Emergence of Stable Value Coins and A Trust Framework For Fiat-Backed Versions

This paper explores and compares stablecoins — a category of cryptographic token that seeks to maintain stable value to a reference asset. Three approaches are recognised: off-chain collateralised (IOU), on-chain collateralised, and non-collateralised (algorithmic). Further distinction within this taxonomy stems from the type of collateral used, algorithm design, and the degree of decentralisation and regulatory posture. Contrasted versus 'normal' cryptocurrencies such as bitcoin and ether, a different, complementary set of use cases are put forth, and potential adoption is estimated. Early evidence of performance (stability) is analysed, and a trust framework for fiat-backed, regulatory compliant stablecoins is established.

January 2019

pwc

LOOPRING

Content

Executive Summary

This report studies the current state of stablecoins, their uses and usefulness, and their potential impact on the cryptocurrency and adjacent industries in a regulatory context. Stablecoins seek to maintain a fixed value to a reference asset such as fiat currency or gold, or more prospectively, a basket of goods and purchasing power.

Money, according to mathematician John F. Nash Jr., "is the lubrication which enables the efficient transfer of utility." [1] While cryptocurrencies such as Bitcoin offer improvement over the intermediate commodities we use to store value today, they are — due to volatility — not sufficiently slick to grease global economic wheels.

Stablecoins present themselves as this lubricant, capable of facilitating trade, transfers, and a digitised economy.

Three types
Three stablecoin designs are recognized: off-chain collateralised (IOU), on-chain collateralised, and non-collateralised (algorithmic). In sections 5 & 6, this paper focuses on the regulatory considerations of the IOU fiat-backed (fiatcoin) model, which issues a token for each collateral unit held in custody.

Usage
By every measure, stablecoins have had an impressive 2018, and are shaping up to capture more cryptoasset market share in 2019. In December 2017, stablecoins had a market capitalisation of ~$1.2 billion; in December 2018, its more than doubled to ~$2.6 billion, with daily trading volumes of ~$5 billion.

Still dominated by a single large player (Tether), competition has heated up, with many projects on the horizon, but less than 10 live, meaningful players. Four USD-backed regulated fiatcoins, and one
on-chain collateralised stablecoin (DAI) have emerged or risen to prominence on Ethereum in 2018.

Use Cases
Trading, representative of the general cryptoasset landscape, is where stablecoin usage is concentrated. Stablecoins allow exchanges and traders to price pairs in fiat terms, easily move on/off board, hedge exposure, and seek shelter in uncorrelated assets — all without bank connectivity and the corresponding latency.

Trading, however, is but a beachhead. Stablecoins could possibly underpin the next generation of **payment rails**, facilitating cheap, instant, global transfers. Stablecoins also fulfill another

[1] Nash, John F. Jr. "Ideal Money and Asymptotically Ideal Money." October 1997. http://personal.psu.edu/gjb6/nash/money.pdf

monetary role as a **store of value**, especially for users with a hyperinflationary national currency who may now opt in to more prudent monetary policies.

Stablecoins are blockchain-native and can contain advanced logic in the token itself. **Programmable** money is capable of improving current processes, but also enabling an entirely new design space. As open source, **standards-based money**, walled gardens can be eliminated, allowing interoperability across (decentralised) applications, products, and assets.

As **financialisation** of blockchain-based assets increases — and as **tokenisation** of traditional assets increases — stablecoins can be expected to gain importance for two reasons: 1) fiat denominations are the status quo 2) financial contracts can not be meaningfully specified in uncertain terms. Unstable money is unusable money in any time-based financial contract, and really, any economic interaction at all.

Regulation
Regulatory compliant fiat-backed coins have recently been issued by large cryptoasset companies with prominent financial institutions as partners. Legal treatment of stablecoins differs across jurisdiction, and in some cases are regarded as similar to “prepaid” or “stored value” instruments. Regulators often treat issuers of these assets as “money service businesses”, with a focus on enforcing KYC/AML processes, and preventing financial crimes and bank law circumvention.

Compliance programs are primarily enforced at the “gates” of the system; the fiat on/off ramps where collateral is exchanged, and tokens are created or redeemed. Once on the blockchain, tokens can typically move freely, while issuers maintain the right and ability to blacklist nefarious users, and feeze token balances and collateral. This centralisation stands in contrast to the decentralised methods which do not impose oversight.

Fiatcoin Trust Framework
Fiatcoins are instruments of trust more so than technology. Risk primarily stems from counterparties — issuers and custodians — and is addressed by subjecting operations to stringent and transparent oversight. We propose a trust framework for fiatcoin issuers to consider, covering custody, audit, insurance, and technical choices.

Outlook
Stablecoins may be the first blockchain “product” with mass appeal and utility. We believe we will see continued adoption and competition in 2019. For fiatcoins, the business case for issuers is often strong, allowing for user aggregation, ancillary product (exchange, wallet) synergies, and potentially productive use of custodied assets.

Money, as a social technology, is predicated on confidence and coordination. We believe companies with strong user bases and goodwill may stand to benefit by issuing their own stablecoin to facilitate on-platform transactions. More than anything, we expect continued experimentation, with the ultimate benefit of familiarising users with blockchain and a tokenised economy.

Foreword

In 2014, Tether introduced USDT, a dollar-backed cryptocurrency. Even before the term stablecoin was popularised, the mechanism was easily understood: for every USDT issued, a corresponding US dollar is held in reserve at a bank. While novel for the world of blockchain-based assets, this IOU system has existed across time and geographies.[2]

Like the “Qianzhuang” (private banks) of ancient China, these operations were dedicated to the storage of merchants’ burdensome coins, and facilitation of increasingly globally-dispersed trade. The bank would accept deposits from the merchant, account for this sum on a bank note, issue the bank note to the depositor, who would thereafter (hopefully) be able to redeem it.

Stablecoins — particularly the fiat-backed variety that much of this paper focuses on — are a natural progression of this same phenomenon, only now, the technological advantages of blockchains present even greater efficiencies and possibilities.

This paper does not pass judgement on different stablecoin designs or implementations, but merely attempts to touch upon a multitude of stablecoin considerations. While potentially informative for a wide audience, we believe the reader who stands to gain the most is a person/entity who (1) has little existing knowledge on the topic, or (2) intends to issue a fiat-collateralised token. A technologist seeking deep explanation on the matter would likely be best served with the technical documentation of live projects.

To that end, it’s worth noting that while stablecoins have thus far been a decidedly ‘crypto’ topic — solve volatility in crypto — a point can be made that they are equally approachable from a legacy ‘fiat’ vantage point: help solve some of the remaining inefficiencies in fiat.

The latter part of this paper focuses on a trust framework for fiat-collateralised, regulated stablecoins. While uninteresting to ethos-driven crypto-enthusiasts for the considerable censorship concessions made, they nonetheless present interesting opportunities to businesses, and as compliant bridges between legacy institutions and a tokenised economy. With that framing, we find it helpful to view these assets as blockchain-powered products that may usher in the first wave of true mass adoption.

[Please note that we reference multiple stablecoin projects throughout this paper, and nothing herein should be interpreted as any endorsement for any token, investment, or anything of the nature. Cryptoassets — even stablecoins — pose risks, and thorough research should be done before owning, investing, or otherwise interacting with such instruments.]

[2] Szabo, Nick. "The Many Traditions of Non-governmental Money (part I)." Unenumerated. March 23, 2018. Accessed November 13, 2018. https://unenumerated.blogspot.com/2018/03/the-many-traditions-of-non-governmental.html

1. Introduction

The Bitcoin whitepaper recently turned 10 years old, and cryptocurrencies of different form and function have proliferated in its wake.[3] Mainstream and investor interest has grown considerably stronger in the past few years, owing to, among other things, Ethereum's ERC20 token standard, and the ease with which would-be token issuers can create and distribute their tokens on a ready-built platform.[4]

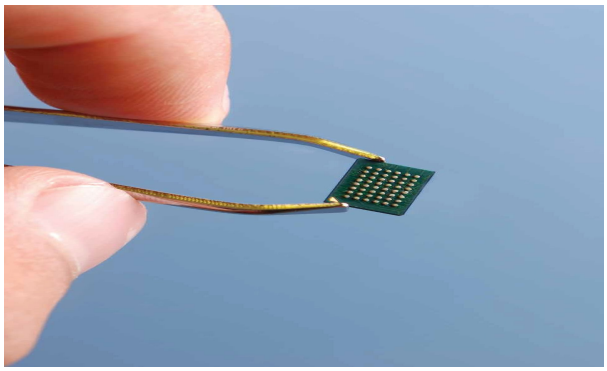
A common criticism of cryptocurrencies, however, is the pronounced price volatility, and the fact that there is 'nothing' underpinning their value. These digital assets are hardly usable as money (or at all) if extreme price changes are expected while buying/selling goods, sending/receiving payments, or otherwise transacting in the course of personal and professional life. Of the seminal roles money is meant to play, cryptocurrencies have heretofore fallen specifically short in attempts to be a medium of exchange and unit of account. (Many would argue that *current* volatility also precludes its success as a store of value, notwithstanding the fact that they have generally appreciated in price.)

Of course, for many, these price swings are a feature and not a bug: speculators globally have been drawn to this nascent asset class in pursuit of profit. Their role should not be underestimated, though, as risk-takers and traders are a prerequisite in bootstrapping networks and aiding in price discovery. Indeed, price discovery is what's happening right now, and by some measure, will never end: how else should the 'proper' exchange rate of USD to BTC be known? It is no trivial task to ascertain how much of fiat currency '*X*' one should be willing to trade in for a new monetary asset like BTC. Was $0.50 too cheap? Was $18,000 too expensive? Only time and the collective mind of billions of people will tell.

> "The main volatility in bitcoin comes from variability in speculation, which in turn is due to the genuine uncertainty about its future." [5]

For those who seek to truly use cryptocurrencies, however, price uncertainty is a bug. It is in this light that many have yearned for, researched, and deployed stable value coins (stablecoins). Of course, value stability begs the question: a stable value in terms of what? USD? CNY? Or, perhaps ideally, not measured in terms of fiat currency at all, but in the context of purchasing power, such as a basket of goods, or the Big Mac Index.[6]

Thus, a truth of stability is uncovered: value is relative, and a stablecoin must choose what to track and remain stable to. Price is always a ratio between two assets, and indeed only exists when there are two parts to consider. At the time of writing, all known, live stablecoin projects target a fixed exchange rate (as opposed to purchasing power), with two-thirds of these pegged to the USD. [7,8]



[3] Nakamoto, Satoshi. *"Bitcoin: A Peer-to-Peer Electronic Cash System."* October 2008. https://bitcoin.org/bitcoin.pdf
[4] Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform." April 2014. https://github.com/ethereum/wiki/wiki/White-Paper
[5] Sams, Robert. "A Note on Cryptocurrency Stabilisation: Seigniorage Shares." April 28, 2015. quoting Nick Szabo. https://github.com/rmsams/stablecoins/blob/master/paper.pdf
[6] "The Big Mac Index." The Economist. https://www.economist.com/news/2018/07/11/the-big-mac-index

1.1 Do we need them?

Depending on your interpretation of what Bitcoin or other cryptocurrencies are meant to be, its price volatility should not be solved for; it is a matter of fact, and a repercussion of design. Fixed supply (or fixed supply schedule) means demand shocks are absorbed wholly into price. As stated in one of the first publicly discussed notes on the topic of price-stable cryptocurrencies, "*Cryptocurrencies like Bitcoin govern the supply of coin through simple and deterministic coin supply rules. changes in coin demand get translated into changes in coin price, making price volatility proportional to demand volatility*". [9]

Volatility, though, is often cited as the greatest impediment to adoption. For the vast majority of potential participants - and for the potential underpinnings of a modern financial system — elevated volatility is a non-starter. Whether it be investors fearful to step into such an asset, businesses who cannot take price risk given their real-world fiat expenses/exposure, or employees averse to earning and storing their wealth in uncertain terms, cryptocurrencies are not on the precipice of mass acceptance for economic activity.

Year to date, BTC is down 75% in USD terms.[10] From mid-November to mid-December, BTC lost 44% of its value in USD terms. Coincidentally, the bulk of this paper is being written in the weeks and month where "the return of volatility" has viciously reared its head, following a relatively stable range near ~$6500 for some months. The trepidation of market participants makes it clear that if a significant portion of the digitised economy had actually depended on Bitcoin, activity may have ground to a halt. In the final months of 2018, cryptoassets have experienced 4%-5% daily volatility. [11]

For this reason, and for only some purposes, it is our view that stablecoins are complementary to 'normal' (non-pegged) cryptocurrencies, at least — or especially — in the short to medium term. With reduced volatility, much of the latent demand and use cases have the opportunity to engage with a new tokenised economy, and see firsthand the benefits afforded.

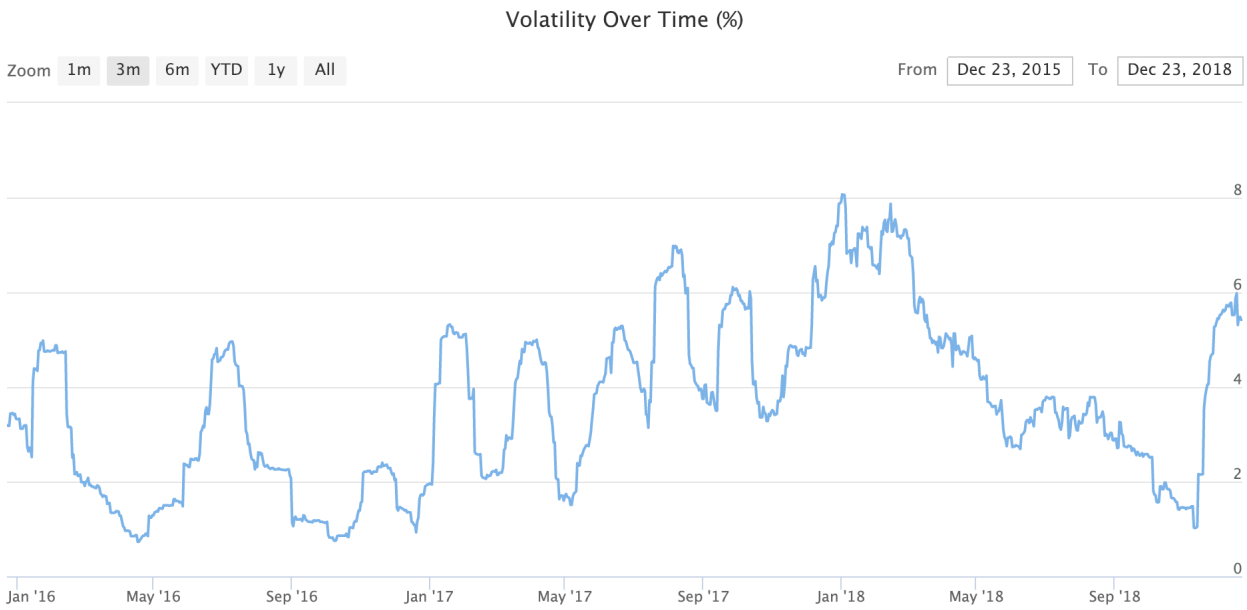
In the long term, normal cryptocurrencies — specifically the 'payment' variety such as BTC — seek to become an alternate monetary asset in parallel — or in lieu of — fiat currencies. For that goal, pegging price to fiat currency, or any value index, would defeat the purpose. To reach that reality, however — where new forms of money may proliferate — price-stable cryptocurrencies may represent the single best hope, bridge and educational tool. True familiarity with BTC or ETH may be easier for the average user's conception if departing from a stablecoin — itself 'living' on a blockchain — than from paper fiat.

