On the Stabilization of Stablecoins

By Caleb Clark & Blake Byrnes

Version 1.1

First drafted June 12, 2018

First published July 30, 2024

Last updated August 11, 2024

Abstract. Stablecoins are cryptocurrencies designed to solve the volatility of Bitcoin by pegging to a reference asset, most commonly the dollar. Success has been mixed. Some stablecoins have gone into death-spirals, ultimately falling to worthless. Others have managed to survive, although all have de-pegged at various points in their history.

This paper surfaces two critical issues inherent in every stablecoin known to-date.

The first is that, regardless of whether a stablecoin has so-far managed to avoid death-spiraling, every stablecoin is at a constant risk of death-spiraling due to their collateralized-asset designs.

The second issue is that the collateralized-assets underlying these stablecoins create an unavoidable systemic dichotomy: the greater their move towards risk reduction, the less decentralized their currency.

This paper argues a contrarian view within the crypto space, which is that collateralization is not only unneeded, it is harmful. A truly stable stablecoin should have zero collateral. We show that in the world of currency, collateralized assets create more negatives than benefits.

This paper also introduces a novel stabilization approach, a new type of algorithmic stablecoin that uses deterministic profit incentives to remove the possibility of death-spirals. It's a self-regulating, decentralized structure that works regardless of the market's confidence in the stablecoin.

Table of Contents

Introduction

This is the first in a series of three whitepapers on the stabilization of stablecoins. The purpose of this paper is to analyze the current market and its structural problems. It also describes broadly-defined options for fixing these problems. The final two whitepapers present detailed solutions for creating a stabler stablecoin. For an overview of the remaining papers, see Next Steps on page 25.

Stablecoins are cryptocurrencies designed to anchor their value to an external reference asset, most notably, the dollar. Their goal is to create a stable currency that holds consistent value and can be used as a global medium of exchange for everyday commerce.

The world's dominant cryptocurrency is Bitcoin. It has a market value equal to the combined value of the entire rest of the crypto industry[1]. However, Bitcoin's volatility severely limits it as a medium of exchange[2]. Stablecoins were invented to solve Bitcoin's volatility, but their results have been mixed — some have managed to hold their pegs while others have failed disastrously[3].

Asset collateralization is the primary mechanism upon which stablecoins stabilize the value of their currency. It was first used in 2014 for BitUSD[4], the world's first stablecoin, and it has been religiously followed ever since. Each subsequent team has sought to iteratively improve upon the collateral mechanism of previous stablecoins rather than use first-principles to question whether collateral has a place within stablecoin design.

The basic idea is this: regardless of whether the underlying collateral is endogenous, exogenous, or a combination of the two, collateral allows the stablecoins to operate as an IOU. The holder of the stablecoin can swap the coin on-demand for its underlying assets. In effect, this creates a stablecoin whose fundamental value does not reside in the stablecoin but in the underlying asset.

It is generally believed making a stablecoin swappable with an underlying asset gives the stablecoin holders assurance of the token's value. Unfortunately, it has the opposite effect. Although collateralization is a beneficial property of many financial instruments, such as real-estate loans, when applied to currency, collateralization introduces harmful destabilization effects that far outweigh any benefits. It opens the door to black swan events and death-spirals, and it has been the primary cause of many a stablecoin's downfall.

This paper argues the currently accepted wisdom of underpinning stablecoins with collateral is a major blind spot of the crypto industry. In fact, we believe collateralization is perhaps the industry's most fundamental mistake.

The Need for Digital Currency

Satoshi Nakamoto published his Bitcoin design[5] on a sparsely-known mailing list in 2008[6]. It was the world's first decentralized cryptocurrency, and few people paid attention, at least initially. Sixteen years later, hundreds of millions of people around the world own Bitcoin[7], and an entirely new industry now exists with over 22k cryptocurrencies and a total market capitalization of $1.69 trillion[8].

Bitcoin wasn't the first attempt to create a digital currency. The first was eCash, developed by David Chaum in 1982. Chum refined his eCash technology for many years, turning it into a company in 1989. However, his design used a centrally managed database, which required his users to have full trust his company would always honor their debts. This approach had limited value and user adoption. The company went bankrupt in 1998.

Over the following decade, multiple teams attempted to establish a functioning digital currency. However, none solved the essential elements needed for decentralization. Then Satoshi emerged.

Satoshi's desire to create a decentralized digital currency was driven by three broad ideas:

1) **The world is increasingly digital**. Over the last three decades, numerous aspects of our lives have transitioned from physical to digital, including photos, messages, documents, games, and even business meetings. One notable exception persists: money. Despite the apparent digitization of bank balances through apps, there is no true digital dollar. Financial institutions have merely crafted digital representations, which, in reality, are IOUs tied to the traditional paper currency. This hidden dichotomy results in multiple layers of concealed costs and complexities, ultimately impacting unaware consumers.

2) **Transactions are increasingly global**. People are traveling and conducting business at unprecedented rates worldwide. Despite this, the fluidity of currency faces many obstacles. Geopolitical dynamics and convoluted

regulations result in high costs and complexity of cross-border transfers.

3) **Government monetary policies are destroying value**. Money is no longer a unit of gold whose value is determined by the open market. It has become an overpriced piece of paper whose value is controlled by governments with their own objectives and incentives. The dollar, generally regarded as one of the world's most stable currencies, has seen 96% of its value destroyed over the last 100 years, which has wrought severe havoc on the savings of everyday citizens.

Satoshi realized a well-designed digital currency could solve or simplify many of the world's monetary issues.

For example, few people consider the high complexity and cost of transferring capital between two participants. There are many reason for this complexity and cost, which we won't breakdown here, but when you boil it down to first-principles, cross-border digital transfers should theoretically cost no more than mere pennies, regardless of how much capital is transacted. This is because a transfer of digital currency between two users requires little more than changing two cells in a database table. This is one of the simplest actions that can be executed in a computer system, and it's almost instantaneous to complete.

Figure 1 shows such a digital currency transfer. It only updates two fields.

FIGURE 1 — TRANSFERRING DIGITAL MONEY

Name	Value
Joe	~~75~~ 125
Sue	30
Bob	500
Amy	~~200~~ 150

50

The challenge with digital currency is determining which third-party can be trusted by the transaction participants to update the new balances. It must be handled by someone neither participant believes might accept a bribe, steal the money or pull a nefarious accounting stunt.

In a centralized system, counterparties place their trust in a single corporation or entity whose business model centers around their perceived or "branded" honesty. In contrast, decentralized systems establish trust through an interlocking mathematical structure, preventing either party from cheating without incurring greater losses on themselves. These approaches differ significantly, representing a choice between surrendering control of one's wealth and power to an unfamiliar entity or retaining sovereign control over one's own financial destiny.

Satoshi's invention of Bitcoin marked the first success of a decentralized currency. However, the system wasn't flawless: it didn't allow for instantaneous transfers, and the costs of transfers were higher than ideal. Nevertheless, Satoshi achieved the remarkable feat of creating a functioning system that operated without the need for governments, banks, or other institutions as trusted third-parties. Bitcoin was entirely digital, devoid of reliance on real-world assets or external capital. It signaled a future where individuals could assert control of their own finances, and it created an economic scenario where the deleterious effects of inflation could become a thing of the past.

The Need for Stablecoins

Satoshi's vision was to see Bitcoin become a global medium of exchange for "commerce on the Internet… without [requiring] a trusted [third-]party."

Regrettably, Satoshi's envisioned outcome has not materialized. Centralized currencies remain the dominant medium of exchange. Despite being available for sixteen years, Bitcoin and other cryptocurrencies make up less than 0.00000001% of global transactions[9]. The number of companies accepting Bitcoin is even more minuscule[10].

Although Satoshi ingeniously solved the significant challenges of getting a decentralized currency to work, he overlooked one of the most crucial aspects of what makes currency desirable for commerce: price stability.

Bitcoin's Volatility

In any given year, Bitcoin's price volatility can swing 50% or more. This makes it difficult for businesses to rely on Bitcoin as a stable currency. Figure 2 shows the last six years of volatility. If you analyze Bitcoin's price swings on a month-to-month basis, the lowest volatility was 30%. The highest was 98%. That is when viewed from the perspective of 30-day rolling snapshots; when viewed annually, the volatility is well over 600%.

FIGURE 2 — THE UPS AND DOWNS OF BITCOIN

Price volatility is fantastic for traders and speculators — volatility means opportunity — but it's terrible for users who want a general currency for everyday commerce. Users need assurance that what they earn today will be viable tomorrow. Volatile assets do not provide this assurance, which is why most merchants who accept Bitcoin immediately convert their earnings to dollars[11].

Imagine receiving your income as Bitcoin only to find the token's price plummeting several weeks later, leaving you unable to pay your dollar-denominated expenses. Figure 3 is a real view of Bitcoin's price movement from May 2021 to June of 2021, and it shows what would have happened had you tried to use Bitcoin to pay your USD rent.

FIGURE 3 — THE RISK OF BITCOIN AS A CURRENCY

The problem isn't Bitcoin per se; the problem is Bitcoin's relativity to the dollar. If everyone in the world instantly switched to Bitcoin, the volatility problem described above would theoretically disappear. If everyone used Bitcoin, your rent would also be denominated in Bitcoin, which might make Bitcoin's volatility unnoticeable. But therein lies the chicken and egg problem. How does the world move from a dollar-dominated world to a Bitcoin world? It's practically impossible for the world to switch currencies overnight without a centralized forcing function. A gradual adoption requires Bitcoin transactions to work harmoniously with the dollar for at least some period of time, but it

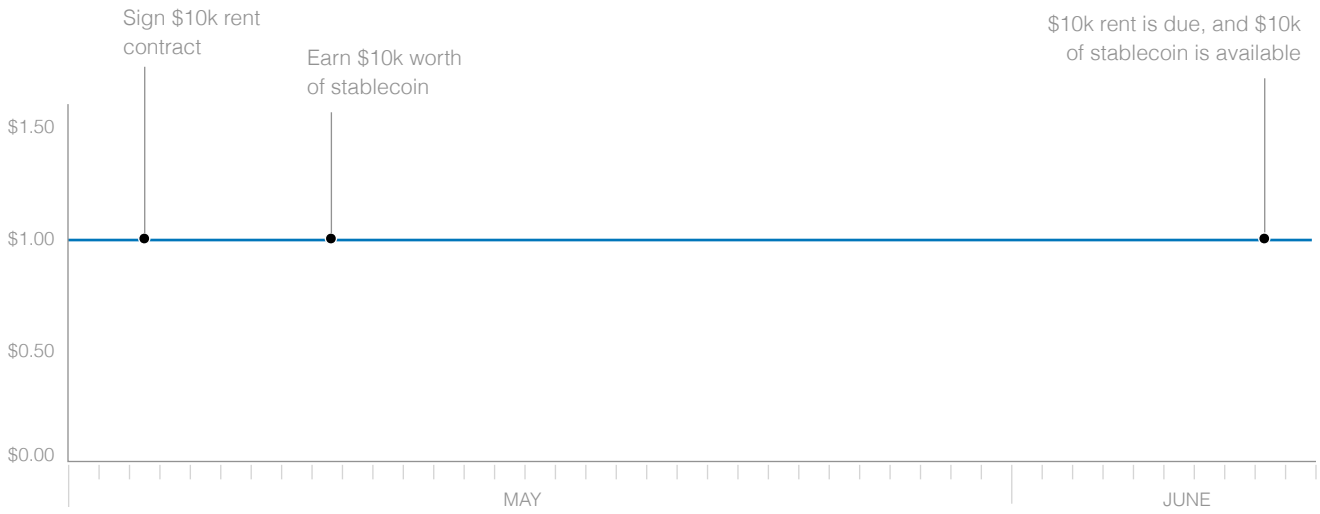
doesn't work harmoniously, as evidenced in the example above. This is why sixteen years later, Bitcoin is still used in less than 0.00000001% of the world's transactions.

