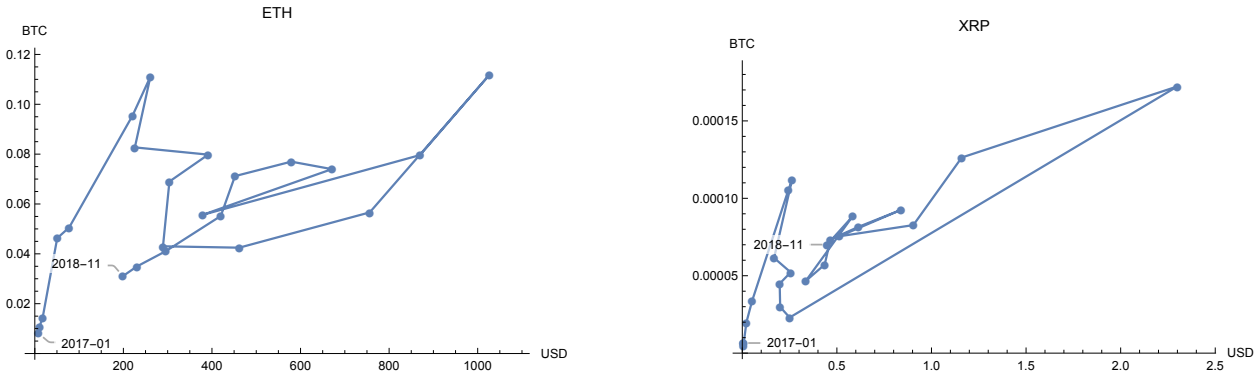


(a) Gas with respect to ETH and USD

(b) Gas with respect to ETH and Electricity price

Figure 3: Ethereum average GasPrice chart. As mentioned in the Section 6.3, the two spikes in the chart represent specific events happened in certain dates which have increased the GasPrice.

8 plots



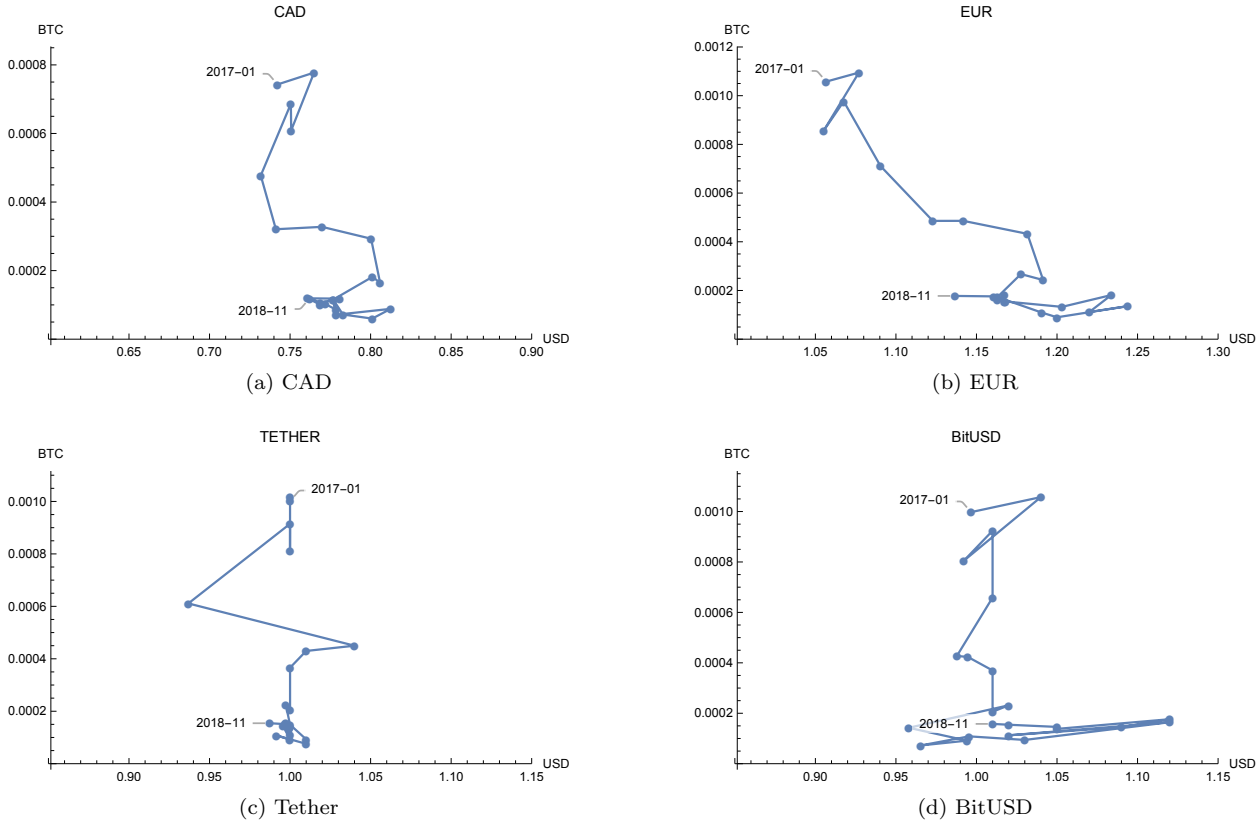
(a) ETH

(b) XRP

Figure 4: Volatility in cryptocurrencies

[8] Cryptokitties website `https://www.cryptokitties.co/`

[9] Fcoin website `https://www.fcoin.com`



(a) CAD (b) EUR

(c) Tether (d) BitUSD

Figure 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.