1.2 Why now?

If 2017 was the year of the ICO, then 2018 may have been the year of the stablecoin — or at least its beginnings. There has been acute interest in stable value coins, and an abundance of issuance and innovation in this segment of the digital asset market. By some measures, as at the end of 2018, there are more than 150 stablecoin projects in existence, with less than 20% being live, and less still — under 10 — actually used. [12,13]

There are many reasons which may account for this recent proliferation. The most sobering would perhaps be that, in response to the price crash following the end of 2017's historic run-up, cryptocurrency participants

Figure 1 — BTC/USD 30 Day Volatility Of Daily Returns (Source: bitvol.info)



[7] Blockchain.com. "The State of Stablecoins." September 26, 2018. https://www.blockchain.com/research/
[8] Freeman, Nevin. "2018 - The Year of the Stablecoin." Hacker Noon. June 27, 2018. Accessed November 13, 2018. https://hackernoon.com/2018-the-year-of-the-stablecoin-6a6ca5d3637b
[9] Sams, Robert. "A Note on Cryptocurrency Stabilisation: Seigniorage Shares."
[10] CoinMarketCap. Accessed Dec 9. 2018. BTC @ $3,640. https://coinmarketcap.com/currencies/bitcoin
[11] Coinscious Market Report. 2018-11-23. https://coinscious.io
[12] Cement DAO. https://www.cementdao.com
[13] Stable Report. https://stable.report

simply don't have the stomach they once did, and fiat-pegged coins seem like an attractive proposition. Being able to hideout in value-stable coins without exiting the digital realm may have spurred activity in this sector.
Again, at time of writing, crypto-market participants — or at least active traders who move about assets — are thankful for stable $1 price tags versus multiple 10% daily drawdowns.

Another reason is the emergence of decentralised applications (dApps), some of which are beginning to become truly usable. A price stable token is now warranted and required. Indeed, some dApp use cases are infeasible, if not impossible, without a stable medium of exchange. Examples of these are explored in section 3, but mainly revolve around use cases where value must be 'locked' for some period of time, such as insurance, loans, or prediction markets.

Finally, as the entire ecosystem matures, especially in regards to regulatory compliance, the next wave of entrants may be gearing up to take part. Onboarding users and institutions into the decentralised economy has become a focal point for many in the space. However, the lack of simplified processes for connecting legacy fiat rails to the blockchain-based world is a pervasive problem. Stablecoins, by acting as an intermediate steppingstone, are a compelling — and in some instances, compliant
— solution.

2. Taxonomy

Before delving into stablecoin taxonomy, it's helpful to frame where stablecoins as a whole fall within the broader classification of cryptoassets. There are many emerging frameworks for general cryptoasset taxonomy, but at the highest level — and from a regulatory perspective — a relatively strong consensus is evolving around classification schemes. Using the recent classifications from the Swiss FINMA and UK FCA, there are: Payment / Exchange Tokens (BTC, LTC), Utility Tokens (ETH, LRC), Asset / Security Tokens (Tokenised equity, debt, etc.). [14,15]

Figure 1 — Cryptoasset Classification

Stablecoins fall into the category of Payment Tokens — those which seek to function as money, and what people generally think of today as currencies. As we note in sections 5.1 & 5.2, however, according to some regulatory frameworks, stablecoins are not treated as cryptocurrencies at all.

Although we identify three general types of stablecoin design, at an even higher level, there are but two types: collateralised and uncollateralised. Collateralised stablecoins are backed by some type of asset — such as fiat, gold or other crypto — while uncollateralised stablecoins have no asset-backing, and instead rely on algorithmic solutions. It's important to note that in addition to the collateralised and uncollateralised distinction, there is a dichotomy that can just as comprehensively cut the stablecoin landscape: trustlessness vs trustedness. Does the stability mechanism rely on trusting a centralised party, or does it rely on a distributed network of rational actors
and math?

2.1 Off-Chain Collateral

The simplest form of stablecoin involves an issuer holding an off-chain, real-world asset like fiat currency or gold in a bank account, and issuing a token that represents each unit. This token is a 1:1 IOU for the asset held in reserve. Stability is maintained by virtue of the fact that there is a corresponding 'physical' asset for which the token can always be redeemed.

Tether (USDT) and USD Coin (USDC) are examples of such IOU systems. We may rightfully call the subset of these structures that holds fiat (as opposed to gold, etc.), *fiatcoins*.

This form of stablecoin is the most simple to understand, and is where we have seen the largest increase in issuance in the second half of 2018. There has been a spate of fiat-backed stablecoins being issued by fully regulated and compliant companies: GUSD, TUSD, USDC, and PAX. [See section 6].

Redeemability of these tokens for dollars held in reserve is what inspires trust in this system. If a token owner cannot convert into fiat USD, either because the USD is not there (or only partially there), or because the issuer (or its regulator/ government) is prohibiting, all faith — and the peg — would be lost.

Note how this system is much like a national currency board: pegging its domestic currency to a foreign currency at some fixed exchange rate, and holding that foreign currency in reserve.

In this design, participants are wholly required to trust centralised parties. The centralised issuers of this system may position themselves as more trustworthy by making their operations more transparent with regular audits, working with reputable partners, and submitting themselves to regulatory oversight. Allowing users of these stablecoins to periodically self-verify the solvency of the system is paramount. In reality, verification is an auditor's assertion that the collateral is there.

[14] "FCA Cryptoassets Taskforce, Final Report." FCA. October 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf
[15] "FINMA Publishes ICO Guidelines." FINMA. February 16, 2018. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/
[16] There is certainly a finer level of granularity to explore, especially within utility tokens. There are also some tokens which may fall into two categories.

With licensed stablecoin sponsors, these tokens lend themselves most easily to implementing KYC/AML and other compliance processes. Remaining on the right side of regulators is a top priority for these systems, so tight control is kept by the issuer. As we will see in section 5, current designs primarily place KYC/AML at the 'gates' of the fiat on/off ramps.

It should be noted that many crypto-enthusiasts would refrain from labeling fiatcoins as 'crypto' at all. To them, these stablecoins are simply a better digital representation of fiat currencies; digital dollars, much like we have today in our debit, credit, and PayPal accounts. Even if tokenising these dollars on a public blockchain like Ethereum has benefits versus legacy infrastructure (faster/cheaper transactions, global reach, programmability, etc.) they are still just fiat representations.

2.2 On-Chain Collateral

The other type of collateralised stablecoin design uses on-chain assets, such as ether (ETH), as collateral.

The solution typically involves overcollateralisation, such as requiring $2 worth of ETH for every $1 worth of stablecoin issued. This builds in a buffer against downward price swings and protects the peg from being breached. If the collateral value sinks past some threshold, say, $1.50, the system requires turning in the stablecoin, and getting back your ETH. If not 'liquidated' by the user, this process can be enforced automatically by smart contract logic.

This stability mechanism is not distinct for the *type* of collateral per se, but for the fact that collateral and stablecoin are both on the *same chain*, so everything is self-contained. That means collateral is also publicly auditable, and logic can be written into the system itself. Like this, mechanisms can run unmediated, kept intact by economic incentives alone. This design can be as decentralised as the underlying blockchain, with no requirements to trust a single counterparty.

Much of this stability solution depends on the assets being held as collateral. The more stable the collateral, the more stable the system. Even better than low volatility assets backing the peg is a diverse *portfolio* of low volatility assets. A diversified, low volatility collateral pool can absorb shocks, and effectively prevent the more 'failsafe' features from being relied upon.

On its own, however, overcollateralisation isn't sufficient. In addition to the extra padding, there must be a mechanism to defend against black swan risk, and specifically against accelerated price decreases. It's also imperative that participants in the system be able to respond quickly and effectuate the processes that protect the peg. In MakerDAO's case, the last line of defense is called 'global settlement' — essentially a sweeping unwinding and returning of the collateral.

MakerDAO's DAI is the leading example of an on-chain collateralised stablecoin.[17] DAI is pegged to 1 USD through a system of smart contracts, excess collateral, dynamic feedback mechanisms, and incentive structures incorporating MKR, its non-stable governance token.

Anyone can create DAI by locking up their ETH (in future, other assets as well) in a smart contract known as a Collateralised Debt Position (CDP). These CDPs basically hold a user's ETH in escrow and issue DAI against it. A user must lockup ETH that is more valuable than the total amount of DAI they will receive, currently minimum 150% of the DAI value. For a user to retrieve their ETH, they turn in their DAI, which is then removed from circulation. Of course, any user can also buy/use DAI without knowledge of the backend intricacies.

Creating DAI from a CDP requires paying interest, or 'stability fee', currently at 0.5% per year. Interest is paid in MKR tokens to MKR holders. For this earning potential, along with ability to govern over protocol parameters, MKR holders take the risk that, in the case that global settlement would be unable to return $1 worth of ETH to every DAI holder, MKR tokens would be issued (inflated) and auctioned off to pay the difference.

Creators of CDPs must keep above the minimum 150% collateralisation ratio. If they fail to do so, they are liquidated (ETH auctioned off) and must pay a 13% penalty fee.

It's interesting to note that besides its utility as a stablecoin, this system allows ETH holders to margin trade. Consider the example of locking up $200 worth of ETH, drawing $100 worth of DAI from a CDP, and buying $100 worth of ETH with said DAI; $300 ETH total exposure.

While these mechanisms support stability, the first line of defense is simply traders having faith in the system, and being willing to arbitrage away any deviations.

One negative to overcollateralised on-chain systems is their capital inefficiency. By definition, the stablecoin is backed by a greater value of assets, thus requiring more resources to achieve its goal. Locking up these assets has opportunity costs.

2.3 Algorithmic

Uncollateralised stablecoins do not have any assets backing them up and instead rely on mathematical mechanisms. Price stability is achieved by algorithmically increasing or contracting the coin supply to offset changes in coin demand.

Say the peg is to 1 USD: if the price of the coin goes above $1, new coins are issued to devalue each one; if the price of the coin goes below $1, coins are removed from supply to increase the value of each one. With flexible demand and flexible supply, *price* can be the fixed variable.

[17] "Overview of MakerDAO | Dai" GitHub. Accessed November 13, 2018. https://github.com/makerdao/awesome-makerdao/blob/master/README.md.

As mentioned earlier, given that most cryptocurrencies have fixed or pre-defined supply schedules, price gyrations are essentially the result of changes in demand. Instead of having a preset supply schedule, algorithmic stablecoins alter the equation by having a fixed price peg, and flexible supply. This is akin to how central banks approach price stability and inflation-targeting mandates by influencing money supply. Indeed, like central bank policy, much of this mechanism is based on the Quantity Theory of Money, which states that price levels are proportional to the amount of money in circulation.[18]

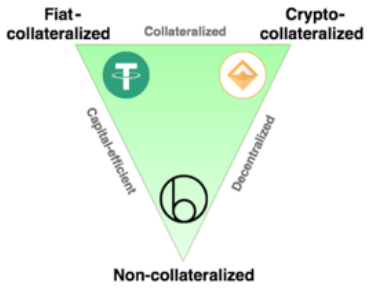
A difficult problem to solve is how exactly supply can be increased or decreased given a diverse set of ecosystem participants and coin holders. Increasing the supply is typically the easier shift to account for: the system can inflate the supply and distribute new coins in an auction, or proportionally to holders of auxiliary tokens in the ecosystem design. How a *decrease* in supply may be carried out is the more difficult problem. Whose coins can be burned? Is this process imposed, or can coin holders volunteer? What incentive would a coin holder have to turn in and burn their coins? There must be some benefit. These questions are answered by using other *non-stable* tokens in the system design, which often have equity or debt characteristics.

Basis was one such example that was set to launch this year (but actually folded during the writing of this paper). [19] In their system, 1 Basis was pegged to $1. In periods of contraction, users would purchase 'bond' tokens for less than 1 Basis, which would burn the Basis, and entitle them to receive 1 Basis in the future, if/when supply expands again. Thus, bond holders were 'rational' actors helping maintain the peg. A potential problem with this is that bondholders' willingness to purchase/ hold bonds is predicated on the belief that they will get more stablecoins when the system inflates supply. Thus, a foundational assumption is that there will be constant or monotonic growth in the system over time. [20] There was another non-stable token in Basis' design: shares. This was the fixed-quantity, equity-like component that, once all bondholders were made whole, received the newly issued Basis in proportion to their shares.

Sometimes referred to as seigniorage shares, there has not been enough evidence of live algorithmic stablecoins yet — and some, as we'll see in section 4.1, have failed after launch — so they remain the most experimental. It's worth noting that Basis cited potentially being afowl of SEC securities regulation among the reasons for shutting down and returning most of the $133 million raised to investors. Because of the likelihood that the non-stable tokens in these systems are securities, or the general uncertainty thereof, the growth of algorithmic stablecoins may be further stunted.