Many Bitcoin enthusiasts assume the token will one day achieve price stability, if not fully, then at least enough to become a usable currency. However, no realistic plan has been proposed for transitioning from volatility to stability. It is somehow implicitly assumed that stability will occur when Bitcoin reaches a large-enough market size[12], or perhaps through a yet-undiscovered mechanism. This is naive at best and delusional at worst.

Ensuring Price Stability

Stablecoins are designed to operate as cryptocurrencies without the volatility of Bitcoin. Figure 4 shows the same rent example from Figure 3 to demonstrate how a stablecoin is expected to work.

FIGURE 4 — USING STABLECOINS AS A CURRENCY



Are stablecoins really as stable and useful as the above chart indicates? The short answer is no.

Although stablecoins appear to solve Bitcoin's volatility, they introduce several new issues.

- From a risk standpoint, stablecoins open themselves to disastrous death-spirals, which are far worse for users than any 50% drop in Bitcoin value.
- From a monetary standpoint, stablecoins have lost Bitcoin's ability to remain independent of central fiscal policies, meaning they absorb all the downsides of U.S. debt and inflation.
- From an expense standpoint, stablecoins have added multiple layers of hidden costs on top of the dollar.

The following pages address the reason behind each of these stablecoin issues. It also proposes a novel stability mechanism that is fundamentally different from what has been introduced to-date.

Current Stablecoin Usage

Most stablecoins portray themselves as the new global medium of exchange that will transform everyday commerce. Their actual usage tells a different story.

Stablecoins are rarely used for everyday commerce; their primary application is crypto trading[13]. The banking industry lacks easy on/off ramps into the crypto space, and stablecoins have stepped into this void. If you want to buy Bitcoin or other tokens, it's easier to do so with stablecoins than dollars. Similarly, if you want to liquidate some crypto and sit on the sidelines for a bit, stablecoins are the easy choice for parking.

Some retail investors also utilize stablecoins as vehicles for speculative investments. Though merely holding stablecoins doesn't yield direct returns, given their ability to maintain a stable-ish value, holders sometimes use

stablecoins within decentralized finance (DeFi) platforms. These platforms purportedly offer interest rates that significantly surpass what retail investors might achieve through conventional avenues, such as savings accounts.

Even with their limited usage, stablecoins have witnessed substantial growth over the last three years. They catapulted from a market capitalization of roughly $20 billion in mid-2020 to over $120 billion by mid-2023[14].

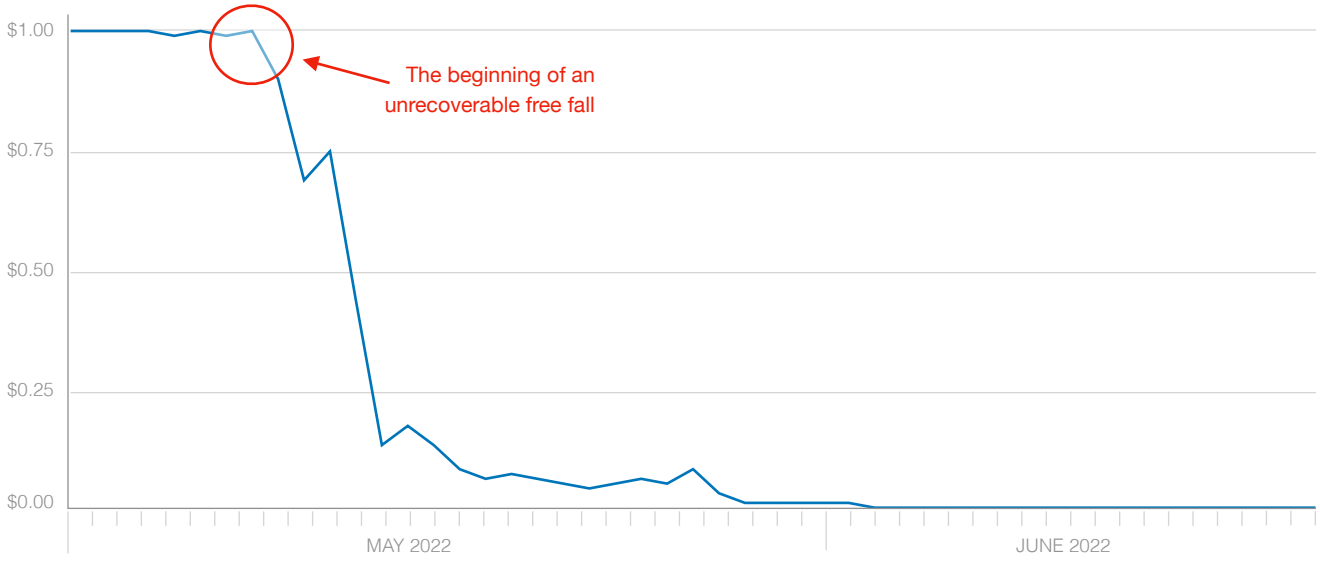
As mentioned in the previous section, stablecoins have several issues that limit their broader adoption, such as their absorption of centralized inflationary policies, hidden costs, and death-spirals. The most vivid is the death-spiral.

The Reality of Death-Spirals

There have been many stablecoins over the past ten years, and many of them have de-pegged or outright failed[15]. One of the largest flameouts was TerraUSD in the summer of 2022. The following chart shows what happened in the days immediately before and after its collapse. The team behind Terra made several attempts to stop its demise, but to no avail.

By the end of Terra's slide, over $60 billion had evaporated, and the currency was worthless[16].

FIGURE 5 — THE EPIC COLLAPSE OF TERRA USD

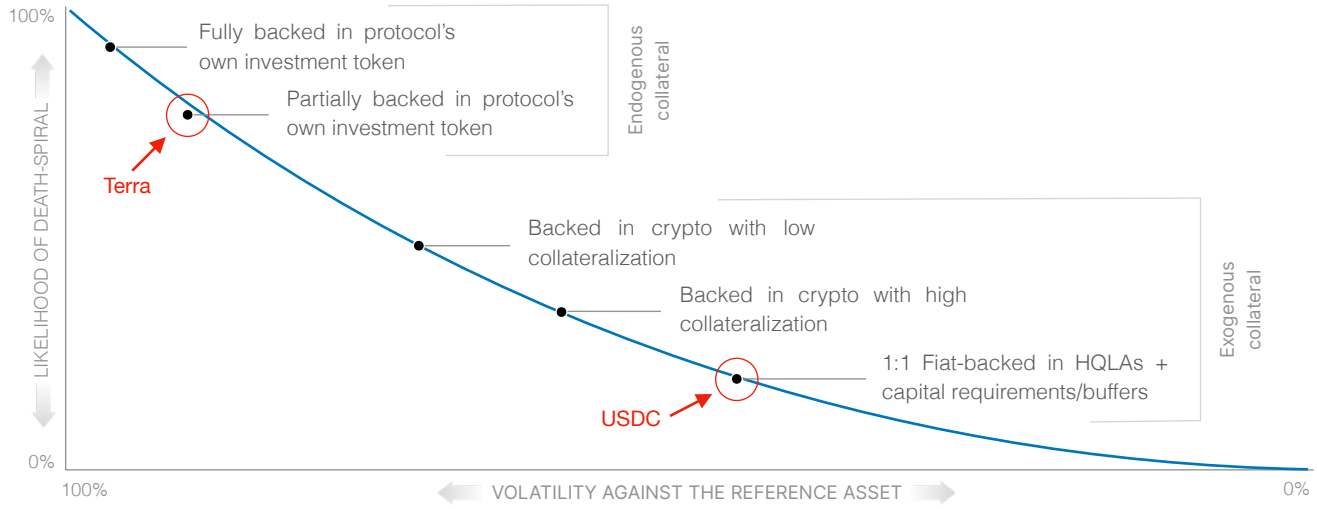


Much has been written about Terra's collapse, such as the way it used a two-token endogenous collateral structure, which helped exacerbate its fall. However, most have overlooked Terra's most devastating feature, which is that it used collateral. Few realize collateral within a stablecoin is like uranium-235 within a nuclear reactor. It is the trigger for the death-spiral, which is essentially the same as a bank run. Many within the stablecoin industry think the probability of a death-spiral is solely related to the quality of its collateral.

The Importance of Collateral Quality

Christian Catalini is a professor at MIT who wrote a widely referenced whitepaper titled *On the Economic Design of Stablecoins*[17]. It was published nearly a year before Terra's collapse, and in it, Catalini laid out arguments for why Terra would collapse. It also analyzed the various collateral types used by stablecoins and their impact on death-spirals — some collateral creates higher likelihoods. The following chart is a visual representation of Catalini's rankings. HQLAs (high quality liquid assets) are the safest.