8.1 Consequences for Central Banking

9 Conclusion and Discussion

In this paper, we analyze the current state of stablecoins with the various options that have been so far proposed to achieve price stability. We also discuss various issues that stablecoins would address. According to the charts represented in the paper, gas is relatively stable in price, while Bitcoin and Ether show volatile behaviour. The reason could be the fact that how users interact with the interface to set the gas price when sending transactions to the Ethereum. By analyzing the properties of gas together with the existing methods to create stablecoin, we can later propose what properties stablecoins should attain.

References

[1] Black swan. `https://www.investopedia.com/terms/b/blackswan.asp`, 2008.

[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] 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).

[6] 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.

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

[8] M. Huillet. Ibm backs new us dollar-pegged stablecoin that runs on stellar network. https://cointelegraph.com/news/ibm-backs-new-us-dollar-pegged-stablecoin-that-runs-on-stellar-network, 2018. Accessed: 2018-07-17.

[9] P. Lee. Forget bitcoin: stablecoins will change how money works. https://www.euromoney.com/article/b1bbk5rb8gp227/forget-bitcoin-stablecoins-will-change-how-money-works?copyrightInfo=true, 2018. Accessed: 2018-10-29.

[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] M. Orcutt. "stablecoins" are trending, but they may ignore basic economics. https://www.technologyreview.com/s/611370/stablecoins-are-trending-but-they-may-ignore-basic-economics/, 2018. Accessed: 2018-07-06.

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

[15] L. Schor. Stablecoins explained. https://medium.com/@argongroup/stablecoins-explained-206466da5e61, 2018. Accessed: 2018-10-29.

[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.

10 Appendix

A The current state of stablecoins (might be needed for the paper)

Stablecoins have a market value of $3 billion and this corresponds to the 1.5% of the total market value of the cryptoassets [4]. Each proposing different properties, stablecoins can be categorized into three groups based on the way they achieve stability: fiat-collateralized, crypto-collateralized, and non-collateralized.

1) Fiat-collateralized stablecoins: These types of stablecoins are backed by fiat currency. Generally, there is a 1:1 peg between the fiat currency and the stablecoin that indicates a convergence between their values [6]. While USD is currently the most common choice to back the stablecoin, IBM states that they are also interested in projects that use other national fiat currencies, as they will be helpful for their blockchain integration [8]. Tether and TrueUSD are prominent examples of USD pegged tokens.

Discussion about centralization: In order to back up with stablecoins with fiat, one needs to place trust on a third party. Centralization ensures that the amount of money to back the stablecoin with, is held in an account [13] and the peg is attained. However, involvement of a third party causes controversy, as the third party can deny giving money to the users. Tether explains this point as follows [11]:

> "Redemptions will not be unreasonably denied, but we reserve the right to selectively deny redemption and creation of Tethers on a case-by-case basis."

2) Crypto-collateralized stablecoins: These types of stablecoins use other cryptocurrencies as a back up value rather than fiat currency.
Over-collateralization is needed in this case as the underlying cryptocurrency is also volatile [6]. MakerDAO and Reserve use this approach – utilizing a smart contract to back the stablecoin with another cryptocurrency [8].

If there is a black swan event [10] where the underlying currency loses its value and does not worth anything, the stablecoin also loses its value [15]. Due to the over-collateralization in this type of stablecoins, the loss of value will be drastic. This is the reason that a group of experts strongly discourage this approach.

3) Non-collateralized stablecoins: Unlike the previous types, this group of stablecoins are not backed by fiat currencies or another cryptocurrency. Here, the stability is achieved algorithmically which helps to provide better scalability [4].

Basis is one of the first projects of this type that achieves price stability using the dual-token model [11]. In this method, there is dynamic adjustment of the existing supply of the stablecoin. While one token is stable, the other is used to achieve the stability of the value. If the value of Basis increases (an increase over $1), more Basis tokens are produced to increase the supply which will lead to a decrease in the price and if there is a decrease in the price, a bond that is worth a Basis token is issued and some Basis tokens are bought to decrease the supply [9].

A.1 Remittance

Although cryptocurrencies, especially Bitcoin, play a revolutionary role in financial systems, they are yet not easy to transact with due to their volatile characteristics. Therefore with stablecoins, one can benefit from decentralized nature of the token, while there is no price volatility risk. In addition, stablecoins make the cross border payments, remittances, easier.

[10] A black swan event is characterized as being unexpected, random and having significant effects to the current situation. This type of an event is hard to predict [1].