Many experts believe there is also greater chance of failure over *time* with this type; unlike crypto-collateralised designs which may strengthen over time by having more uncorrelated assets (including securities) in the debt pool. Furthermore, many believe that these systems must bootstrap stability by using collateral, until belief in their success is sufficiently strong to create the
required incentives.

Figure 2 — Stablecoin Trilemma (Source: Haseeb Qureshi)



2.4 Competition or Complement?

In addition to the three designs, we add Central Bank Digital Currency (CBDC) for the sake of comparison. CBDC is effectively blockchain-issued government money: it is the same as fiat money, just administered on a distributed ledger in attempts to achieve some of the associated efficiency or security gains from being purely digital, programmable, etc.

Figure 3 — 3 Stablecoin Designs and Their Characterisitics

	Off-Chain Collateral	On-Chain Collateral	No Collateral
Stability (in crypto-market crashes)	Yes	Maybe (so far, yes, as demonstrated by DAI)	Unproven (and dependent on growth)
Transparent/ Auditable	No (can approach 'trustworthiness' with audits, etc.)	Yes (everything on chain)	Yes (if everything happens on-chain)
Decentralized	No	Yes	Yes
Scalable	Yes (until limits brought by systemic risks, banks)	Maybe (only if underlying assets can scale)	Maybe (only if participants act 'rationally')
Capital-efficient	Yes	No	Yes

i. It should be noted that hybrid structures of the above exist, drawing stability from different sorts of collateral and algorithm-responsive supply.

ii. As mentioned, algorithmic stablecoins are largely unproven, and may have an increasingly difficult time finding their regulatory footing in light of recent Basis precedent. As of now, only collateralised versions have succeeded.

[18] "What Is the Quantity Theory of Money?" Investopedia. https://www.investopedia.com/insights/what-is-the-quantity-theory-of-money/

[19] Chaparro, Frank. "Stablecoin Basis is shutting down and returning nearly all capital raised to investors." December 12, 2018. Accessed December 12, 2018. https://www.theblockcrypto.com/2018/12/12/stablecoin-project-basis-is-shutting-down-and-returning-the-majority-of-capital-raised-to-investors/

[20] Monotonic Function. https://en.wikipedia.org/wiki/Monotonic_function

In terms of usage of the different types of stablecoins, it's reasonable to believe that different architectures will coexist and even complement each other. For example, fiatcoins can be used as collateral for DAI, broadening the collateral pool. It's also reasonable to believe that there is room for multiple coins within each architecture.

We believe stablecoins will exhibit differentiated usage patterns: crypto projects, dApps, and ethos-driven enthusiasts may be proponents of algorithm-based or crypto-backed stablecoins, while traditional financial institutions and traders may prefer fiat-backed designs.

From this perspective, it's perhaps palatable for philosophically-inclined crypto evangelists to see fiatcoins' place in the ecosystem. Although not fully aligned with the vision of a trustless P2P currency, fiat-backed stablecoins are a centralised product built on top of a distributed platform, showcasing the versatility of the technology. Centralised stablecoins will thus most probably find market fit in use cases that are least likely to be censored by central entities.

As we will see in the next section, different stablecoins will lend themselves to different use cases. Like traditional technology companies, creators of these coins should have an idea of product-market fit. If indeed stablecoins are viewed from a 'product' lense, it's clear that these cryptoassets may be the most likely to first capture a truly global audience.

3. Use Cases

For many decades, the open protocols underpinning the internet have allowed people all over the world to freely communicate and share information with the proverbial click of a button. Global connectivity and zero marginal cost of information exchange have been pillars of modern economies and living standards. We are quite frankly constantly in some sort of data sharing instance, either consuming or providing content.

Money, on the other hand, is not capable of the same fluidity within our modern systems.

Until this point, the crypto market has mostly sought stablecoins (Tether) for trading related purposes. Speculation has its place, but as we'll see, the use cases made possible with a trusted or transparent stablecoin are much more ambitious and impactful.

3.1 Trading

For all the tremendous technological change that blockchain-based money can inspire, its killer app has thus far been less lofty, and has resided on the orderbooks of exchanges, borne by traders and speculators.

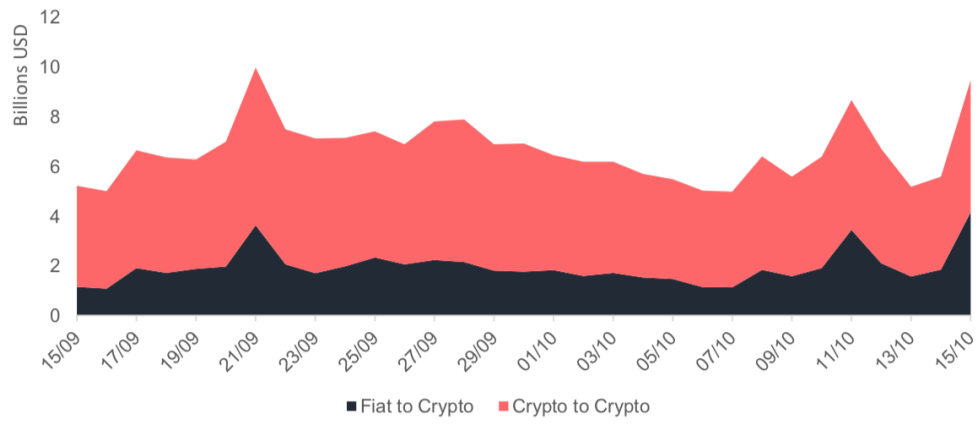
Trading or investing is, for now, the dominant activity that occupies the minds of the general public regarding cryptoassets. It is also the activity that generates the most obvious pockets of profit, with exchanges reaping the greatest rewards. In the second half of 2018, daily trading ranged between $10-$20 billion of cryptoassets, representing roughly 5%-10% of the total
market capitalisation.

Stablecoins, as a quote currency for trading pairs, represent a huge opportunity to be on one side of every trade. Given that traders typically price assets in fiat terms, as well as measure their performance and risk in fiat terms, fiat-pegged stablecoins are a natural tool for traders.

Examining recent figures, USD represents half of BTC to fiat trading on average, followed by JPY (21%), KRW (16%), and EURO (9%). [21]

Stablecoins are especially useful on exchanges that don't offer fiat to crypto trading. On such exchanges, pricing trades or hedging in fiat is impossible. With stablecoins, traders are able to use de facto fiat tools for their strategies, and exchanges are able to price pairs in fiat without bank connectivity. About half of all exchanges offer fiat to crypto trading, but these exchanges account for only one quarter of total market volume.

Figure 4 — Crypto to Crypto versus Fiat to Crypto Spot Volumes (Source: CryptoCompare)



[21] Cryptocompare. "CCCAGG Exchange Review." October 2018. https://blog.bitmex.com/wp-content/uploads/2018/11/cryptocompare_exchange_review_october_2018.pdf
[22] ibid.

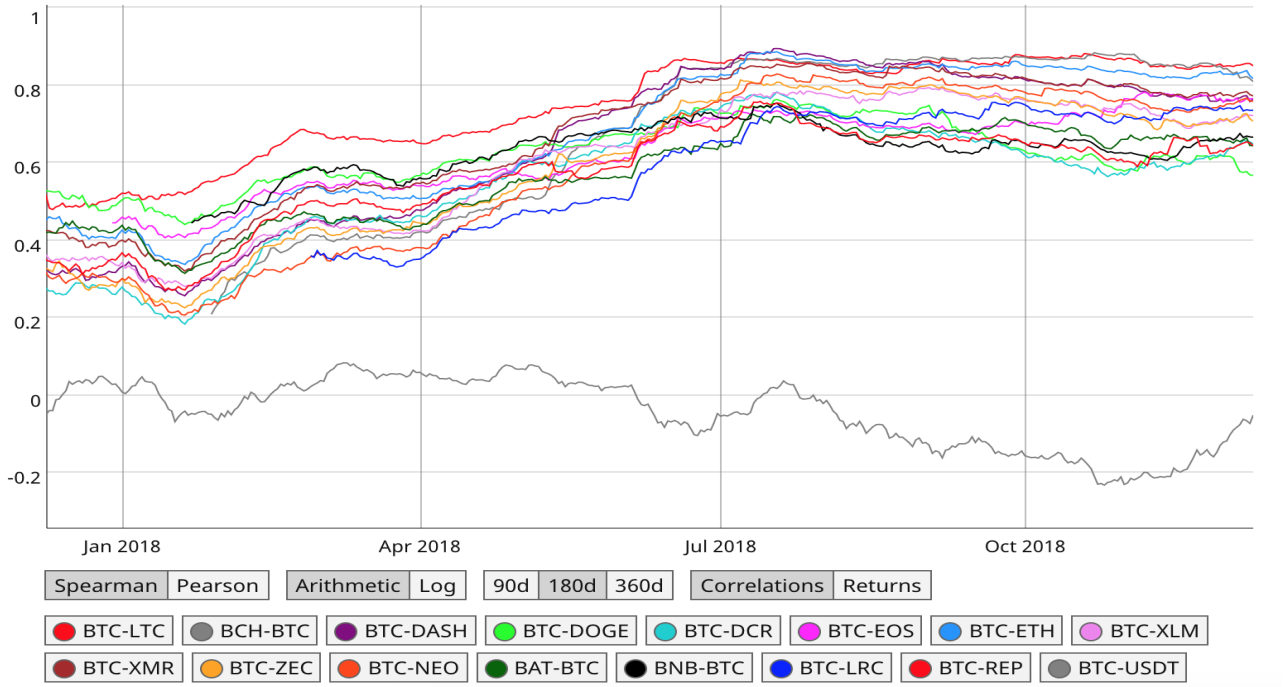
Stablecoins also present an opportunity for their issuer to be at the center of a robust ecosystem of other products and aggregate users. For example, USDC, a USD-backed coin issued by CENTRE, a consortium including Circle and Coinbase, recently announced zero trading fees on USDC pairs at Poloniex, a Circle-owned exchange.[23] With such tactics, issuers have means by which they can increase usage and volume of their ancillary products, as well as the stablecoin itself.

Non-exchange-linked stablecoins are also wasting no time in attempting to bootstrap usage and gain volume dominance on third-party exchanges. PAX recently announced a trading competition rewarding Binance users with the greatest PAX trading volume with prizes of 150K PAX. [24]

Elsewhere in the exchange world, the lines between stablecoins have been intentionally blurred. Huobi launched its HUSD program, which abstracts and replaces the stablecoins users see with a single stablecoin, HUSD, instead of the four potential fiatcoins behind it. [25]

Besides as a pricing token, having a stable asset to park 'cash' in is especially beneficial during protracted market downturns. Given the high positive correlations between cryptoassets, having an uncorrelated asset such as fiat-pegged stablecoins could mean the difference of surviving market cycles or not. In this sense, stablecoins can be seen as short-term stores of value.

Figure 5 - 180-day Return Correlations (Source: Coinmetrics.io)



On a more forward looking basis, as traditional financial assets such as stocks, bonds, and real estate become tokenised and ported to blockchain infrastructure, stablecoins will be of greater importance as a quote currency. These traditional assets will necessarily be priced and traded in fiat terms.

Many on-chain derivatives even require stablecoins as an input to their creation, such as to provide inverse exposure to assets like ETH (short-ETH tokens).[26]

[23] "Stablecoin Wars: Poloniex Eliminates USDC Trading Fees to Boost Volume." CCN. November 09, 2018. Accessed November 15, 2018. https://www.ccn.com/stablecoin-wars-poloniex-eliminates-usdc-trading-fees-in-bid-to-boost-volume/
[24] "PAX Trading Competition - 150,000 PAX To Give Away!" Binance. November 29, 2018. Accessed December 3, 2018. https://support.binance.com/hc/en-us/articles/360020102112
[25] Faridi, Omar. "Singapore-based Huobi Launches HUSD Solution for Better Stablecoin Management." CryptoGlobe. October 19, 2018. Accessed November 17, 2018. https://www.cryptoglobe.com/latest/2018/10/singapore-based-huobi-launches-husd-solution-for-better-stablecoin-management/
[26] Short Tokens. https://shorttokens.io

3.2 Money

Fiatcoins do not so much compete with fiat as they do just tokenise it. The decentralised designs, on the other hand, may one day directly vie against fiat money. As mentioned, money performs three functions; medium of exchange, store of value, and unit of account. Below, we evaluate the first two — unit of account is not considered since stablecoins by definition adopt another unit.

3.2.1 Medium of Exchange (Payments)

Legacy payment rails still exist in disparate silos, and do not provide the same contiguous user experience we feel with non-money communication.

A strong case for stablecoins comes from the possibility of opening up money and payment networks in the same way the Internet opened up email and social networks. Correspondingly, the biggest advantages of such a paradigm shift are the improvements and design space we cannot yet imagine.

Part of cryptocurrencies' initial promise was the ability to exchange value with one another quickly, cheaply, globally, and autonomously. In one short decade, that is basically a reality, marked by difference of degree. However, the act becomes less impressive if the cryptocurrency being sent is liable to lose a fifth of its value en route. With volatility 'solved', stablecoins have substantial ability to overhaul payment rails.

Stable value units atop blockchain infrastructure make a compelling case as technology to underpin modern money transfer systems:

- There are no opening hours nor holidays to consider on a *world* computer such as Ethereum; users can send payments any day, any time.
- 'Instant' settlement (~15 second block times on Ethereum).
- Payment fees are much cheaper than the status quo and do not scale with the amount transferred.
    - Sending a typical ERC20 token to another address costs 0.00019 ETH ($0.03) at time of writing. [27]
- For decentralised designs, there are no borders and no censorship.
    - For centralised designs: can 'transfer' anywhere, but may be unable to redeem in certain instances or jurisdictions [see section 6].

While stablecoins certainly edge out wire transfers and SWIFT on convenience, speed and cost, a fair retort may be that PayPal, Visa, mPesa and WeChat also allow for 'anytime', instant, cheap transacting. Although true in some cases, these networks have maximum amounts that can be transferred so easily, with further tiers requiring greater delays. In fact, maximums are enforced in general, not just for speed: PayPal allows $60,000 maximums, often in $10,000 increments.[28] For centralised fiatcoins, notwithstanding any regulatory restraints, $1 can be sent as easily and cheaply as $10 million. For decentralised stablecoins, there is of course no limit; the entire supply can theoretically be traded in one transaction.