FIGURE 6 — PROFESSOR CATALINI'S IMPACT OF COLLATERAL QUALITY AND QUANTITY ON DEATH-SPIRALS



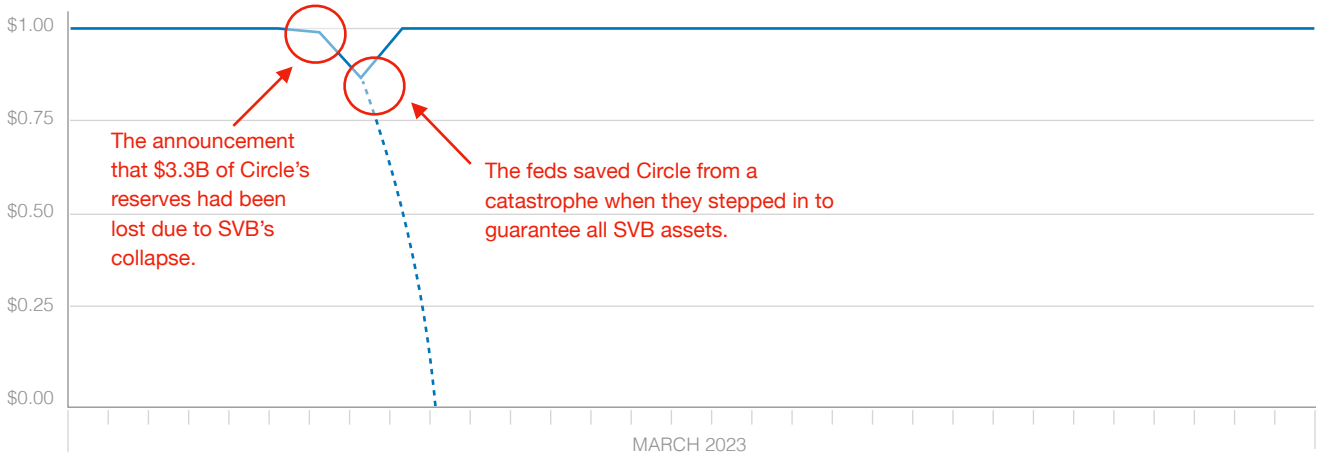
A recent whitepaper by a16z's Crypto Policy Team[18] pushes Catalini's collateral views even further. It argues "stablecoins do not fail as a result of the use of an algorithm, but rather due to collateral design", and it urges regulators to only "permit the use of over-collateralized stablecoins backed solely by exogenous [capital]."

We believe Professor Catalini and a16z are correct in that collateral-backed stablecoins need high-quality assets to improve stability and, ideally, they should be over-collateralized, regardless of the inherent capital inefficiency of doing so. However, the bigger question is, should collateral-backed stablecoins even exist? Recent evidence proves even stablecoins with HQLA collateral aren't immune from death-spirals.

Collateral-Backed Stablecoins Have a Failure Point

USDC is a top-three stablecoin by market cap[19]. It was created in 2018 through a collaborative effort between Circle and Coinbase, two prominent companies in the cryptocurrency industry. Short of it becoming a CBDC (centralized bank digital currency), USDC uses the highest quality collateral structure possible (1:1 dollar-backed HQLAs), as rated by Professor Catalini. Nevertheless, high-quality collateral didn't stop USDC from de-pegging during the Silicon Valley Bank debacle[20] in March 2023. As shown in Figure 7, USDC de-pegged from $1.00 per coin down to $0.87. It came within hours of a potential full-scale collapse before the feds stepped in to guarantee SVB's assets, thereby restoring the stablecoin's peg.

FIGURE 7 — USDC FOLLOWING THE COLLAPSE OF SVB



What would have happened had the feds not secured SVB's assets? USDC would likely have faced a death-spiral.

Circle had $44B of USDC tokens in circulation[21], and therefore the market expected Circle to have $44B of dollar-backed HQLAs in reserve. When $3.3B disappeared into SVB's black hole, only the first $40.7B of USDC tokens would be redeemable for U.S. dollars. The remaining coin-holders representing $3.3B would be left holding nothing. As with most bank runs, a rush to redeem would pressure Circle to liquidate their HQLAs faster than the market could absorb, causing a further drop in the value of USDC's collateral, thereby accelerating more losses and increasing the panic to withdraw.

The lesson from USDC's de-peg is much more than that a stablecoin's collateral should be protected to survive a bank's collapse. The real lesson is, the number of black swan events capable of destroying a stablecoins' collateral is infinite. There is no such thing as event-immunity or guaranteed capital safety. Given enough time, every stablecoin will experience situations that risk a panic run on its collateral.

Stablecoin Issuers Are Essentially Unregulated Banks

The problem of de-pegging and death-spirals is not a new phenomenon. It was not created by stablecoins or the crypto industry. It is a problem of banking, and it is as old as banking itself.

Few think of stablecoin issuers as banks, but that's effectively what they are. They perform many of the same core functions as conventional depository banks, such as enabling customers to deposit, hold, transfer, and withdraw funds on demand.

According to statute 12 USC § 1841(c)(1) of the Bank Holding Company Act of 1956[22], an institution is considered a bank if it does two things:

1) Accepts demand deposits or deposits that the depositor may withdraw by check or similar means for payment to third parties or others; and

2) Engages in the business of making commercial loans

Stablecoin issuers accept capital from "depositors" and in return they issue stablecoin tokens. Their received capital is, for all intents and purposes, in the form of demand deposits. This means depositors (i.e., token holders) can deposit and withdraw funds without prior notice. Issuers use this capital as a lending instrument to generate revenue — these investments are commonly in the form of treasury notes, money markets, and other HQLAs[23].

Figure 8 shows the high-level flow for how a bank accepts deposits, makes loans, and returns deposits.

FIGURE 8 — BASIC FLOW OF BANKS

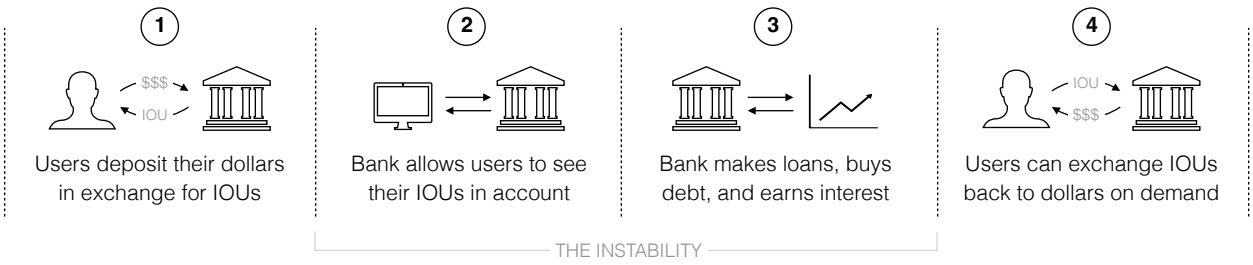
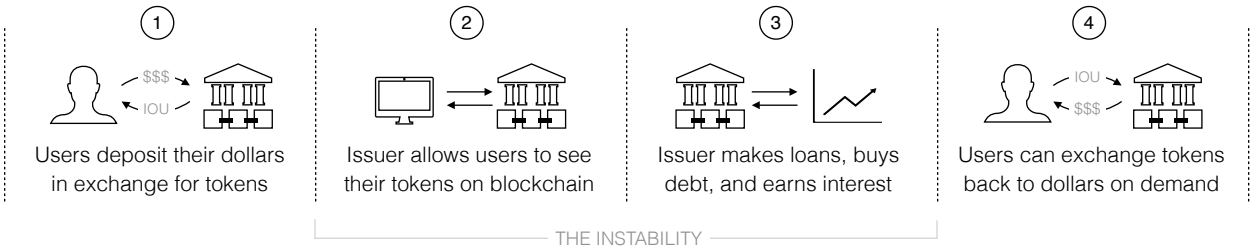


Figure 9 shows the similar high-level flow of a collateral-backed stablecoin issuer. It's nearly identical to the bank. A user deposits cash into the stablecoin issuer's organization or DAO (decentralized autonomous organization). The organization then puts those assets to work by buying debt or other assets in order to earn interest. Holders of the stablecoins can redeem their coins at par and at will for cash, just like demand deposits.

FIGURE 9 — BASIC FLOW OF STABLECOINS



Stablecoins are designed to ride the crypto payment rails, meaning they can be used to easily facilitate the buying and selling of crypto assets. Banks aren't. Nevertheless, when you drill into the core structure of what makes a bank a bank, today's stablecoin issuers are essentially unregulated banks. The primary differences are simply the terminologies and the customer interface mechanisms used.

Professors Gary Gorton and Jeffery Zhang wrote a paper called *Taming Wildcat Stablecoins*[24] that goes into great detail on this subject. It argues collateralized stablecoins are essentially a blend of demand deposit accounts and money market funds. It is only due to minor technicalities imposed by several court decisions that allow these stablecoins to side-step most of the regulatory frameworks.

Some in the crypto industry view minimal regulation as a positive[25], however, when it comes to collateral-backed stablecoins, this lack of oversight exposes stablecoin holders to the worst risks of fractional reserve banking.

Regulatory Benefits

Human nature often drives us to act in our own self-interest, and the banking industry is no exception. A research paper by Professor Dan Awrey in Cornell Law Review from 2020[26] posits that fractional-reserve banking creates by default what he calls "bad money". By bad money, he means absent tight regulatory oversight, decision makers are incentivized to do things that devalue the capital and expose it to destabilizing runs. This arises from the inherent disconnect between the promise of value (the IOU) and the actual underlying value (the assets).

It happened with banknotes in the 1800s.

It happened with deposit accounts in the early 1900s.

It happened with dollars in the 1960s and 1970s.

It happened with subprime mortgages in the 2000s.

Few if any of these situations started as greed. Many began with good intentions, but in the end, the desire for profit and power won the day. Loose regulatory environments gave those with influence a free rein to leverage unsecured loans (or poorly secured loans) in high-risk ways, much to the harm of average depositors. Sooner or later the piper comes calling, and massive amounts of value were destroyed in the panics that followed.

Professor Awrey showed how government regulation plays the critical role in turning "bad money" into "good money". By "good money" he means value that can be trusted without unnecessary friction. "Good money" regulations have evolved over hundreds of years from best practices shared across many countries. They're not perfect — far from it — however, they play a pivotal role in creating consistency, accountability, and fairness through multi-layered systems of enforceable laws, independent auditors, and insurance guarantees.

The challenge with today's stablecoins is they share the same weaknesses that created so much banking instability over the last two hundred years. At the same time, they sidestep the regulatory structures explicitly designed to solve those instabilities. As a result, holders of these stablecoins do not benefit from the government's lender-of-last-resort facilities, deposit guarantees, or special resolution regimes available to banks and, by extension, their depositors. Although in the recent case of USDC, users were indeed saved by government intervention, it was a special-situation decision that has no guarantee of being repeated.

Stablecoin Issuers Function As Nineteenth-Century Banks

The most relevant analogy for stablecoins is the Free Banking Era of nineteenth-century America. During that time, states allowed almost anyone to open a bank, and those banks were allowed to issue their own banknotes[27]. Banks were required to follow some rules but not many.

Users would take their assets to the bank — usually gold or silver. The bank would give them paper banknotes in exchange. Those private banknotes functioned as money-substitutes. They were in essence IOUs for a predetermined amount of gold or silver held by the bank. Hundreds of different banknotes circulated in any given community. Because of the different reputations of different banks, different banknotes traded at different discounts[28]. This made everyday transactions difficult to calculate, and further, panic runs on banks were quite common. These panics resulted in many banknotes becoming worthless and banknote holders losing much of their value[29].

Today's stablecoins have recreated a similar financial structure as those nineteenth-century banknotes. Issuers accept assets of value from the end-user, and in return, the user receives an IOU. The main change is, instead of paper

banknotes, stablecoin issuers hand out digital tokens. Like banknotes, these tokens have no intrinsic value. Their only value lies in the expected hope the issuer will redeem the IOUs for a pre-determined amount of dollars (or other assets) when the user requests.

It was incredibly difficult for nineteenth-century users to ascertain which banknotes were "good money." Doing so required visiting each bank to understand their management decisions and financial books. It's similar for stablecoins today. What percentage of users possess the sophistication or time (not to mention the access rights) to fully assess the decisions behind Tether and Circle's investment holdings and monetary liabilities?

The National Bank Act of 1863 effectively put an end to private banknotes by rolling everything into a national currency[30]. However, it did not end the banking panics. The panics simply shifted from banknotes to demand deposits[31]. In fact, banking panics didn't slow down for another seventy years. It took a combination of the Federal Reserve Act of 1913[32] and the implementation of federal deposit guarantees in 1934[33] to finally bring order. Today there are still banking panics, such as Silicon Valley Bank in 2023[34], but they are much fewer and farther between.

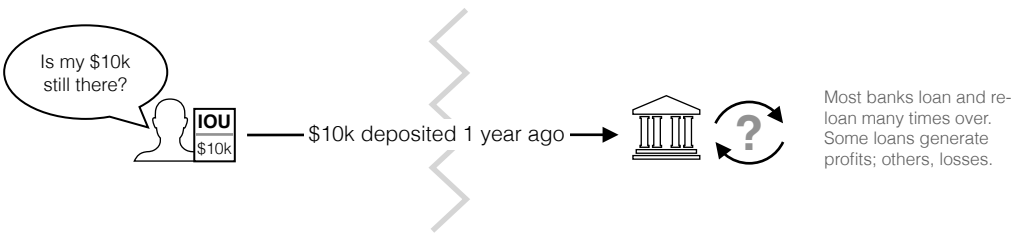
One of the important lessons from history is that private currencies have never been the fundamental reason for banking panics. The panics continued long after private currencies disappeared. The fundamental problem is Fixed-Price Assets. Specifically, it's the physical disconnect between a Fixed-Price Asset's IOUs and the associated value of the underlying assets.

For the purposes of this paper, assets in the banking industry can be categorized into two main buckets: Floating-Price and Fixed-Price. It might be helpful to briefly explain the difference.

Floating-Price Assets include debt funds with active liquidity as well as other market-priced credit instruments. The expected return of these assets, and therefore their market price, continually floats based on performance. For example, if 6% of a CMBS (commercial mortgage-backed securities) fund's assets are impaired due to underlying mortgage failures, the price naturally adjusts to reflect the new situation, but it doesn't necessarily trigger a complete meltdown. As long as the situation is quantifiably contained, the urgency to quickly sell mostly dissipates. This is because, with Floating-Price Assets, selling isn't always the best decision. The mortgages may start performing again or the management team might do better next quarter, and the price might bounce back. Those who sell out of fear aren't necessarily in a better financial position than those who have patience and hold.

Fixed-Price Assets include demand deposits, promissory notes, banknotes, and stablecoins. These assets, and their connection to losses, drastically differ from how Floating-Price Assets operate. When you put $10k cash into a bank account, the bank provides a promise to return the same amount of capital. However, putting this cash into the bank disconnects you from your actual physical money due to fungibility — you release control of your capital to someone else. From that moment forward, you only see a number on your bank statement. The real money — the underlying asset — is somewhere else. It is being invested in various enterprises by someone you've probably never met. One year later, your specific $10k deposit might exist or it might have disappeared due to someone else's poor decisions. All you know is, your bank statement still shows a fixed $10k. This is where it gets interesting.

FIGURE 10— THE RISK OF FIXED-PRICE IOU



The probability of your $10k existing one year later is dependent on a number of factors. For banks, this includes the quality of government regulations, the trustworthiness of the auditors overseeing your bank's decisions, and of course, the bank's management. For stablecoins, there is much less regulatory oversight, which leaves almost everything hinging on the honesty and intelligence of the management team.

The only way to definitively know if your money exists is to pull it out. And this is where panics begin. Whatever the underlying reason, if more IOUs exist in circulation than assets in the bank, the last person to pull their money loses. It's like playing musical chairs as a child. As Figure 11 shows, if three people are holding $10k each, but only

$20k exists at the bank, only the first two can redeem their IOUs. This economic necessity of not being the last to withdraw is what drives the panic.

FIGURE 11 — THE MOMENT OF PANIC

One of the biggest weaknesses of Fixed-Price Assets is their lack of transparent, physical connection between the holder of the IOU and the underlying capital being deployed. It's also one of their biggest strengths. The entire $30k of capital is thrown into the same opaque pool. By blending profits and losses across all bank investments, stability is achieved for all. Most of the time. When there are entity-wide deficits, massive instability can occur.

Tokenizing an off-chain asset, such as USDC's tokenization of dollars, does not improve the fundamental properties of how IOUs work or of how panics occur. Tokenization simply pushes the problem another level deeper. This is because blockchains only provide proof of IOU custody. They do not and cannot provide proof that you have custody of the actual underlying asset in the physical world, or even that the asset exists. Therefore, tokenizing dollars into a blockchain provides no more security from death-spirals than a bank gives through monthly statements. In both cases you are trusting someone somewhere to wisely protect your physical dollars.

The Problem with Stablecoin Collateral Is Their Absence of Collateral

The vast majority of stablecoins describe themselves as being backed by "collateral." According to the Oxford Dictionary:

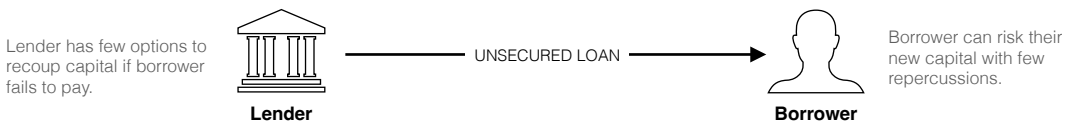
> *col·lat·er·al*. noun. Something pledged as security for repayment of a loan, to be forfeited in the event of a default.

The stablecoin industry has developed a clever sleight-of-hand — whether intentional or not — that obfuscates their risks by using the term "collateral" to describe their coins' supposed stability mechanisms. The "collateral" used by these stablecoins is not collateral in any financial understanding of the last four thousand years. In fact, it's the exact opposite of collateral, as we'll reveal below.

The easiest way to understand this is by taking a swing through time, back to the cradle of civilization. It involves clay tablets, loans, the Silk Road, and of course, modern paper money.

The first documented evidence of financial loans comes from clay tablets in ancient Mesopotamia around 3000 BCE[35]. Records from this era indicate loans of silver and barley were made and were expected to be repaid with interest. These earliest loans were likely unsecured.

FIGURE 12 — UNSECURED LOAN



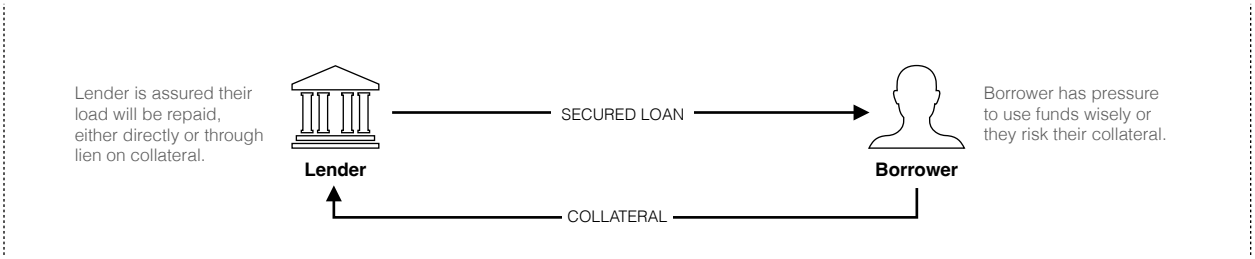
Unsecured loans place nearly all risk on the lender. Although the lender can be selective as to whom they offer loans, once a loan is given, the lender is at the mercy of the borrower. Without collateral as a forcing function, the lender has little recourse other than physical violence and social shaming to compel the borrower to pay.

The invention of secured loans was a game changer.

By 2000 BCE, most loans were secured loans. According to historical artifacts from that time period, collateral included agricultural lands, livestock, slaves, and crops.

Figure 13 shows a secured loan. In a secured loan, the lender places a lien on a collateral asset before capital is extended. At some predetermined time in the future, the borrower must repay the loan to receive their asset back. If the loan is not repaid, the lender keeps the asset as repayment.

FIGURE 13 — SECURED LOAN



What does any of this have to do with money or stablecoins? It is the combination of secured and unsecured loans that brought about the invention of modern money.