Micropayments are oft cited as a benefit becoming possible with stablecoins. However, if micropayments were to scale to meaningful size, it would bring with it blockchain bloat, and a potentially unusable or prohibitively expensive payment environment. In other words, its success may mean its demise, unless offloaded to off-chain payment channels with near zero costs. USDC plans to support optional state channels for CENTRE node operators.[29]

Finally, for cryptonative businesses or normal merchants that just want to accept crypto, stablecoins are a welcome asset to earn, hold, and forget about price risk.[30]

[27] ETH Gas Station. Accessed November 21, 2018. https://ethgasstation.info/
[28] "Are There Any Limits to How Much I Can Send or Receive from My PayPal Account?" PayPal. Accessed November 21, 2018. https://www.paypal.com/ca/smarthelp/article/are-there-any-limits-to-how-much-i-can-send-or-receive-from-my-paypal-account-faq732
[29] CENTRE. "CENTRE Whitepaper" May 2018. https://www.centre.io/pdfs/centre-whitepaper.pdf
[30] Paxos Standard. "Paxos to Partner with Bitpay, Global Bitcoin Payment Service." November 20, 2018. Accessed November 23, 2018. https://medium.com/paxos/paxos-to-partner-with-bitpay-global-bitcoin-payment-service-aba00c7b1c7b

3.2.2 Store of Value

Pegging value to a fiat currency such as USD effectively outsources a stablecoin's monetary policy to the Federal Reserve. Thus, while the stability mechanism ensures a fixed rate between token and fiat, fiat-pegged currencies are relying on real-world central banks to maintain stability versus the rest of the world, and in terms of purchasing power.

Again, while this may be anathema to cryptocurrency purists, it represents an important improvement for citizens of unstable monetary regimes such as Venezuela.[31] Should such citizenry hold USD-pegged stablecoins, they can effectively escape their hyperinflationary currencies, and store value with more certainty. All a user would need is an internet connection, and can then opt-in to the monetary policy of a much more credible central bank. This would also be less prone to seizure by national banks than cash or savings accounts. Censorship resistance is of course more assured with decentralised stablecoins.

If there were sanctions or restrictions on holding USD for some users, and the institutional issuers of regulated fiatcoins complied with these rules, then fiatcoin holders may be limited in their access to the asset. As we will see in sections 5 & 6, the centrally issued fiatcoins have power to blacklist addresses, or prohibit redemptions of fiatcoins back to fiat.

One potential concern is what would happen if a fiatcoin becomes sufficiently popular that it represents a substantial part of the money supply. If, for example, we get so accustomed to using USD-backed fiatcoin, it's possible at some point we'd start to forget about USD itself, which, we posit, may not matter, as it's an abstraction. The decoupling could actually be trivial as it's not backed by a hard money anyways — they're both fiat.

This would still give a nation sovereign control of their money — maybe even more so, if *they* were the issuer of the digital money themselves. This would provide increased ability to pursue policy goals, such as better transmission of interest rates. Indeed, governments have shown interest in potentially issuing 'fiatcoins' — purely digital dollars — known as Central Bank Digital Currency.[32]

For decentralised stablecoins, repercussions of popularity would not be as clear-cut, as de facto fiat would be 'minted' that does not correspond to the existing or controllable monetary base.

3.3 Programmable for Digital Economy

Blockchain-based money is digitally-native money. Cryptocurrencies basically have built-in computers and the ability to execute arbitrary logic. Money is enabled to run like software, and programmers can shape the way it functions and how users interact with it.

The digital wallet and money itself may become more of a homescreen. It's where a user starts, and from where they can do anything: a browser holding and running on real value. Experiences would emanate from programmable assets.

The decentralised web is already taking shape before our eyes. So called Web3 is an internet where users have more control of their data, money, and outcomes. This time around it's the shared and open protocols that capture valuable 'state', not solely the applications and companies on top.

Decentralised applications (dApps) are the interfaces to explore global digital playgrounds, and many experiences do indeed operate with tokens like arcade games. To the extent that all dApps, exchanges, wallets, payment rails, and games converge on a standard — such as ERC20 — a fiatcoin may be an appropriate ticket to this world as tokens that have a stable value may be easier to use in these networks.

Some dApp use cases may be rendered inconvenient, if not unusable, without stablecoins. This mostly centers around instances where a non-negligible amount of time is involved.

- **Credit markets**. Borrowing or lending with a volatile base asset makes a system too complex or untenable, with users apprehensive to participate.
- **Insurance markets**. Long-lived products such as life insurance — may require a stable unit to make underwriting feasible and premiums calculable. Can you imagine actuaries having to factor in expected volatility of cryptocurrency into their risk pricing?
- **Prediction or gambling markets**. Predictors (or gamblers) lock up stake but only mean to wager on the outcome of the event and not worry about the extra risk of market price. A price-stable unit may be useful to make these financial decisions, and many others involving decentralised derivatives, etc.
- **Staking**. Securing apps or even entire networks with proof-of-stake, the fiat-denominated return of staking still depends more on the vagaries of the market pricing said token than on the expected rate of token return. As long as fiat price volatility remains elevated, the opportunity cost of staking is very high, or incalculable.

As a corollary, many developers who may come to depend on these dApps for their livelihood would prefer to receive a value-stable income.

The true beauty of 'hosting' currency on such a platform, however, is the interoperability it allows. Value can flow freely throughout the entire blockchain on which a money is based, where each disparate developer's work compounds the value of the network — no more walled gardens, or walled wallets.

Further expanding the opportunities, different blockchains will be able to speak with each other and port value across using a multitude of methods.

Stablecoins may also be an attractive native currency for bespoke blockchains. With a stable unit of account to pay for whatever the network is offering — storage, computation, content, exchange — transacting becomes easier. Recently, xDAI POA blockchain was deployed, where DAI is the native unit. [33]

[31] Airdrop Venezuela. Accessed November 25, 2018. https://airdropvenezuela.org
[32] Griffoli, Tommaso Mancini, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu, and Celine Rochon. "Casting Light on Central Bank Digital Currencies." IMF. November 12, 2018. Accessed November 18, 2018. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233
[33] POA Network. "POA Network Partners with MakerDAO on XDai Chain, the First Ever USD-Stable Blockchain!" October 18, 2018. Accessed November 23, 2018. https://medium.com/poa-network/poa-network-partners-with-makerdao-on-xdai-chain-the-first-ever-usd-stable-blockchain-65a078c41e6a

4. History & Current Landscape

Developers and thought-leaders have been thinking about stable value coins for some time. In 2014 Vitalik Buterin wrote a paper, *The Search for a Stable Cryptocurrency*, in which he asks, "Can we get the best of both worlds? Can we have the full decentralisation that a cryptographic payment network offers, but at the same time have a higher level of price stability, without such extreme upward and downward swings?"[34]

2014 also marked the beginning of the two most well known stablecoins, each taking a starkly different path: Tether and DAI.[35]

Since then, there have been well over one hundred stablecoins dreamed up or deployed. A recent report found and focused on 57 different stablecoins live on market or in planning stages. Of these 57 projects, 77% of them are the collateralised variety, with an almost even split between collateralising with off-chain assets (46%), and on-chain assets (54%).[36]

The US dollar remains the reserve currency even in the digital realm, with two-thirds of coins targeting $1 as the reference peg. Other pegs include fiat currencies such as Euro (EURS), and commodities such as gold (DGX).

4.1 Empirical Evidence: Performance and Stability

Tether, the 'original' stablecoin has remained remarkably stable, oscillating tightly around its $1 peg: USDT prices of $0.98 and $1.02 can usually be explained by supply/demand imbalances across exchanges relating to fees, etc.

However, stablecoins' real value and mettle is only truly tested in times of turbulence. Recently, amid the broad and deep market sell-offs, Tether has held up well, but there have been instances where market worry about collateralisation did show. Continuous questions about producing an audit and uncertain banking relationships have tested market confidence that Tether Ltd has the appropriate amount of USD in reserve.

In mid-October, USDT briefly traded as low as $0.87 on some exchanges, but the token quickly repriced closer to its $1 peg.[37] Around the same, Tethers began being redeemed — traded in for fiat USD — in large quantities, with approximately $1 billion worth of USDT being removed from circulation. [38]

[34] Buterin, Vitalik. "The Search for a Stable Cryptocurrency." Ethereum Blog. November 11, 2014. Accessed November 23, 2018. https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/

[35] DAI was not issued on mainnet until 2017, but MakerDAO was founded in 2014

[36] Blockchain.com Stablecoin Report, https://www.blockchain.com/research/

[37] De, Nikhilesh. "Stablecoins All Want to Be $1, But They're Not Worth the Same." CoinDesk. October 17, 2018. Accessed November 18, 2018. https://www.coindesk.com/which-stablecoin-is-the-riskiest-the-crypto-market-is-pricing-that-in

[38] "Upcoming USDT Redemption — October 24th, 2018." Accessed November 21, 2018. https://tether.to/upcoming-usdt-redemption-october-24th-2018/.

It should be noted that Tether did produce a recent third-party assertion regarding their solvency, but some market participants would still like to see greater and more regular reviews.[39] Although we are beginning to see a new class of regulated fiatcoins produce transparent reviews, in general, because of crypto's nascency and predated auditing standards, there are difficulties in acquiring the level of public assurance that many demand or are familiar with in traditional accounting realms.

Persistent deviations from the peg can be interpreted as the market quantifying risk premia across coins. A month after divergence started taking shape, USDT has at times traded at slight discounts, while the regulated fiatcoins trade at slight premiums. However, that is certainly not always the case, with USDT also frequently trading at premiums. The $1 peg could serve as a demarcation of confidence in the coins.

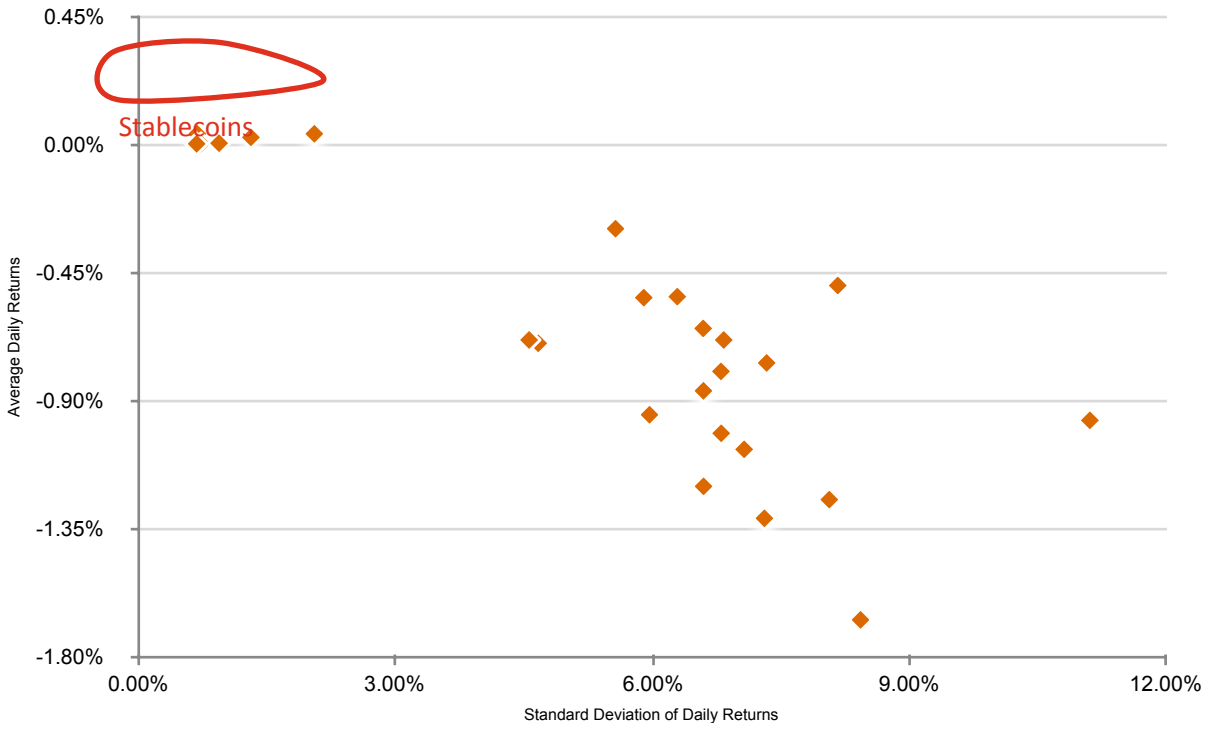
Temporary peg breaks aside, fiat-backed models have performed well, and outright failure has not occurred.

More impressively, on-chain collateralised models such as DAI have also maintained their mandate, continuously hovering around the $1 peg. This has been all the more notable given recent rapid price declines in ETH — the collateral backing DAI — with the CDPs being recollateralised or unwound quickly and effectively. Just as importantly, traders *believe* it will continue to function, and arbitrage the dips away.

The same performance track record cannot be said for some of the more experimental designs. Nubits (USNBT), a seigniorage share design, successfully held its $1 peg for over one year before breaking off in mid-2016 and trading as low as $0.20.[40] This was explained as Nubits succumbing to heavy selling pressure as traders piled into Bitcoin during a price spike. Nubits now lingers at ~$0.05. Notably, the peg broke to the upside at times as well, with Nubits trading as high as $1.25. This coincided with periods where Bitcoin was depreciating quickly and people sought the safety of stablecoins. Contrary to what may seem like a 'good'problem to have, it is not, as stability is the goal, and appreciation would in fact harm some users, such as borrowers who may have to repurchase the token at term-end.[41]

As one would hope, the current class of stablecoins have held their pegs during the recent violent price rout. Measuring the entire crypto industry's past month performance highlights stablecoins as the best performing cryptoasset sector.[42] It's exactly when fiat-pegged tokens are the 'biggest gainer' of the month that users want to own them.

Figure 6 — Plot of mean daily return against daily volatility; October 23, 2018 to November 22, 2018. Stablecoins and selection of top 50 coins. (Data from Coinmetrics.io)



[39] Hochstein, Marc. "Tether Review Claims Crypto Asset Fully Backed — But There's a Catch." CoinDesk. June 21, 2018. Accessed November 21, 2018. https://www.coindesk.com/tether-review-claims-crypto-asset-fully-backed-theres-catch.
[40] Reserve Research Team. "The End of a Stablecoin - The Case of NuBits" Medium.com. July 12, 2018. Accessed November 21, 2018. https://medium.com/reserve-currency/the-end-of-a-stablecoin-the-case-of-nubits-dd1f0fb427a9
[41] "NuShare Holders: Shortage of US NuBits." NuBits Forum. December 21, 2017. Accessed November 17, 2018. https://discuss.nubits.com/t/nushare-holders-shortage-of-us-nubits/5674.
[42] Coinscious Market Report 2018-11-23

4.2 Volume and Usage

Stablecoin usage has increased dramatically over the past year as more mainstream trading has provided a boost in appeal and utility. The recent increased issuance of fiat-backed coins and late-year downturn in prices have also driven activity in the sector.

Tether is still the leader across measures of stablecoin success and usage. Mirroring general cryptoasset interest, usage and volume picked up significantly towards the end of 2017. Today, Tether routinely sees $2-$4 billion of daily trading volume, accounting for 96%+ of all stablecoin trading.[43] Tether trades 1-2x its total market capitalisation, meaning, on average, every single USDT trades once or twice a day.

Figure 7 — Stablecoin Market Cap and Volume (Data from: www.coinmetrics.io)

01-Oct-18

Name	Price	Market Cap	Exchange Volume (24h)	Market Cap %	Volume %	Velocity (Volume/M.Cap)
Tether (USDT)	$1.00	$2,797,491,702	$3,069,480,000	94.5%	99.4%	109.7%
TrueUSD (TUSD)	$1.00	$107,147,805	$15,807,500	3.6%	0.5%	14.8%
Dai (DAI)	$1.00	$55,886,263	$3,184,430	1.9%	0.1%	5.7%
Total		**$2,960,525,770**	**$3,088,471,930**	100.0%	100.0%	

Note: PAX, USDC, GUSD only started existing/trading around this time, so data is incomplete for those coins on Oct 1.

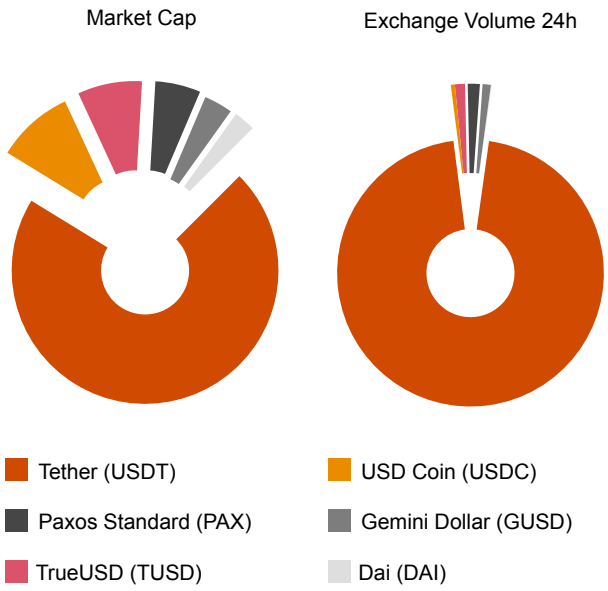
15-Nov-18

Name	Price	Market Cap	Exchange Volume (24h)	Market Cap %	Volume %	Velocity (Volume/M.Cap)
Tether (USDT)	$0.97	$1,659,628,239	$4,956,910,000	75.9%	97.3%	298.7%
TrueUSD (TUSD)	$1.02	$160,662,888	$43,802,400	7.3%	0.9%	27.3%
USD Coin (USDC)	$1.02	$145,288,638	$18,776,600	6.6%	0.4%	12.9%
Paxos Standard (PAX)	$1.01	$131,560,843	$60,039,800	6.0%	1.2%	45.6%
Dai (DAI)	$0.98	$72,370,890	$9,209,190	3.3%	0.2%	12.7%
Gemini Dollar (GUSD)	$1.01	$17,281,111	$3,293,580	0.8%	0.1%	19.1%
Total		**$2,186,792,609**	**$5,092,031,570**	100%	100%	

29-Dec-18

Name	Price	Market Cap	Exchange Volume (24h)	Market Cap %	Volume %	Velocity (Volume/M.Cap)
Tether (USDT)	$1.02	$1,898,037,885	$4,372,940,348	71.3%	95.7%	230.4%
USD Coin (USDC)	$1.01	$248,951,712	$22,783,697	9.3%	0.5%	9.2%
TrueUSD (TUSD)	$1.01	$208,223,689	$55,522,929	7.8%	1.2%	26.7%
Paxos Standard (PAX)	$1.01	$146,552,983	$66,809,144	5.5%	1.5%	45.6%
Gemini Dollar (GUSD)	$1.02	$92,480,324	$45,384,295	3.5%	1.0%	49.1%
Dai (DAI)	$1.01	$69,602,899	$4,526,737	2.6%	0.1%	6.5%
Total		**$2,663,849,493**	**$4,567,967,150**	100%	100%	

[43] Stablecoin Index. Accessed December 8, 2018. https://stablecoinindex.com/volume



USDT is the second most traded cryptoasset after BTC, measuring at 60% of BTC's volume. Its ~$1.8 billion market capitalisation ranks it as a top ten cryptoasset. It is also the most ubiquitous stablecoin, sporting the most exchange listings; 50+, and most trading pairs; 200+.

With the launch of the four new regulated fiatcoins, however, and specifically since the market downturn beginning in mid-November, Tether has been slowly ceding its large lead in terms of volume and even more so with market cap.

Meanwhile, MakerDAO's DAI is currently holding 1.5% of all ETH as collateral in CDPs, having doubled this proportion in the last 3 months.[44] CDPs are currently collateralised at an average ratio of 250%, meaning there is $2.5 in ETH for every 1 DAI.

DAI's $1 peg has stayed steady, and its smart contracts have handled the increased usage and stress without hesitation. With 55 million DAI in circulation, DAI is quickly becoming the de facto decentralised stablecoin for the tokenised economy. Its integration in dApps and protocols — especially those building open financial infrastructure — is widespread and significant.

5. Regulation & Compliance

Regulatory compliance is imperative for any stablecoin issuer that seeks to interact with the established global financial services industry. It is the goal of many in the stablecoin space to coexist and cooperate with legacy financial institutions, and to do this, they must submit themselves to the same stringent standards.

While a fully regulated and licensed operation is the clear goal for compliant stablecoins, it's worth noting that for the decentralised cohort of stablecoins, compliance requirements often stand in direct opposition to elements of their ethos.

5.1 Legal Treatment

With uncertainty surrounding legal treatment of different cryptoassets and token types, it's important to understand how stablecoins are recognised by regulators. After ascertaining *what*, stablecoins actually are from the perspective of regulators, we can understand how stablecoin issuers are regulated.

Especially with recent Securities and Exchange Commission (SEC) enforcement against ICOs as unregistered securities, and against unregistered securities exchanges, properly navigating regulatory waters is imperative.[45]

Intuitively, stablecoins seem to lack the definitive signs of a security, as they are expressly meant to do anything but appreciate (or depreciate). Specifically, a rational user does not purchase stablecoins with the expectation to profit from a third party's enterprise and success.[46] Success would in fact preclude it from being a good investment.[47]

Because stablecoins are meant to be money, they much more resemble currencies and, in some cases, commodities. The operative concept is that stablecoins (at least fiatcoins) are simply digital representations of off-chain assets. If those assets are currencies or commodities, so must be the tokenised versions. If not treated as currencies directly, they can be treated as vehicles which represent the currency — as in prepaid instruments. Indeed, below we analyse how specific jurisdictions are treating fiatcoins,and see that a theme of prepaid instruments is evolving.

Regulatory bodies have begun forming consensus that treatment is based on the target asset, not tokenisation thereof. The UK FCA has recently stated that, "The regulatory status of an asset or activity should not be affected by the use of DLT [distributed ledger technology] and the process of tokenisation, provided that doing so does not change the financial risk characteristics of the asset or the legal title to the underlying asset. If an existing asset is regulated, representing it as a token using a DLT platform should not change its regulatory status. However, the use of DLT may change the way in which regulation applies. For example, there may be differences in the systems and controls that a firm needs to have." [48]

[44] MKR Tools. Accessed December 10, 2018. https://mkr.tools/cdps/all
[45] "Cyber Enforcement Actions." SEC. June 20, 2017. Accessed November 17, 2018. https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.
[46] Reiff, Nathan. "Howey Test." Investopedia. March 13, 2018. Accessed November 17, 2018. https://www.investopedia.com/terms/h/howey-test.asp.
[47] There are scenarios where there is a dual or tri token model in the stablecoin system, such as seigniorage shares, where the non-stable tokens may possess some equity-like features.
[48] "Cryptoassets Taskforce: Final Report." October 2018.

5.2 Current Regulatory Environment

Traditionally, for an enterprise to operate with full legality and compliance means adhering to the laws and regulations of where the enterprise is based, and how it interacts with its customers and business partners.

With the emergence of the digital economy, and in the context of stablecoins, we are faced with a global regulatory environment, in the sense that the issuance and use of stablecoins and similar class of digital asset oftentimes extend to more than one legal jurisdiction.

At the time of writing this paper, there is as yet no dedicated laws and regulations for stablecoins; regulators of many jurisdictions have merely extended current regulations governing banking, securities and other financial services areas (such as payments) to this emerging domain.

Despite this, in September 2018, two new stablecoins obtained conditional approvals from the New York State Department of Financial Services (NYDFS) [49] in the U.S. In Japan, the Financial Services Agency (FSA) [50] [51] granted self-regulatory status to the cryptocurrency industry in October, and at the same time indicated that stablecoins are not cryptocurrencies as defined under the Fund Settlement Law and the Payment Services Act — legislations that cryptocurrency companies currently need to follow. In Hong Kong, the Securities and Futures Commission (HKSFC) announced new regulatory approach for virtual assets on 1 November 2018.[52]

In the following sections, we provided an overview on the latest regulatory approach for Hong Kong, U.S. and Japan as it relate to stablecoins. Around the world, regulators are divided on the subject of cryptocurrencies, and the emergence of stablecoins will inevitably add new dimensions to the discussions.

5.2.1 Hong Kong

To date, Hong Kong's regulatory stance towards stablecoins has not been fully clarified. The HKSFC has previously applied securities and futures regulation on "virtual assets" that fall within the legal definition of "securities" or "futures contracts".[53] However, given their nature, it is unlikely that stablecoins will be treated as such instruments, and thus, unlikely to be subject to HKSFC oversight and licensing. The HKSFC has indeed mentioned that they will abstain from regulating virtual assets which it deems to lie outside their securities and futures contracts domain.[54]

The HKSFC believes the crypto space moves too fast to fully pin down newly constructed legal frameworks, and will instead require creativity and collaboration for effective regulation.[55] Showing their willingness to adapt with this emerging asset class, on November 1st, 2018, the HKSFC announced that they shall allow willing virtual asset trading platform operators to be placed into the SFC Regulatory Sandbox.[56] The sandbox enables experimentation with emerging financial technology that does not necessarily fall within current regulatory frameworks. When applicable regulation of a financial technology is lacking, it may be applied in select scenarios with qualified investors. Under more meticulous monitoring and exploration from the SFC, operations are iterated upon until decided that risk can effectively be mitigated in a wider range of applications, at which point a license may be granted.[57]

Stablecoins, however, may be another animal altogether and not fit within virtual asset frameworks nor sandboxes. Regulatory treatment depends on what exactly a stablecoin is interpreted to be, and thus far, one likely candidate is a "Stored Value Facility" (SVF). According to the *Payment Systems and Stored Value Facilities Ordinance*, an SVF is a facility (instrument) that "may be used for storing the value of an amount of money...that may be used as a means of making payments for good and services or payments to another person."[58]

Interestingly, two types of SVFs are recognised: device based SVF and non-device based SVF. Non-device based SVFs are also referred to as network-based SVFs. Network-based SVFs are further defined as: "value is stored on a network-based account which can be accessed through the internet, a computer network or mobile network Examples include internet-based payment platforms which provide "network-based accounts" with which users can store value for making payments for online purchases, or for person-to-person funds transfers."[59]

With these definitions and distinctions, we find it intuitive that stablecoins are properly captured as a network-based SVF.

Businesses involved in the issuance of SVF are subject to licensing administered by the Hong Kong Monetary Authority (HKMA). The licensing regime seeks to ensure the soundness of SVF operations and adequacy of the "float" to protect users' stored value. The HKMA not only decides whether an SVF licence should be granted, but also conducts ongoing supervision of licensees and opens investigations when needed.

[49] https://www.dfs.ny.gov/about/press/pr1809101.htm
[50] https://www.reuters.com/article/us-japan-cryptocurrency/japan-grants-cryptocurrency-industry-self-regulatory-status-idUSKCN1MY10W
[51] https://thenextweb.com/hardfork/2018/10/29/japan-stablecoins-not-cryptocurrencies/
[52] https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR126
[53] Alder, Ashley "Fintech: Meeting the regulatory challenges". Keynote speech at Hong Kong FinTech Week 2018. November 1, 2018. https://www.sfc.hk/web/EN/files/ER/PDF/Speeches/Ashley%20HK%20FinTech%20Week.pdf
[54] ibid.
[55] ibid.
[56] Securities & Futures Commission of Hong Kong. "Statement on Regulatory Framework for Virtual Asset Portfolios Managers, Fund Distributors and Trading Platform Operators." November 01, 2018. https://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/reg-framework-virtual-asset-portfolios-managers-fund-distributors-trading-platform-operators.html.
[57] Securities & Futures Commission of Hong Kong. "Circular to Announce the SFC Regulatory Sandbox." September 29, 2017. https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC63.
[58] Hong Kong Monetary Authority. "Explanatory Note on Licensing for Stored Value Facilities". November 2015 https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/retail-payment-initiatives/Explanatory_note_on_licensing_for_SVF.pdf
[59] ibid.

It's worth noting that certain types of SVF, notably a single-purpose SVF, such as gift card vouchers, are not subject to the licensing regime. Exemptions also apply for SVFs which are not single-purpose, but pertain to instances such as bonus rewards or loyalty points. Stablecoins, as we have defined them in this paper, are mostly concerned with being a general purpose and ultimately usable currency, and seem to fall within the SVFs that require licensing.