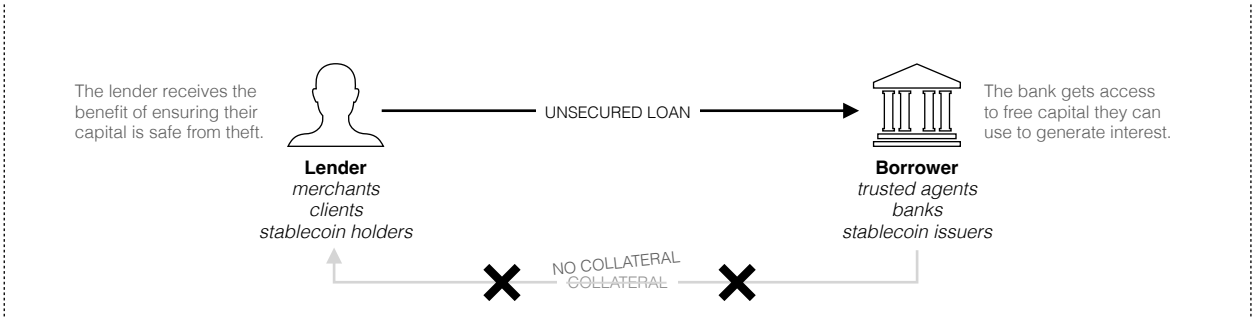
Paper money was first invented in China during the Tang Dynasty of 618–907 AD[36]. Transporting precious metals over long distances, such as the Silk Road, was dangerous and cumbersome. Merchants began leaving their coins with trustworthy agents who were paid to keep their coins secure.

Agents would record on paper how many coins the merchant had given them. This paper would then be given to the merchant as an IOU. It was a sort of money-substitute, which could be exchanged between merchants for goods. Any holder of this IOU could take the paper note to the agent and redeem it for coins.

As time progressed, trusted agents began loaning out the coins they had been entrusted to keep. These loans were nearly always structured as secured loans to minimize the agent's risk. Agents were soon generating more income from loans than from safeguarding fees. As the concept continued to develop, trusted agents morphed into what we now call banks, and the business model began to flip — the more coins they accepted, the more coins they could lend, and therefore the more income they could generate. Someone eventually had the bright idea to completely remove safeguarding fees in order to incentivize more merchants to hand over more capital.

The new banking model created a system whereby merchants became de facto lenders and banks became their borrowers. As Figure 14 shows, the merchant-to-bank transfers were effectively unsecured loans to the bank.

FIGURE 14 — BANKS RECEIVING UNSECURED LOANS



Banks use this "borrowed" capital to generate income through loans to other parties. In the modern world, this usually means investments in treasuries, money markets and other HQLAs. Sometimes these investments go sideways, which creates capital deficits, and sometimes these capital deficits cause banking panics. However, as described in the previous section, most of these panics have been removed through a combination of government regulations and national deposit guarantees.

Stablecoins follow the same banking model — this is true regardless of whether they're centralized entities like Circle or decentralized organizations like MakerDAO.

Over the past ten years, stablecoins have amassed nearly $200B in borrowed user capital[37], which they call "collateral." This is an egregious misnomer as this capital under management is in no way collateral for anything. It is essentially unsecured loan capital borrowed from their stablecoin users at zero percent interest, utilizing zero collateral, and with an indefinite term length. Unlike their nineteenth-century banknote-printing predecessors, stablecoin issuers are marketing their IOU-unsecured-loan machines as if they were providing their users with fully-collateralized currency assets. They're not.

If stablecoins were actually collateralized, the borrowers (stablecoin issuers) would commit collateral assets to the lenders (users), which the lenders could unilaterally seize if the borrowers found themselves unable to redeem their IOUs, such as the $3.3 billion that went missing due to SVB's collapse.

Instead, the massive $200B stablecoins industry is giving out crypto tokens with zero intrinsic value. The value of these tokens only exist through the good-faith promise of the borrowers (stablecoin issuers) to pay back their unsecured loans when requested by the lenders (stablecoin users). Therefore the value of these stablecoins hinge solely on the management decisions and trustworthiness of the issuer, which if one understands history, is a very risky proposition given enough time.

Moreover, these stablecoins exist outside the banking sector, and therefore, they are not protected with regulatory oversight or federal deposit guarantees. This means the issuers place the risk of these unsecured loans squarely on the backs of their stablecoin users (the lenders)[38].

A Somewhat Caveat

Stablecoins come in a wide variety of designs, and the previous descriptions might be considered an over-simplification for how some unsecured loan mechanisms work in the crypto industry.

Most stablecoins use a straightforward centralized approach that leaves no question as to their unsecured loan and IOU issuance models. By centralized we mean a central entity owns and manages the entire operation. USDC and Tether fall into this bucket. These two stablecoins control more than ninety percent of all stablecoins in circulation, and their structure is almost an exact replica of what is described above.

Other stablecoins employ a more complex decentralized approach that mask their underlying unsecured loan structure. MakerDAO and Frax are two such projects. They use a series of smart contracts and balancing algorithms to present themselves as collateralized-currencies within a decentralized model. By decentralized we mean a structure that allows anyone to join the network and participate in its governance. Some might argue these stablecoins are a type of secured loan through self-collateralization, but they're not. When you realize a large portion of their underlying assets are centrally-managed[39], it becomes clear that not only are they not truly decentralized, further, they face many of the same risks as their more centralized peers.

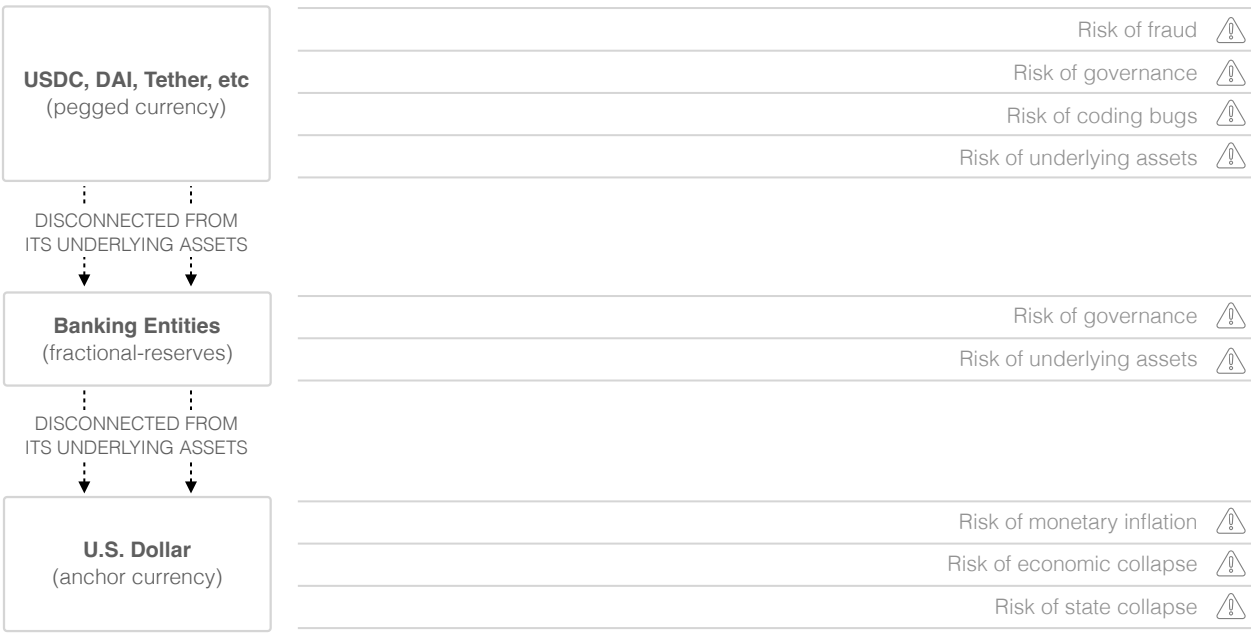
Risk On Top of Risk

The biggest issue of so-called "collateral-backed" stablecoins is, they're layering risk on top of existing risk. This isn't unique to stablecoins. It's true of every fractional-reserve product on the market. It's also true of every currency that pegs itself to another currency.

The challenge with stablecoins is they're doing both — they're operating with the same liquidity risks of traditional fractional-reserve products while also pegging themselves to another currency.

Figure 15 shows the multiple tranches of risk within a stablecoin. Each tranche has its own unique risks, and any instability within a single layer creates domino effects into the layers above.

FIGURE 15 — THE LAYERING OF RISK



The bottom layer of the stack contains the underlying currency. For example, the dollar is the world's dominant currency, but regardless of its current status, it carries risk. There is an increasing probability that someday the dollar will lose its reserve currency status[40] — no country remains on top forever. It also carries a probability of escalating inflation due to runaway government spending[41], servicing $34T in debt[42], and other monetary issues. Regardless of how probable or improbable those risks within a given timeframe, if any risk materializes, the buying power of every pegged currency will be affected. For example, if the dollar loses 10% in value due to inflation, as the U.S. dollar did last year, the holders of all related stablecoins — such as USDC, DAI and Tether — will have no alternative except to also lose 10%.

Move another level up and you'll find banks carry even more risk than currencies. Since all major stablecoins have some or all of their underlying value stored in fractional-reserve banking entities, any single bank failure can have a serious impact. For example, when Silicon Valley Bank failed in March of 2023, it caused major upheaval to USDC as well as a cascading effect into other stablecoins that relied on USDC.

Finally, there are the unique risks of the top layer, the stablecoin protocol itself. This includes such areas as governance structures, management decisions, operational issues, and coding bugs. A weakness in any one of these areas, or in any of the layers below, can destroy the stablecoin.

Few stablecoin holders seem to understand the risk of holding a "collateral-backed" stablecoin versus an actual dollar. The risk of stablecoins is orders of magnitude higher. Nevertheless, there are many situations where stablecoin benefits outweigh their downsides. If you transact within crypto, stablecoins are a huge improvement over the dollar which isn't yet digital and of the banking industry which doesn't yet interface with crypto.

The Hidden Cost of "Collateral-Backed"

When evaluating the value of "collateral-backed" stablecoins, it is essential to recognize their one-to-one price peg with the dollar (or whatever currency they're pegged to) does not fully represent the economic realities of issuing and maintaining digital assets. There are substantial costs to handling "collateral-backed" stablecoins, and although these costs are rarely discussed or explicitly laid out, they create an inextricable conundrum around the basic idea of stablecoins being equivalent to their underlying currencies.

Some of these costs include:

Audit and Compliance Costs. Collateral-backed stablecoins require regular audits to give the market assurance that their tokens are fully backed by equivalent assets. These audits, along with related regulatory compliance, require significant and continuous resources.

Operational Costs. Operating a stablecoin involves a wide array of functions including technology development, platform maintenance, cybersecurity, customer support, and general administrative tasks. The infrastructure to support a stablecoin's issuance, transaction processing, and redemption involves costs related to staff salaries, technology investment, and office maintenance, among others.