In Hong Kong's attempt to remain an international finance center, they have streamlined overlapping laws, such as those regarding a Money Service Operator (MSO). To enable SVF to handle cross-border remittance and redemption in foreign currencies, the HKMA has stated that SVF licensees are not required to separately obtain an MSO license, but instead able to carry out MSO business as part of their activity.[60]

Minimum requirements to qualify for an SVF license surround a few important topics:[61]

- The operation of a stored value facility must be the principal business of the company;
- Must have share capital of no less than HK$25,000,000.00;
- Must have adequate control systems to ensure that the HKMA is kept informed;
- The CEO, directors and controller of the company must be a fit and proper person to hold the position

That being said, the HKMA has, as yet, made no formal ruling on the applicability of the SVF regulatory regime to stablecoins, and no licence has yet been granted to stablecoin operators.

5.2.2 United States

In the U.S., stablecoin issuers are interpreted to perform functions that are similar to certain types of cryptocurrency exchanges. As noted by Coin Center, cryptocurrency exchanges are generally regulated as money transmitters by state licensing authorities and must register as Money Service Businesses (MSBs) at the federal level with the Financial Crimes Enforcement Network (FinCEN).[62]

Although the definition of a money transmitter varies by state, it is generally similar to the federal definition of MSBs, which pertains to entities performing activities involving "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[63]

MSB status largely depends on custody — who is in control of client or participant assets. Fiat-backed stablecoin issuers do accept custody of deposits, either directly or through third party banks in order to collateralise and create the coin. As such, it's intuitive that fiatcoin issuers are regulated as MSBs, and must register to earn the right to perform certain activities, such as money transmission (activity 409), or provide access to prepaid services (activity 414).[64]

While there is considerable overlap between cryptocurrency exchanges and fiatcoin issuers, there is an important distinction to be made between exchanges that offer trading of cryptocurrencies which are deemed non-securities (BTC, ETH), versus those that offer trading of tokens that are (or may be) securities.

Current implementations of fiatcoins have been interpreted to not resemble securities. According to TrustToken, issuer of TUSD, they are more akin to deposit and safekeeping receipts, which the SEC has previously recommended no enforcement actions against.[65] Paxos seconds that sentiment, and according to their legal counsel, the Paxos Standard stablecoin (PAX) does not meet the definition of a security under either the Securities Act of 1933 or the Securities Exchange Act of 1934.[66]

Cryptocurrency exchanges trading assets that do qualify as securities according to the Securities Act of 1933 and Securities Exchange Act of 1934 are regulated as securities exchanges by the SEC — not purely as money transmitters by FinCEN.

At the state level, New York's regulator, the Department of Financial Services (DFS), has taken an active stance in regulating and licensing virtual currency businesses. DFS oversees and grants licenses related to Virtual Currency Business Activity, known as the BitLicense.[67] The BitLicense is needed for a business performing any of a multitude of activities with virtual currencies, such as transmission, exchange, buying/selling, storing, and importantly for stablecoins, issuing and administering. DFS has thus far granted fourteen licenses for virtual currency businesses.

In addition to the BitLicense, DFS regulates further financial services innovations by licensing technology-based money transmitters under NY money transmitter law, and authorises businesses to act as limited purpose trust companies under NY State Banking Law. With this combination of licenses, an issuer would have all the requisite regulatory clearance to issue and operate a stablecoin, but still needs explicit permission from the regulator.

[60] "Hong Kong Stored Value Facility License — Updated 2018." OffshorePremium.com. Accessed November 21, 2018. https://www.offshorepremium.com/2018/01/hong-kong-stored-value-facility-license-updated-2018/.
[61] ibid.
[62] Van Valkenburgh, Peter. "What can the EtherDelta settlement tell us about how decentralized exchanges are regulated?". Coin Center. November 8, 2018. https://coincenter.org/entry/what-can-the-etherdelta-settlement-tell-us-about-how-decentralised-exchanges-are-regulated
[63] FinCEN. "Subject: Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform" October 27, 2014. https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf
[64] MSB Registrant Search, FinCEN. https://www.fincen.gov/msb-registrant-search
[65] TrueUSD. Q&A. Accessed November 29, 2018 https://medium.com/hbus-official/hbus-q-a-with-rafael-cosman-of-trusttoken-creator-of-the-trueusd-tusd-stablecoin-9f0095043eff
[66] "FAQ." Paxos. Accessed November 21, 2018. https://www.paxos.com/standard/faq/.
[67] NYDFS. "Information and Resources for Virtual Currency Business Activity (BitLicense)." NY Department of Financial Services. Accessed November 21, 2018. https://www.dfs.ny.gov/banking/virtualcurrency.htm.

DFS has approved both Gemini Trust Company LLC and Paxos Trust Company LLC to offer USD-backed stablecoins, the Gemini Dollar (GUSD), and Paxos Standard (PAX), respectively.[68]

The approvals are based on strict requirements for these products, some of which include:

- Ensure that authorised stablecoins are fully exchangeable for a U.S. dollar, with conditions to ensure monitoring and recordkeeping.
- Implement, monitor and update effective risk-based controls and appropriate BSA/AML and OFAC controls to prevent the Gemini Dollar or Paxos Standard Token from being used in connection with money laundering or terrorist financing.
- Implement, monitor and update effective risk-based controls to prevent and respond to any potential or actual wrongful use of stablecoin, including but not limited to its use in illegal activity, market manipulation, or other similar misconduct.
- Compliance with DFS's transaction monitoring and cybersecurity regulations.
- Post terms and conditions in a prominent location on both Gemini's and Paxos's respective websites, and in any other form or manner required by DFS, that warns consumers that:
    - Any stablecoin and/or the fiat currency available upon redemption of any stablecoin may be forfeited if the stablecoin has been, or is being used for, illegal activity
    - Any stablecoin may be subject to forfeiture to, or seizure by, a law enforcement agency in the event that there is a legal order or other legal process
    - Any stablecoin or fiat currency available upon exchange of stablecoin that has been subject to freezing, forfeiture to or seizure by a law enforcement agency, and/or subject to any similar limitation on its use, may be wholly and permanently unrecoverable and unusable and may, in appropriate circumstances, be destroyed
- Maintain policies and procedures for consumer protection and to promptly address and resolve customer complaints.

Besides NY DFS regulated stablecoins, there are other compliant issuers in the U.S. TrueUSD, issued by TrueCoin LLC (commercial name TrustToken), is a USD-backed coin subject to regulation by FinCEN as an MSB. As such, it must comply with the Bank Secrecy Act, and the accompanying KYC/AML, anti-terrorism financing, and OFAC regulation.[69]

Legal protection for TUSD token holders is provided with funds held in escrow by independent trust companies and fiduciaries, Prime Trust LLC and Alliance Trust Company LLC. Given that these trust partners are regulated by the Nevada Department of Business and Industry (DBI), TrustToken is also required to comply with DBI regulation. Specifically, TrustToken is obligated to exchange TUSD for USD, enforceable by trust law of the Nevada DBI.

5.2.3 Japan

In Japan, the Financial Services Agency (FSA) recently concluded that stablecoins should not in fact be treated as 'virtual currencies' (cryptoassets).[70]

The supporting legislation stems from the amendments to the Fund Settlement Act, which perceives virtual currencies as means of payment, affording them, amongst other things, exemptions from consumption tax. Simultaneous amendments to the Payment Services Act added for the regulation and licensing of virtual currency related businesses, such as exchanges.

According to the FSA's interpretation of the Payment Services Act, stablecoins backed by fiat currencies do not meet the definition of virtual currencies. Instead, companies may need to register as an issuer of 'Prepaid Payment Instruments' or as 'Funds Transfer Service Providers'.

Prepaid Payment Instruments are distinguished by whether they pertain to services procured by the issuer itself, or for third parties. Funds Transfer Service Providers are able to facilitate fund transfers for up to one million yen, with transactions greater than this amount only being performed by companies with a banking license.

It's instructive to note how the frameworks have evolved on this issue. Initial enactment of the Payment Services Act in 2010 was crafted to deal with electronic chip-based cards issued by transit companies and the like.[71] An amendment in April 2017 provided for virtual currency regulation. In this light, we can see how these instruments may be a forebear to virtual currencies, providing access to a network's good or service.[72]

Japan's current regulatory environment means that stablecoin issuers — apart from being prepaid payment instruments issuers and funds transfer service providers — are more likely to be applying for banking licenses than virtual currency exchange licenses. Stablecoin issuers are found to be dissimilar to virtual currency ICO issuers or ancillary virtual currency business operators.

Regulation of virtual currency exchanges and assets has been placed under the purview of the self-regulatory agency, Japanese Virtual Currency Exchange Association (JVCEA).[73]

[68] NYDFS. "DFS continues to foster responsible growth in New York's fintech industry with new virtual currency product approvals." NY Department of Financial Services. September 10, 2018. Accessed November 21, 2018. https://www.dfs.ny.gov/about/press/pr1809101.htm.
[69] TrueUSD. "TrueUSD Regulatory / Compliance Policies." Accessed November 25, 2018. https://www.trusttoken.com/regulatory-compliance/.
[70] Helms, Kevin. "Japanese Regulator: Stablecoins Are Not Cryptocurrencies Under Current Law." Bitcoin News. October 29, 2018. Accessed November 25, 2018. https://news.bitcoin.com/japanese-regulator-stablecoins-cryptocurrencies/.
[71] "Japan's Financial Services Agency Set to Update Cryptocurrency Regulations in Speculation Countermeasure." The Japan Times. August 8, 2018. Accessed December 2, 2018. https://www.japantimes.co.jp/news/2018/08/08/business/japans-financial-services-agency-set-update-cryptocurrency-regulations-speculation-countermeasure/.
[72] "FinTech Support Desk." シティバンク在日支店に対す...：金融庁. July 17, 2018. Accessed December 2, 2018. https://www.fsa.go.jp/en/news/2018/20180717.html.
[73] JVCEA. Accessed December 2, 2018. https://jvcea.or.jp/about/

5.3 KYC/AML

Being regulated according to any of the above jurisdictions or regimes requires businesses to have a comprehensive understanding of their customers, and a program in place to mitigate risks.

In the U.S., for example, to be regulated by FinCEN, one must satisfy requirements for the Bank Secrecy Act (BSA), and associated Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.

For fiat-backed coins, KYC and BSA-AML programs are meant to establish and verify customer identities to prevent the issuer from dealing with customers it is not allowed to; namely, those who may be using the stablecoin to evade national and international banking laws, launder money, or perform other nefarious acts.

These requirements are addressed by requiring users to make an account with the issuer, and passing through their identity verification and diligence process. This can be performed by the issuer themselves, but is more often than not outsourced or coordinated with professional third-party identity verification services.

TrueUSD, for example, collects the following information from potential customers (individuals or businesses, domestic or international): [74]

- Legal Name (Individual or Business)
- Date of Birth (Individuals)
- Physical Address Identification Number (SSN, TIN, Passport Number, Foreign Alien ID Number)
- Email Region of Formation (Business)
- Articles of Incorporation (Business)
- Organization Authorization Document (Business)
- Beneficial Ownership Information (Business)

If the information provided does not match the information on file with third-party verifiers, the person or business will not be cleared, and further due diligence is performed prior to any clearance. Identities are also cross-checked against government watchlists. Issuers have the ability to reject any individual or business failing to meet the required standards.

In current fiatcoin implementations, KYC/AML is enforced at issuance (token creation) and redemption (token burning). At these entry and exit points, a user initiates a wire from/to their bank account, to/from the issuer's specified bank or trust account. Thus, KYC/AML is essentially applied when interfacing or connecting with traditional financial institutions. Funding and redemption can usually only be performed with funds and accounts held in the name of the user.

For regular transmission of a fiatcoin, KYC/AML is not expressly enforced — it is just a typical Ethereum token transfer (see GUSD in section 6.2). However, blacklisted addresses can be labelled, monitored and avoided.

Recently, the US Treasury Department enforced its first sanctions on cryptocurrency addresses: through its Office of Foreign Assets Control (OFAC), two bitcoin addresses suspected to belong to criminals were blacklisted, with any US person or business expressly forbidden to interact with them.[75] While a notable first step, the ease with which new addresses can be created does present a problem. However, as it relates to fiatcoins, new, unverified addresses would not be able to redeem into fiat.

Critics of the effectiveness of these enforcement measures can rightly question if KYC/AML at only entry and exit points is sufficient in a world where a substantial portion of economic activity may exist and be transacted within these networks. Such systems result in a meaningful reduction of surveillance capabilities versus legacy centralized systems where accounts cannot be as trivially and infinitely created.

However, KYC is also done elsewhere in the economic circuit, such as on (some) exchanges. Of the top 100 exchanges by volume, just under half impose strict KYC requirements, while more than a quarter do not require KYC at all. The remaining quarter are exchanges that impose KYC for clearance of certain activities, such as greater withdrawal limits, or crypto to fiat trading.[76]

The gating of entry and exits leaves many stablecoin supporters and privacy enthusiasts suspicious about 'last-mile' anonymity solutions. Is there a way to preserve privacy at both ends of the fiat on/off ramps? Failure to preserve this privacy can hinder an asset's 'moneyness' and utility, and may expose users to predatory tactics by powerful platforms. There are hopes for new solutions using advancements in self-soveriegn identity and
other approaches.

In addition to the creation of KYC/AML internal control programs, an issuer should have a designated person to oversee the program day-to-day, and provide education and training to appropriate personnel regarding the program. In the U.S., MSBs are required to obtain annual third-party audits of their KYC/AML policies and procedures.

Proper KYC/AML processes are helpful specifically for the institutionalisation of the crypto space; regulated fiatcoins are an easy and compliant onramp for the institutions who have remained on the sidelines. Besides being an onramp for them, it ensures that the pool of counterparties who make up the other sides of their trades are also compliant and KYC'd, and up to par from a regulatory perspective.

[74] TrueUSD Regulatory / Compliance Policies. Accessed December 2, 2018. https://www.trusttoken.com/regulatory-compliance/
[75] "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses". US Department of the Treasury. November 28, 2018. Accessed December 3, 2018. https://home.treasury.gov/news/press-releases/sm556
[76] CryptoCompare Exchange Report. October 2018

5.4 Technical Design & Enforcement

The first and most important technical decision for stablecoin issuers to make is on which platform their coin should be deployed. Thus far, with the exception of Tether — which is deployed on Omni Layer (a protocol built on the Bitcoin blockchain) — all stablecoins previously mentioned are deployed on top of the Ethereum blockchain as ERC20 tokens.[77]

By choosing to follow the ERC20 token standard — the standard that ignited the ICO boom — these assets can be sent and stored by any Ethereum address. As such, ERC20-compliant stablecoins benefit from a widespread ecosystem of wallets, applications, and other supporting tools. From day one, any ERC20 stablecoin inherits an impressive network of products and services meant to 'speak its language', and perhaps more importantly, inherits users as well..

From a development standpoint, these tokens also waste little (or no) resources in designing their own standards or tinkering with unfamiliar interfaces and smart contracts. Indeed, besides adhering to the standard, issuers can make use of even more developed templates or packages to deploy their token; this was the case with CENTRE building their USDC on top of ZeppelinOS, a smart contract development platform.[78]

As regulated issuers, technical designs are needed that provide the ability to upgrade fiatcoin smart contracts. Reasons for doing so may include the need to resolve vulnerabilities, build new features, and, notably, block or reverse token transfers in response to security incidents, or if legally pressured to do so by court order.

Upgrading smart contracts, however, is no trivial task. As CENTRE noted in their development of an upgradeable USDC Ethereum contract: "Ethereum lets anyone put code on the blockchain. Ethereum assigns the code an address, and anyone can call functions on the code stored at that address. No-one can ever change the code at a particular address, not even the owner. Software upgrades have to be done using address pointers and redirection techniques."[79] In their case, CENTRE decided to use the aforementioned ZeppelinOS contract to employ an upgradeable proxy pattern.

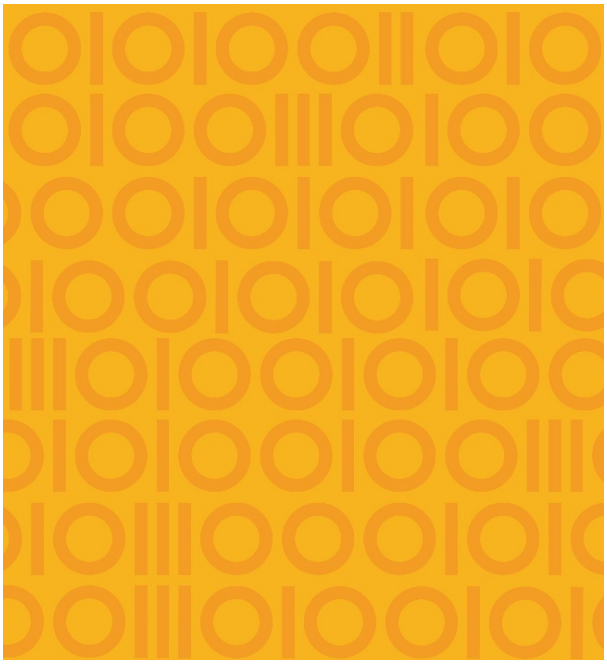
Regarding the ability to centrally control the system of smart contracts, Paxos states that they will never give law enforcement control of the smart contract private keys, which are held by Paxos in high security. While Paxos does have the ability to freeze and seize tokens, they have labeled the relevant code to make it clear that they would only use this functionality if required by law. As a regulated trust, illegal activity is of course prohibited, and if determined after investigation that certain PAX have been used for illegal activity, such PAX and the US dollars backing them may be forfeited.[80]

Along with centrally-controlled contracts, minting mechanics are an important part of the technical design and user experience, with users unwilling to wait a long time to tokenise their fiat. TUSD recently announced halving their minting time to 6 hours once a wire settles. There is also often a set schedule for creation and redemption of tokens to and from fiat. This is not as automatic nor immediate as simple token transfers since (1) this interfaces with legacy financial institutions and their banking hours, and (2) because the crypto assets (private keys) are held in cold storage (offline) for maximum security.[81]

Notably, similar key management solutions meant to provide checks-and-balances are implemented when tokenising a cryptoasset from one chain to another. One such project is Wrapped Bitcoin (WBTC), a design to bring bitcoins over to the Ethereum blockchain.[82] This will allow Bitcoin to interact with the nascent yet vast ecosystem of financial protocols populating Ethereum, such as decentralized exchanges. With this schema, bitcoins are 'wrapped' in an ERC20 interface according to a network of maintainers who collectively control a multisignature contract and approve members to issue, redeem, and custody BTC and WBTC.

Such a solution of porting one cryptoasset to another platform leads to an interesting question of which blockchain transaction model — namely, account-based (Ethereum) or UTXO-based (Bitcoin) — is better for a stablecoin, or if there are practical/legal differences at all. Particularly pertinent is if proving ownership of an 'address' is equivalent on both architectures.

Another technical consideration is 'fork management'. Given blockchains are liable to split in two or more directions (and indeed Bitcoin and Ethereum both have), stablecoin issuers need a contingency plan on how to treat the resulting chains. For TrueUSD, in the event of an Ethereum fork, the 'non-chosen' fork will not be valid for any purpose and TUSD thereon shall be frozen.[83]



[77] Tether has actually secondarily deployed USDT on Ethereum as well.
[78] Burniske, Chris. Twitter. October 25, 2018. Accessed November 29, 2018. https://twitter.com/cburniske/status/1055477902995832832.
[79] Belenkiy, Mira. "Designing an Upgradeable Ethereum Contract — CENTRE Blog". September 26, 2018. Accessed December 5, 2018. https://medium.com/centre-blog/designing-an-upgradeable-ethereum-contract-3d850f637794.
[80] "Use for Illegal Activity Prohibited." Paxos. Accessed December 6, 2018. https://www.paxos.com/standard/pax-illegal-activity-prohibited/
[81] "FAQ." Paxos. Accessed December 6, 2018. https://www.paxos.com/standard/FAQ/#schedule
[82] Wrapped Bitcoin. Accessed December 1, 2018. https://www.wbtc.network/
[83] TrueUSD Terms of Use. Accessed December 1, 2018. https://www.trusttoken.com/terms-of-use/

6. A Trust Framework for Fiat-backed Stablecoins

The new class of fiatcoins have trustworthiness and regulatory compliance as a main selling point. They shine a bright light on their regulated status and fully-backed, professionally audited reserves held at prominent third-party trust companies. These fiatcoin issuers are effectively signalling a commitment to high standards — subjecting themselves to strict oversight — in order to engender the belief in users that they and their coin are not going anywhere.

In a somewhat surprising sense, this costly signalling is quite similar to what 'backs' Bitcoin: proof of *work*.

Why would fiatcoin issuers spend the time, money, and effort attaining the licensing and building their system if they were not going to stick around and operate it as described? For the same reason, we would argue, that Bitcoin miners spend tremendous resources in capital and operating expenditures (hardware and electricity); to reap the rewards over time. This proof of work, it so happens, is why we already innately trust our banks: they expend tremendous resources to help us understand that they are honest, and expect to be here when we come back tomorrow. Their marble floors and accoutrements are simply a costly signal that they have put in the work.[84]

With fiatcoins, honesty pertains to a rather straightforward promise: there is 1 unit of fiat currency in a bank account for every digital unit in existence, and, crucially, any fiatcoin holder can convert their digital asset for its analog at any time. This convertibility is the crux of the system. It's simple to understand and can only reasonably fail if (1) the collateral is not pegged 1:1, or (2) there is some restriction upon redemption, be it issuer, custodian, or government imposed.

Whatever (slight) deviation from 1:1 may occur on a daily basis is not the real risk — the real risk is binary: the system breaks in catastrophic manner, and the stablecoin approaches 0.

As previously mentioned, 2018 saw multiple reputable institutions become keenly interested in issuing digital dollars. These issuers garnered support from traditional financial partners to bootstrap and buttress the requisite trust. We will examine five such issuers and their fiatcoins.

With an understanding of how current issuers have brought their fiatcoins to market, we propose a trust framework for evaluating fiat-backed coins. This trust framework is equally applicable for other types of off-chain collateralised stablecoins.

6.1 Trust Framework

Designing and issuing a fiat-backed stablecoin is an exercise in trust as much as technology. As such, the below trust framework contends that creation of a fiatcoin rests on exposing the entire system to as much regulatory oversight as possible. The fiatcoin trust framework recognises seven crucial components.

0. Issuing Entity's Corporate/Legal Structure

- What is the structure of the issuing entity?
  - Trust company, etc.
- In what jurisdiction(s) do they operate?
- Is it one company or a consortium/network?

1. Regulator and Applicable Laws

- Who regulates the issuer?
  - State regulators, Federal, Self-regulatory organisation
  - NYDFS, FinCEN, etc.
- What are the applicable laws?
  - BSA, NY State Banking, etc.

2. Custodian and Banking Relationships

- Does the issuer take custody of the deposited funds, or is it an independent third party?
- Are funds held by one bank or many?
- Are the institutions holding funds qualified trustees/ custodians?
  - Do they hold the funds as a fiduciary, in escrow, in segregated accounts?
  - Can they reinvest the assets? In illiquid securities?
  - Are reserves held in full? Or are fractional reserves allowed?

3. Independent Auditor

- Who is the the independent auditor attesting to adequacy of reserves?
  - Reputable accounting firms should be used to inspire trust
- Full audits or just attestations?
  - What level of assurance is provided? [85]
  - Does it follow AICPA Attestation Standards?
- How often are attestation of funds performed and presented?
  - Quarterly, monthly or bi-monthly attestations [86]

4. Smart Contract and Technical Design

- What blockchain is the asset issued on?
  - If on a popular blockchain, does it conform to ubiquitous token standards?
- Is the smart contract designed in such a way to protect users from issuers?
  - Are there features in place which mitigate issuer's arbitrary power?
  - Timelocks and multisignature requirements to ensure contracts can't be changed or upgraded on a whim.
- On the other side of the power spectrum, do issuers have enough control?
  - Can they blacklist addresses and prevent nefarious actors from moving funds?

[84] Incentives Despot. "What Is Bitcoin Backed By?". August 23, 2018. Accessed December 1, 2018. https://medium.com/@DrSammyD/what-is-bitcoins-backing-the-same-as-marble-floors-f224413f7999.
[85] De, Nikhilesh. "Circle's Dollar-Tied Stablecoin Fully Backed, Auditor's 'Attestation' Says." CoinDesk. November 21, 2018. Accessed December 6, 2018. https://www.coindesk.com/circles-dollar-tied-stablecoin-fully-backed-auditors-attestation-says.
[86] TrustToken. "TrueUSD Attestation Reports." TrustToken. May 23, 2018. Accessed December 7, 2018. https://blog.trusttoken.com/trueusd-attestation-reports-86f693b90a4.

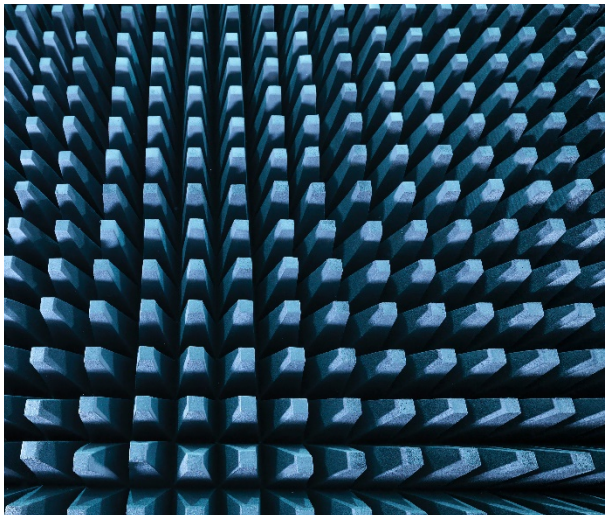
5. Independent Security Audit/Code Publicity

- Has the smart contract code been audited by a professional company?
- Is the code published publicly?
- Have their been bounties offered?

6. Insurance of Risks

- Are dollar deposits insured against unknown risks?
  - Many fiatcoins reserves are covered by FDIC (Federal Deposit Insurance Corp)
  - Excess funds above FDIC limit can be placed in short term US treasuries, etc.
  - Private insurance?

The below table summarises how five fiatcoins fare in our trust framework. It adds additional information such as minimums/ maximums for dollar-token creation/redemption, and fees.



	USDT	GUSD	USDC	TUSD	PAX
Coin name	Tether	Gemini Dollar	USD Coin	TrueUSD	Paxos Standard
Issuer	Tether Limited	Gemini Trust Company, LLC	Circle, Coinbase (CENTRE network)	TrueCoin, LLC	Paxos Trust Company, LLC
Corporate Structure	HK Limited Company	NY Trust Company	Consortium (different issuers)	Delaware LLC	NY Trust Company
Regulator	FinCEN	FinCEN, NYDFS	FinCEN, 48 US state regulators, FCA (UK).	FinCEN, Nevada DBI	FinCEN, NYDFS
Applicable Laws (i)	BSA	BSA, NY Banking Laws	BSA, E-Money Issuer (UK)	BSA, Nevada DBI Trust Law	BSA, NY Banking Laws
Custodian /Bank	Deltec Bank and Trust Limited	State Street Bank and Trust Company	Silvergate, US Bancorp Asset Mgmt	Prime Trust, Alliance Trust	Numerous US banks
Auditor (ii)	N/A	BPM, LLC	Grant Thornton LLP	Cohen & Co	WithumSmith+Brown
Attestation Frequency	N/A	Monthly	Monthly	Bi-Monthly	Monthly
Blockchain	Omni Layer, Ethereum	Ethereum	Ethereum	Ethereum	Ethereum
Security Auditor	N/A	Trail of Bits	Built on ZeppelinOS	N/A	Nomics Labs
Insurer (iii)	N/A	FDIC, Aon[87]	FDIC	FDIC	FDIC

Table notes:

I. Many issuers hold money transmission licenses in numerous US states not listed here for brevity and may be subject to other laws and regulations or have multiple corporate sub-units

II. As of this point in time, there are no internationally accepted auditing or attestation standards specifically for stablecoins, or cryptocurrencies in general. Existing reports, where issued by audit firms, leverage existing attestation standards and that adaption may vary across time and firms.