Liquidity and Reserve Management Costs. Stablecoin issuers must manage the collateral reserves meticulously to maintain the currency peg. This involves costs related to transaction fees, banking services, and the strategic rebalancing of assets. Additionally, the opportunity cost of holding large reserves of fiat or other assets, which might otherwise be invested for a return, is a significant economic consideration.

Legal and Regulatory Costs. Given the innovative nature of stablecoins, issuers often navigate complex and evolving landscapes. Legal defenses, settlements, and proactive regulatory compliance efforts are costly but necessary to operate within the legal frameworks of multiple jurisdictions and to instill trust among users and partners.

“Collateral-backed” stablecoins cannot have true one-to-one equality with the dollar due to these extra economic burdens. Their costs must exist somewhere on the balance sheet; costs cannot magically disappear into the ether.

Doing Basic Math

Figure 16 illustrates how hidden costs diminish a stablecoin's value relative to its pegged currency. Unless the stablecoin has zero costs, which is impossible, it cannot truly be equal in value to its underlying currency.

FIGURE 16 — CONCEPTUAL VALUE OF A “COLLATERAL-BACKED” STABLECOIN

$$S = D - C$$

In this formula:

S := The effective value of the stablecoin, considering the costs.

D := The nominal value of the stablecoin, typically set at $1.00.

C := The aggregate of all costs divided by the total number of stablecoins.

Determining the aggregate costs of any single stablecoin is complex, and these costs can vary over time due to changes in the regulatory landscape, market conditions, and operational efficiencies. Moreover, the market’s perception and utility of the stablecoin also plays a significant role in its actual trading value — it can sometimes diverge from the nominal peg despite these costs — nevertheless, the basic premise of this formula holds true over the long-run.

When the Piper Comes Calling

Most stablecoin issuers (and/or their investors) absorb the initial costs incurred during startup, such as infrastructure buildout, auditing, legal affairs, and reserve management. However, these costs must ultimately be passed on to the stablecoin holders. No company can lose money forever. And further, the issuer must find a way to generate profit for its shareholders.

There are a variety of mechanisms stablecoin issuers can use to generate revenue:

- **Transaction Fees**. Users might pay a fee when transacting with the stablecoin, especially in trades, transfers, or when redeeming the stablecoin for fiat currency.
- **Redemption Fees**. Some stablecoins charge a fee when users want to redeem their tokens for the underlying asset.
- **Spread in Exchange Rates**. Users might not always exchange stablecoins at a perfect 1:1 value due to fees or slightly unfavorable exchange rates imposed by platforms or the issuers themselves.
- **Opportunity Transfer**. Users transfer control of their underlying asset to the stablecoin issuer, which allows the issuer to generate returns from the strategic management of assets.

In order to minimize the perceived cost of stablecoins, most stablecoins — including USDC and Tether — use the Opportunity Transfer mechanism. Opportunity Transfer generates revenue through investment yields from the underlying assets, which seems harmless, except it incentivizes the issuer to increasingly adopt the risks articulated throughout this paper. And as previously described in this paper, these risks are placed squarely on the shoulders of the stablecoin holders not the issuers.

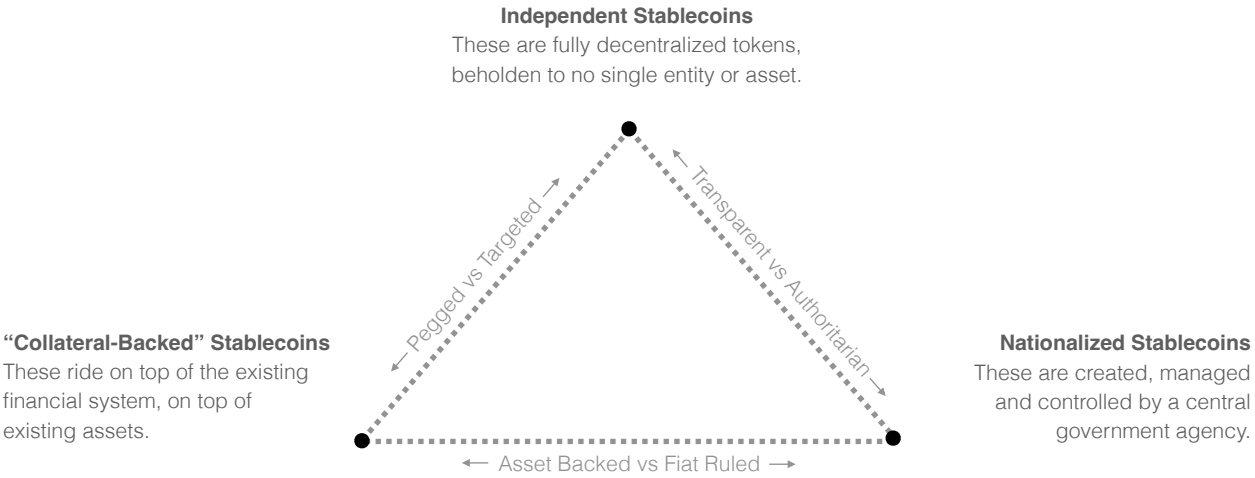
The Three Stablecoin Models

There seems to be an infinite number of ways the crypto industry can classify stablecoins: algorithmic versus non-algorithmic, endogenous versus exogenous, decentralized versus centralized, crypto-collateralized versus fiat-collateralized, asset-backed versus seigniorage-style, etc. For the purposes of this paper, we will focus on what we describe as the three core models:

- "Collateral-Backed" Stablecoins
- Nationalized Stablecoins
- Independent Stablecoins

Figure 17 shows an overview of these three stablecoin models along with their connections and relations to each other. Although it might appear each side of the trigon is a sliding scale whereby the models could blend to create hybrid models, each is in fact diametrically opposed to the others.

FIGURE 17 — A VISUAL GRAPH OF THE THREE



Most of this paper has focused on "Collateral-Backed" stablecoins. It shows how these stablecoins contain critical weaknesses that make it difficult, if not impossible, for them to become a truly global medium of exchange for everyday commerce.

Sooner or later the world will discard "Collateral-Backed" Stablecoins in favor of Nationalized Stablecoins or Independent Stablecoins. The rest of this paper explores these final two models.

Moving Towards a Nationalized Stablecoin

Nationalized Stablecoins are commonly referred to as Central Bank Digital Currencies (CBDCs). They are centrally-controlled stablecoins that seek to replace privately issued stablecoins. Most have been designed to function as crypto tokens, but their use of a blockchain as the underlying database is not a requirement nor does it change how they fundamentally operate. Several countries are already piloting CBDCs[43], although none have been rolled out on a broad scale as of this writing.

The transition from private currency to government-controlled currency is like a well worn clock. It has played out

in seemingly every society, starting with China in the first millennium. What began as private currency during the Tang Dynasty of 618–907 AD centralized into a government-controlled currency during the Yuan Dynasty of 1271–1368 AD[44].

In Britain, local currencies flourished for nearly a thousand years through a combination of private issuers, provincial banks and regional authorities[45]. During the late seventeenth century, local coinage began transitioning to central control. By the nineteenth century, only the Bank of England had the legal right to issue new currency[46].

It's always the same process: it begins with a rapid growth of private currencies followed by market instability, then regulations, centralization, and finally nationalization. A nationalized currency is one where authorities seize the underlying assets and through the levers of force create a fiat system beholden to no one but the government.

The United States of America went through such a process. For several hundred years, the states/colonies had no standard currency. People used everything from Spanish coins to tobacco, beaver pelts, or even wampum (beads made from special clam shells)[47]. The nineteenth-century saw an abundance of private banknotes, but in 1864, the U.S. began rapidly moving towards centralization. The creation of the Federal Reserve Bank in 1913 finished the process of converting the dollar into a government-controlled currency.

In the summer of 1971, an event happened that transformed the dollar from a traditional government-controlled currency into a full-blown nationalized asset.

Nixon's Nationalization of the Dollar

Since 1864, except during periods of wartime or disaster, the U.S. dollar has been generally backed by gold. Silver played a brief role, but in 1873 congress passed a bill demonetizing silver[48], effectively placing the dollar on a gold-only standard. For most of the next century, the dollar's value lay not in its currency but in its underlying asset, the gold backing it.

The United States' victory in World War II and the related Bretton Woods Conference of 1944 cemented the dollar as the world's dominant reserve currency. For the next twenty-five years, the United States controlled two-thirds of the world's gold[49], and they guaranteed every dollar with this gold.

A major weakness of the Gold Standard was that the dollar was physically disconnected from its underlying gold. This opened the door to over-printing and fiscal manipulation.

FIGURE 18 — BACK WHEN THE DOLLAR WAS AN IOU FOR GOLD

A series of backroom decisions in the late 1960s expanded the government's spending capabilities but weakened the nation's money supply[50]. By 1971, the public's belief in the dollar as being backed one-for-one with gold no longer matched actual reality. Wall Street, and especially international markets, became increasingly concerned the U.S. didn't have enough gold (it didn't), and a "run on the bank" started to take shape[51].

The situation became dire. A secret meeting was hastily assembled at Camp David between President Richard Nixon and his top economic advisors. For three days, the President and his brain trust wrestled with what to do[52].

On the evening of August 15, 1971, President Nixon announced on prime-time television the United States would renege on its long-held dollar-for-gold policy[53]. In a single stroke of his pen, Nixon effectively nationalized the

value of the dollar by taking complete ownership of all the gold within its vaults. Countries who held massive reserves in the dollar were irate; France even sent a navy cruiser into New York Harbor to reclaim what they believed was theirs[54]. The French cruiser never got its gold, and the "bank run" was thwarted. The power of the U.S. government forced every country, regardless of their desire, to give up their gold and reorganize their currencies.

The outcome of Nixon's policy was the U.S. dollar no longer functioned as an IOU. It no longer required an underlying stash of assets. It became a true fiat currency, and in doing so, it forever stopped the dollar from experiencing another "bank run". Moreover, all value underlying the dollar now lived within the dollar itself; or better said, all value underlying the dollar was now held directly in the power of the U.S. government.

America wasn't the first country to nationalize its currency. Many countries have made similar moves throughout history. However, no one had done so at such scale. It was shocking. It showed that although "bank runs" can happen anywhere, a strong government with unparalleled resources and power can restore order and stabilize its currency in a manner that is impossible for private institutions to achieve.

The last fifty years has also shown the incredible financial benefits that can accrue to whoever controls a global, untethered fiat like the dollar. By freeing itself from the constraints of physical gold, the U.S. granted itself an infinite license to print money at will. It is now operating at a scale unparalleled in history. Since 1972, total dollars in circulation has grown over 4,000%[55], and its debt engine has further exploded a mind-staggering 7,000%[56]. The capital increase from both these channels directly flows to the U.S. government.

Contagion Risks, Bailouts, and CBDC Assimilation

The cyclical transition of private currencies to central currencies continues via stablecoins. Fifteen Central Bank Digital Currencies (CBDCs) are already in pilot testing around the world[57]. Despite popular skepticism about the adoption of full-fledged CBDCs within a democracy, the crypto industry has created an environment that is remarkably conducive to such developments.

Although less than a decade old, stablecoins face increasingly high failure rates[58], prompting calls for regulatory alignment with banking industry standards. Particularly concerning are the stablecoins pegged to the dollar, which represent themselves as extensions of the dollar.

Increased regulations will likely lead to situations where government bailouts are not only possible but expected. This is because regulations will give stablecoins an extra feeling of safety and legitimacy, and this will likely lead to an influx of users and capital. As the market expands and evolves, the systemic importance of stablecoins will pose risks similar to those seen in money market funds and banks during past financial crises. They will be considered too big to fail.

Furthermore, the programmatic capabilities within crypto stablecoins allow the attributes of one asset to be tied to other assets. This will amplify the fear a single stablecoin failure could trigger a cascading effect, and this will further intensify the political desire for bailouts when those stablecoins fail.

The problem with bailouts is they are never free. The public naturally expects "free money" to come with strings attached, usually in the form of increased regulation and oversight. Sometimes these bailouts even induce the handover of equity to the federal balance sheet[59] — this is especially true for assets viewed as public utilities, which one might presume currencies fall into.

In summary, the current trajectory suggests private "collateral-backed" stablecoins will eventually be assimilated into a national currency. While this might not transpire immediately — it might not happen until 2040 or even 2140 — the ultimate conclusion appears inevitable. At some point, congress will introduce a Central Bank Digital Currency Act that places these stablecoins under the management of the Federal Reserve or a similar institution.

The Benefits

Proponents of Central Bank Digital Currencies (CBDCs) view this technology as the next evolutionary progression in the world of money. They argue CBDCs will elevate fiat to first-class digital status, foster financial inclusion, expedite payments, and streamline the implementation of monetary and fiscal policies[60] — and in the U.S., CBDCs are also discussed as a way to safeguard the dollar as the world's reserve currency. While such optimism may be perceived as overly hopeful, it's undeniable CBDCs offer numerous advantages compared to the current system of paper bills and risky stablecoins.

One significant benefit of CBDCs is the elimination of stablecoin death-spirals. This is achieved by establishing an inextricable fusion between the digital coin and its underlying value, removing the need for fractional-reserve structures.

Additionally, CBDCs will create a more immediate impact of monetary policies in the economy, enabling faster market responses and introducing novel quantitative controls previously unavailable to governments.

Finally, CBDCs will mark a shift away from paper dollars, significantly reducing societal costs and opening new worlds of possibility.

While a large portion of transactions are already electronic[61], our foundational monetary system still relies on paper. The expenses associated with designing, minting and handling this paper money pose a substantial financial burden for banks and financial institutions[62]. As CBDCs become fully operational, the cost of maintaining paper money will likely become untenable, eventually leading to legislated obsolescence.

In a non-paper world enabled by CBDCs, processes like tax collection can be simplified or even automated, eliminating the need for citizens to file tax returns. Moreover, traceability and block-ability of transactions can reduce illegal activities like money laundering and drug trafficking.

Ultimately, the question of CBDCs isn't whether they bring efficiency and benefit to society. They most definitely do. The critical question is whether the upsides are worth the downsides[63].

Absolute Power Corrupts Absolutely

Paper money offers a key advantage over Central Bank Digital Currencies (CBDCs), which is its anonymity. Unlike CBDCs, where the central government gains absolute control over currency usage, paper bills facilitate transactions without revealing details to anyone except the involved parties. Anyone can spend a $100 paper bill without anyone except the participating parties knowing what was bought or when it was bought. Although surveillance and tracking of paper money can be implemented to investigate bank robberies or other criminal activities, doing so requires extra steps and a lot of extra effort. Not so with CBDCs.

CBDCs give the managing entity absolute control over the currency's usage, providing real-time capabilities to track and enforce rules. It gives governments granular power over citizens' everyday financial activity.

CBDCs make it incredibly easy to monitor and censor the transactions of political enemies. This is because CBDCs establish a direct line between citizens and the government itself — they're an instant backdoor into your bank account. The government can see who is spending what and when. Money can be precisely targeted to control what people can do and what people can own. For example, people could be prohibited from buying certain goods, limited in how much they can purchase, or even the complete revocation of their money.

CBDCs can financially exclude individuals or entire groups of people with the press of a button, leaving them with nothing. Governments could target dissidents, sexual minorities, ethnic minorities, or religious minorities. Once paper cash has been removed from circulation, these individuals will be truly helpless.

Governments have long recognized that freezing someone's financial resources is one of the most effective ways to stop unwelcome behavior[64]. For example, Operation Chokepoint was a U.S. government initiative where officials pressured financial institutions to deny services to politically disfavored businesses (e.g., pawnshops, check cashers, and cannabis dispensaries). As one official described it, the operation was designed to stop these businesses by "choking them off from the very air they need to survive."[65] Similarly, the Canadian government made headlines in 2022 when it invoked the Emergencies Act to freeze the bank accounts of protestors.[66]

If paper money no longer exists, and if all digital money is run through a central government system, then turning off someone's access to basic societal functions only requires the click of a single button. It will be instantaneous. No money. No ability to buy food. No ability to pay rent. No ability to fill up their car. No ability to pay their phone bill. Nothing. They will become a pariah to society.

One might argue the same can be done today. This is somewhat true theoretically. The government can (and does) freeze bank accounts of terrorists and other criminals, but it's not efficient. There are thousands of banks and money services, and they they all operate as separate systems without being intricately controlled by a single master-key. A CBDC, on the other hand, is a single system managed by one omnipresent authority.

Freezing the assets of one million political dissidents would be incredibly complex in today's non-CBDC world. It would require multiple levels of authorities, systems, and entities. Word would leak and there would be time for multiple people to object at multiple levels. However, with a CBDC, those million people could be disconnected by anyone with top-level credentials and a twenty line Python script.

Proponents of CBDCs will argue the system can be built so as to limit the government's control. However, it's naïve to believe such a system can be built without establishing the foundation for surveillance. Quite simply, even if surveillance is not included in the initial design, it will be trivial to add at a later stage. Once the door to surveillance is opened, it will be virtually impossible to close. Complex warrants and rules can be set, but the system will always be one step away from someone (or a group of someones) sidestepping those controls. As Snowden showed, it has happened before in the surveillance state[67].

CBDCs might begin with the best of intentions. The first leader might be benevolent, but leaders come and go. It only takes one authoritarian-minded individual for the CBDC to slide into authoritarianism. Once this begins, it will be difficult to stop. It will be backed by guns, armored vehicles and the infinite resources of a national government.

The Question of Bank Versus Central Bank

The Federal Reserve Bank of the United States has been actively experimenting with CBDC technology over the last four years. In addition to researching, designing and developing their own software[68], the Federal Reserve has released several papers that express their view of how such a U.S. CBDC might operate[69]. In every instance, they carefully communicate any potential CBDC will operate under an intermediated model, meaning commercial banks would be the conduit between the CBDC and its end-users. They create the impression that CBDCs are not at risk of being centrally controlled or useful for dystopian purposes. This is naive for several reasons:

Cost of Technology. The cost of creating and managing a CBDC is every bit as complex and costly as managing the printing presses of the Treasury Department's Bureau of Engraving and Printing. Just as each bank is not burdened with printing their own paper dollars, it is inconceivable each bank will be burdened with creating their own CBDC software. At the very least, a single CBDC system will be federally developed and then distributed to each bank. This means there will be a group within the government that has intimate knowledge of how to control the system.

Need for Fungibility. CBDC systems can't operate properly if the digital currency isn't fungible across all banks. This means they must share the same protocols and properties. Further, all the systems must be inter-connected and operable with each other. Consequently, a central blockchain or clearinghouse must be created, laying the groundwork for a central government entity to control the flow.

Need for Oversight. A CBDC doesn't just represent the national currency; it is the currency. Creating a new on-chain token effectively mints a new unit of currency backed by the government. Therefore one can assume the government will require not just insight into the operations of each bank's CBDC but also access to the system itself. It becomes a slippery slope between down the path of how much read and write access to grant.

Government Back Doors. If a federal agency develops the CBDC software, it's highly likely one or more government agencies will have full-access back doors installed into the very core of the system. They've already done so elsewhere in the technology sector[70].

In summary, CBDCs might start with bank-only control, but they will rapidly transition to central government control for the reasons mentioned above. The move might be implicit or explicit, but when it happens, the path to authoritarianism will become one small step from reality.

Establishing an Independent Stablecoin

The most effective solution to counter the looming threat of authoritarian controls posed by CBDCs is to establish a publicly-owned decentralized stablecoin. This stablecoin should not only be functionally isolated from destabilizing market trends but also impervious to the risks of death spirals.

It must be independent. By independent, we mean, independent like Bitcoin. Independent from "collateral-backed" assets. Independent from centralized custodians, financial entities or fiat pegging. Like Bitcoin, it should not require U.S. treasuries held in banks to give it value.

Any stablecoin seeking to become a global medium of exchange must be able to stand independently as its own unit of value. In short, it must have the core attributes inherent in commodity-money.

A Rollercoaster of Progress

Figure 19 shows the various forms of currency and currency-like entities. The columns are ordered from left-to-right based on when they were introduced to society. Each brings improvements in some areas while regressing in others.