III. FDIC provides federal government insurance of up to $250,000 per depositor per bank. Issuers can deposit at multiple banks to increase coverage per user. Any uncovered amounts can be invested in short term US treasury bonds to provide a similar government guarantee. Note: Aon is insuring digital assets in custody.

[87] "Gemini Obtains Digital Asset Insurance via Aon". Business Wire. Accessed December 2, 2018 https://www.businesswire.com/news/home/20181003005283/en/Gemini-Obtains-Digital-Asset-Insurance-Aon .

At a bare minimum, the above trust framework should help answer five questions: [88]

1. Are funds held by a qualified trustee?
   a. Prevent against the risk of fraud
2. Are tokens backed by a full reserve of assets?
   a. Prevent against the risk of theft
3. Are funds adequately insured?
   a. Prevent against the risk of loss
4. Are tokens and funds audited by a reputable auditor?
   a. Instill faith everything is as stated[89]
5. Are there safeguards against financial crimes?
   a. Prevent crime facilitation and regulatory breach

Token Contracts:

USDT: https://etherscan.io/address/0xdac17f958d2ee523a2206206994597c13d831ec7 & https://www.omniexplorer.info/address/1NTMakcgVwQpMdGxRQnFKyb3G1FAJysSfz

GUSD: https://etherscan.io/address/0x056Fd409E1d7A124BD7017459dFEa2F387b6d5Cd

USDC: https://etherscan.io/address/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48

TUSD: https://etherscan.io/address/0x8dd5fbce2f6a956c3022ba3663759011dd51e73e

PAX: https://etherscan.io/address/0x8e870d67f660d95d5be530380d0ec0bd388289e1

Regulated Fiatcoin Usage Statistic as at December 24, 2018 (Data Source: etherscan.io)

Token	Addresses	Transfers
TUSD	6,091	98,258
USDC	3,976	43,274
PAX	3,504	27,477
GUSD	851	10,009

This represents on-chain data. How many addresses hold at that point in time, and how many cumulative transfers there have been.

Note: Tether excluded because its ERC20 token represents only a small portion of USDT and the OMNI USDT units would not be equivalent for comparison.

6.2 Fiatcoin Lifecycle Example

We will go through an example of fictitious 'FiatcoinX' (USDX) to illustrate the lifecycle of a regulated fiatcoin from creation to redemption.

The process for regulated fiatcoin creation and redemption is typically similar across issuers, with idiosyncrasies in implementation details.

- Alice, a new user, would like to convert some USD into USDX. She visits the FiatcoinX platform, and submits the required information for KYC/AML checks.
- Once she is cleared and her platform account is created, she wires funds from her bank account to an account specified by FiatcoinX, held at their custodian bank.
- Once the funds arrive, she 'withdraws' the USD from her FiatcoinX account specifying an Ethereum address; this mints new USDX which is sent to the specified Ethereum address, and debits the USD amount from her FiatcoinX account.
- The USDX are then operable like any ERC20 token; they can be sent to any other address (such as Bob's), or any smart contract, and can be used in any dApps, etc.
- To redeem the USDX for USD, Alice (or Bob, if he has a FiatcoinX account that has passed KYC/AML), deposits the USDX to a FiatcoinX specified Ethereum address, which are then burned, while the USD amount is credited to her FiatcoinX account.

Thus, KYC/AML is enforced upon entry and exit into the USDX system. Entry and exit is where USDX are created and burned, and also where USD and the fiat world are interacted with. What happens in between — during the life of a USDX — is quite like any other ERC20 token: it has access to the entire Ethereum blockchain, and all the corresponding benefits such as fast and cheap transactions, and interoperability with the rest of the ecosystem.

There is, however, one important and transparent caveat. If during transmission of a USDX, it becomes owned by a known nefarious actor (with a known, associated blacklisted address, for example), regulation would require that action be taken and treat those USDX just as a traditional bank would treat laundered funds in the legacy financial system. It would not be redeemable back into USD through a FiatcoinX account, and may be seized (along with the corresponding USD reserves).

To that end, the USDX smart contract likely also has a 'super user' or admin account that can enforce rules, such as freezing assets and prohibiting transfers.[90] This admin account is usually not a single account, but a smart contract with coded logic to allow for transparency and a limit on arbitrary power. The admin cannot simply alter the USDX smart contract at a moment's notice, but must affect change through a process which has time-locked delays built-in (e.g. 48 hours), and uses multisignature authorisation from keys held in cold wallets in geo-distributed locations.

[88] Purcell, Scott. "Are Stablecoins Insured? — Strongholdxchg — Medium." Medium.com. October 17, 2018. Accessed December 8, 2018. https://medium.com/strongholdxchg/are-stablecoins-insured-ce6b7cce069d
[89] CENTRE. Proof of Reserves. November 16, 2018. https://www.centre.io/pdfs/attestation/grant-thornton_circle_usdc_reserves_20181120.pdf
[90] Lebed, Alex. "Gemini can make GUSD non-transferrable at any moment (code review)". Good Audience. Accessed November 15, 2018. https://blog.goodaudience.com/gemini-can-make-gusd-non-transferrable-at-any-moment-code-review-a28d58ef6a61

6.3 Fiatcoin Business Models

For all we have learned about fiatcoins, we have only lightly touched upon what is the main motive - or main economic driver — compelling the recent stream of new issuers.

In section 3.1 on trading, we also discovered that fiatcoins enable their issuers to focus user attention on a specific set of products or services. That is, once users are familiar, trusting, and using a given fiatcoin, the issuer can more easily insert their own ancillary products to monetize. Examples include directing users towards a specific wallet, exchange, custody service, investment service, etc. This is why exchanges have been especially interested in issuing stablecoins: they are effective onboarding tools, and provide further utility on the order books. Of the five fiatcoins we examined above, only TUSD is not tied (in some way) to an exchange.

Besides aggregation of users, however, there are other more direct opportunities to monetize centrally issued fiat-backed coins:

1. Creation & Redemption Fees

When users convert from fiat to token or token to fiat, issuers can enforce a small fee. This is the most straightforward monetization method, but also the most limiting. Fees cannot be too large of a percentage without compromising the stability mechanism: a token will not be pegged exactly to the collateral if there are large fees to go in and out. Arbitrageurs will also take that into account while maintaining the peg. Obviously the goal here is to grow not only the units created (similar to AUM), but also the frequency of in/out transactions, which follows changes in demand.

	USDT	GUSD	USDC	TUSD	PAX
Fees	Yes (0.1% - 3%)[91]	None	None	Yes (0.1%)	None
Min/ Max	$100,000 minimum	$100 min redemption	$100 min redemption	$10,000 min purchase	No min redemption

Note: for all tokens, there may be fees for sending or receiving wires to/from the users' bank. This is especially the case for failed transactions.

2. Investable deposits

The deposits (fiat) held in reserve present an opportunity for issuers to earn a return. With hundreds of millions, or even billions of dollars of collateral, significant returns could be achieved with relatively low yields. Circle, for example, states that in the future, they may invest fiat funds in highly-liquid, AAA-rated fixed income securities, and generate interest on funds held in the segregated reserve accounts.[92] Of course, with fractional reserves, there is heightened risk of a mismatch in tokens to collateral, especially in potential black swan scenarios. Risk is mitigated by only investing in the highest quality and liquid assets, with matched 'duration', such as short-term treasuries. As mentioned above in relation to FDIC insurance, this can even provide enhanced protection for assets above the $250k insured limit. Again, monetization here depends heavily on the stablecoin's collateral pool size, much like traditional funds are driven primarily by assets under management (AUM).

3. Market Making

For stablecoin issuers, once the coin is in the hands of holders, utility can be much improved by providing deep and liquid markets. Especially true for exchange-issued stablecoins, that means listing it as a quote currency for multiple pairs, and making markets therein, earning the bid-ask spread. Beyond that, however, markets can also be made for the stablecoin/fiat pair itself, for example, USDT/USD, allowing users to access both sides without going through the full creation/redemption process. While this would (hopefully) be a very low volatility pair, making markets can still be profitable with high volume. It can be even more profitable with margin, and, interestingly, there are indeed exchanges offering margin trading for the stablecoin/fiat pair. Bitfinex, which shares management with Tether, recently launched USDT/USD margin trading.[93] This means arbitrageurs and market makers can lever up and earn more maintaining the peg, potentially tightening the peg in the process. It also means there is a lending market for USDT, and traders can hedge their stablecoin exposure and even go short. One consideration, however, is that issuers by no means have an exclusive right to make markets with their coin, so do face competition from other market makers.

Of course, there are numerous other potential business models and use cases for stablecoins, and all the above can be combined.

[91] Tether. Accessed December 2, 2018. https://tether.to/fees/ [89] CENTRE. Proof of Reserves. November 16, 2018. https://www.centre.io/pdfs/attestation/grant-thornton_circle_usdc_reserves_20181120.pdf
[92] Circle Support. Accessed December 8, 2018. https://support.usdc.circle.com/hc/en-us/articles/360015478191-What-is-the-revenue-model-for-Circle-USDC-
[93] Bitfinex Blog. Accessed December 23, 2018. http://blog.bitfinex.com/announcements/bitfinex-introduces-margin-trading-usdtusd/

7. Conclusion

The currencies we care about are the ones we see all around us — the ones that denominate our lives. Our affinity for any currency depends on its relative stability to however we buy, earn, and save. This, in turn, is derived from our peers, nation, and society at large feeling similarly confident and comfortable in the same.

Currency is the quantifier of our wealth and its purchasing power, and, crucially, rests on the reasonable expectation that tomorrow will not be too different than today. Failing to satisfy this credible commitment to straightforwardness simply precludes people from making rational decisions and long-term investment.

In some sense, stable currencies are the equivalent of a commonly spoken language; compulsory for coordination and cooperation.

What should be clear is that no matter the mechanism, confidence is the key ingredient in maintaining stability. The underlying means are of course important, but from a theoretical perspective, everyone's belief that a stablecoin should be worth 1 USD — and their subsequent willingness to buy/sell/convert for 1 USD — is a sufficiently self-perpetuating phenomenon to keep it stable. In fact, confidence is what keeps fiat currencies 'stable' in the first place: confidence in monetary policy, or at least confidence in the credible commitment to pursue the policy that a central bank has signalled.

For fiatcoins, the confidence is most basically a testament that there is limited counterparty risk from the issuer (or the issuer's banks). For the on-chain and algorithmic methods, it is mostly a testament to faith in the smart contracts and to users' rationality and
self-interest.

No matter the mechanism, it's exceedingly important for these issuers or developers to take their roles and stablecoins seriously; these assets may hold users' savings, not an allocation to long-shot speculation. Failure — be it fiduciary, legal, technical — could have catastrophic repercussions for token holders and the cryptoasset industry at large.

To some, there is a sentiment of saturation in the stablecoin market. It's fair to question the point of another coin worth USD$1 or HK$1. However, we believe there are useful reasons for why more can be expected, and why that's a good thing.

Chief among them is that more coins likely means reaching more people. Issuers have idiosyncrasies in pegs, geographies, platforms, compliance and marketing. Any onboarding of users into a blockchain-based world is unambiguously good for the ecosystem, especially considering the comprehension barrier. It may also mean reaching the people who need it most.

The market will also likely see many more fiatcoins in particular for the simple reason that it makes business-sense for their issuers. Given that fiatcoins have zero or negligible fees for creation/redemption, the real value it provides issuers is the ability to aggregate users, amass data, and feed them into an ecosystem of ancillary products/services such as wallets, exchanges, etc. Just like in Web2.0, aggregation theory, for better or worse, may still be a winning strategy.[94] With this in mind, we may see a different sort of centralised issuer in 2019; already pervasively popular platforms, such as Facebook or Amazon.[95]

Secondly — pertaining only to the decentralised varieties — given its difficulty, a trustless stablecoin has near mythical meaning. Designing decentralised price-stable cryptocurrencies are hard problems, and there is no reason to believe that we will get it right the first or fiftieth time; the likelihood of any solution's mid-to-long term success is probabilistically low.[96]

Finally, the greatest argument for more stablecoins is the same argument for more of anything related to building on blockchains: experimentation, especially with new forms of money. The unknown unknowns are plentiful, but the design space is much more fertile with stable units of value.

[94] Thompson, Ben. "Aggregation Theory." Stratechery by Ben Thompson. July 21, 2015. Accessed December 8, 2018. https://stratechery.com/2015/aggregation-theory/.
[95] Chaparro, Frank. FB Stablecoin. The Block. December 23, 2018. https://www.theblockcrypto.com/2018/12/23/it-would-both-be-over-rated-and-under-rated-we-spoke-to-some-of-the-top-crypto-experts-about-facebooks-reported-stablecoin-heres-what-they-said/
[96] Problems. Ethereum Wiki. https://github.com/ethereum/wiki/wiki/Problems#10-stable-value-cryptoassets

Contacts

If you are interested in knowing more, please contact our team

PwC

Andrew Watkins
China and Hong Kong Technology and Disruption Leader, PwC China
Tel: +852 2289 2716
andrew.watkins@hk.pwc.com

William Gee
Innovation and Disruption Leader, Risk Assurance
PwC China and Hongkong

Henri Arslanian
FinTech & Crypto Lead, China/HK and U.S. Liaison, PwC China
Tel: +852 2289 2490
henri.arslanian@hk.pwc.com

Duncan Fitzgerald
Financial Services Lead, Risk Assurance
PwC Hong Kong
Tel: +852 2289 1190
duncan.fitzgerald@hk.pwc.com

Chun Yin Cheung
Fintech, Cybersecurity & Privacy, Partner
PwC Hong Kong
Tel: +86 (21) 2323 3927

Loopring Foundation

Daniel Wang
Founder and CEO, Loopring
daniel@loopring.org

Jay Zhou
CMO, Loopring
jay@loopring.org

Matthew Finestone
Director, Business Development, Loopring
matthew@loopring.org

Terence Lam
Advisor, Loopring
terence@loopnest.io

About Loopring

Loopring is a blockchain research organization focusing on decentralized trading protocols. The open sourced Loopring protocol they offer provides a fundamental building block for exchanges and can be integrated into other blockchain applications that may need to manage multiple tokens. Loopring uses a combination of off-chain order messaging and on-chain settlement to ensure users maintain custody of their tokens.

pwc

LOOPRING