FIGURE 19 — COMPARISON OF MONETARY OPTIONS

Commodity-Money	Commodity-Backed Paper	Fiat-Backed Paper	Bank Account	Bitcoin	"Collateral-Backed" Stablecoin	CBDC	????	
✗	✓	✓	✓	✓	✓	✓	✓	Easy transmissibility
✓	✗	✗	✗	✓	✗	✗	✓	Freedom from national monetary policies.
✓	✗	✗	✗	✓	✗	✗	✓	Insulation from bank failures.
✓	✗	✗	✗	✓	✗	✗	✓	Seamless cross-border payments.
✓	✗	✗	✗	✓	✗	✗	✓	Immunity from inflation and deflation.
✓	✗	✗	✗	✓	✗	✗	✓	Unaffected by geopolitical conflicts.
✓	✓	✓	✓	✗	✓	✓	✓	Stable purchasing power.
✓	✗	✓	✗	✓	✗	✓	✓	Immunity from bank-type panics / death-spirals.
✗	✗	✗	✗	✓	✓	✓	✓	Native digital integration
✓	✓	✓	✗	✓	✗	✗	✓	Resistant to big-brother control
✗	✗	✗	✓	✗	✓	✓	✓	Protection from outright theft
✓	✓	✓	?	✗	✗	✗	✓	Usable without a working internet connection

Commodities were the first money, and throughout history, they have been the most common form of money. These commodity-monies have usually had strong intrinsic value in society, things like gold, silver, cattle, grain, etc. They independently maintain their value regardless of the rise and fall of nations, and they're mostly resistant to inflation since governments can't print them on a whim. They work flawlessly in almost every respect.

The primary weakness of Commodity-money is transmissibility. Transporting commodities is cumbersome and so a system of IOU credits developed in various societies, from paper notes during the Tang Dynasty of the fifth century to the Gold Standard of the twentieth-century. Unfortunately, this physical separation of paper IOUs from underlying asset-values creates a ripple effect of instability, much of which has been covered elsewhere in this paper.

The instability of commodity-backed IOUs ultimately gave rise to the fiat dollar of the late twentieth century. Fiat's primary weakness is inflation. Fiat gives governments an infinite ability to print more money, and in doing so, it has given rise to an inflationary-era that has destroyed the savings of everyday citizens.

Bitcoin was meant to replace fiat. Satoshi's objective was to create a currency with better transmissibility than paper, stronger intrinsic value than gold, and an asset that couldn't be destroyed by government inflation. In so many ways, Satoshi succeeded beyond anyone's wildest dreams. But of course, as we know, Satoshi overlooked one of the most crucial requirements of useful currency: stable purchasing power. This omission hindered Bitcoin from becoming a currency that could replace the dollar as a global medium of exchange.

Stablecoins such as USDC, Dai, and Tether were invented to provide stable purchasing power, but they regressed in other areas of importance. Their underlying "collateral-backed" architectures required them to choose stabilization over decentralization. In doing so, they became little more than IOUs for the dollar. Worse, these centralized stablecoin structures created their own instability issues, which is now laying the groundwork for authoritarian-leaning CBDCs to emerge.

So then, how does one create a decentralized alternative to CBDCs without succumbing to the risk of "collateral-backed" architectures?

Two Essential Attributes

As mentioned earlier, the primary weakness of commodity-money is transmissibility. Fortunately, transmissibility is one of the strongest and most innate properties of digital. If only we could combine the two.

Obviously, physical commodities cannot be digitized, at least not without creating an unstable layer of IOUs. The solution is to create a new natively-digital commodity-money that incorporates the key properties from traditional commodity-money. This might seem like the most basic of ideas, but no one has done it.

Commodity-money has two essential attributes that are missing from today's stablecoins:

1) **Hard money.** This means money that cannot be infinitely created on a whim, such as fiat dollars on a printing press. The truth is, there has never been a perfect form of "hard money." The world's stock of gold increases at around 1% to 2% per year[71], which means that gold's inflation is 1% to 2%. Bitcoin has the opposite problem. It is forever capped at 21M tokens, and because a percentage of Bitcoins are lost each year due to misplaced keys[72], over time, this will cause the currency to experience deflation. Regardless of the fact that both gold and Bitcoin experience inflation and deflation, they are still two of the "harder" monies in circulation. Most stablecoins today are pegged to the dollar, which means they inherit all the inflation of the dollar.

2) **Intrinsic value.** This means the commodity has worth independent of its use as money. For example gold does not corrode, which makes it a lasting material for jewelry and coins — its aesthetic appeal and rarity have made it desirable for thousands of years. Fiat money, on the other hand, has little (practically zero) value outside its use as a currency. Although the cryptographical technology of blockchain has intrinsic value to society, it is debatable whether the blockchain address of a USDC or Tether token has any actual value that exists beyond its use as a form of money.

Deterministic Profit Incentives

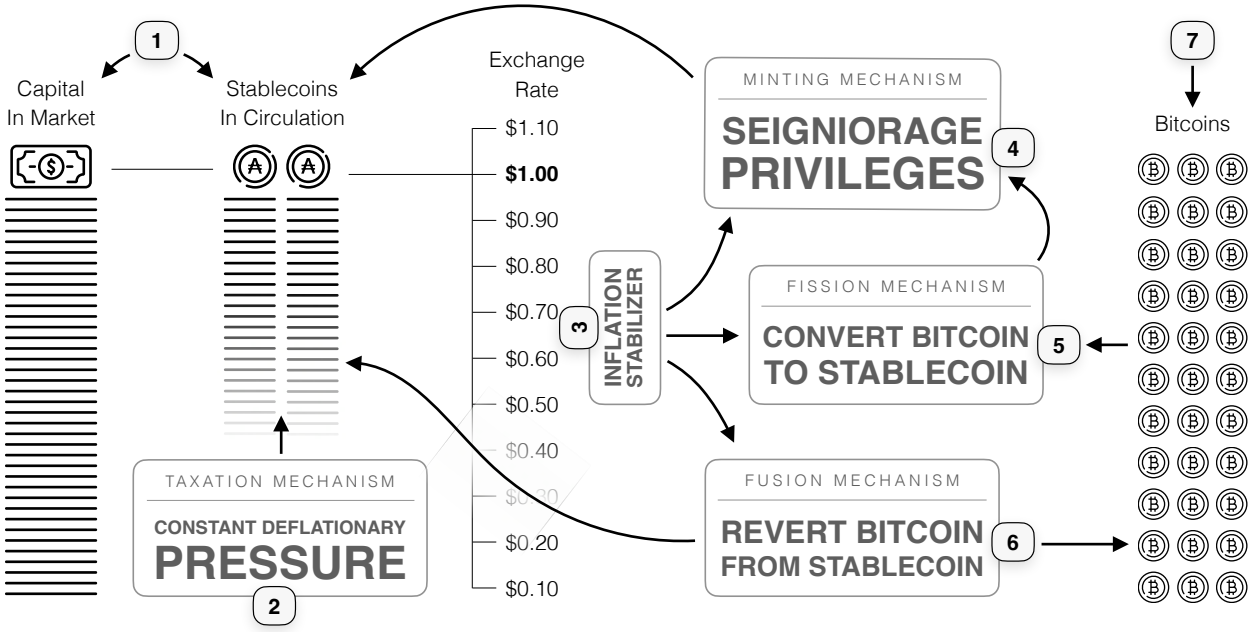
We've invented a novel algorithmic stablecoin design that operates as commodity-money and requires zero "collateral" for stabilization. It uses basic economic principles to create Deterministic Profit Incentives (DPI) that sit on both sides of the stablecoin's target price. These profit incentives are realized via blockchain-native synthetic derivatives that are exogenous to the stablecoin and functionally isolated from any fluctuations in market sentiment.

The result is a self-balancing system where the further the stablecoin falls below its target price, the higher its profit incentives, and therefore the faster its rebound. It has no self-reinforcing loops that would allow for death-spirals or similar implosions. The only scenarios in which this stablecoin could collapse require setting aside fundamental economic principles, such as profit maximization and the law of supply and demand, as well as key tenets of praxeology, including rational choice and agency theory.

It is not the purpose of this paper to articulate the complete details of our stablecoin design. The following page merely presents a summary. For a full breakdown on the technical specifications and mathematical basis behind our DPI protocol, please refer to the second whitepaper in our three-part series, *Designing a Stabler Stablecoin.*

Figure 20 shows a high-level overview of the basic components of our stabilization mechanisms.

FIGURE 20 — THE FOUR DPI STABILIZATION MECHANISMS



1 **Supply and Demand**. DPI differs from other stabilization protocols in that it directly regulates the supply of stablecoins in circulation rather than trying to adjust demand through incentivizing capital inflow/outflow.

2 **Taxation Mechanism**. Taxation uses digitally-native revenue that is exogenous to the stablecoin's stabilization to remove stablecoins from circulation. It does this by implementing a protocol-level tax that is burned instead of being circulated back into the economy. This places a constantly upward pressure on the stablecoin's price.

3 **Inflation Stabilizer**. DPI uses an internal Inflation Index (initially comprised of the USA's Consumer Price Index with an expected gradual shift towards a global basket) to guide the easing and tightening of stablecoins in circulation. This elastic circulation creates a truly hard currency with zero inflation or deflation.

4 **Minting Mechanism**. Minting allows the network's participants/owners to generate new stablecoins whenever the Inflation Index indicates demand is outstripping supply. In doing so, it removes deflation and brings the law of supply and demand back into equilibrium.

5 **Fission Mechanism**. Fission binds the stablecoin's blockchain and Bitcoin's blockchain into an economic interdependence that stabilizes both chains. It stabilizes Bitcoin by fully hedging downside risk, and it stabilizes the stablecoin by creating a wall of shorts against any future depeg.

6 **Fusion Mechanism**. Fusion is a special mechanism allowing Bitcoin owners to cover stablecoin shorts whenever the stablecoin's price drops below target. This short-covering burns excess stablecoins from circulation at between 2x to 50x the value of Bitcoin. By operating in opposing proportion to the stablecoin's nominal value — i.e., the profit incentives increase as the stablecoin's price decreases — intrinsic value is created for the stablecoin token within Bitcoin, regardless of the stablecoin's usage as a currency. This gives the stablecoin lasting value comparable to commodity-money.

7 **Bitcoins**. Bitcoin tokens are the core asset used to create Fission/Fusion's derivative-arbitrage opportunities. It creates a world where Bitcoin is swallowed into a trillion-dollar stablecoin[73] capable of being used as an universal transactional currency. At the same time, Bitcoin becomes the underlying store-of-value and foundational bedrock of the new economy.

For more in-depth breakdowns, please refer to our other whitepapers.

Next Steps

This whitepaper is the first in a series of three stablecoin papers. The goal of this first paper is to set an historical

context for stablecoins and highlight their current challenges. The next two describe the technical and economic details of our solution:

Designing a Stabler Stablecoin. A detailed breakdown of our novel DPI approach to creating a fully decentralized stablecoin that is mathematically impossible of death spiraling.

Bootstrapping a Global Currency. This outlines our strategy for bootstrapping the stablecoin from zero to one trillion. It covers the mining protocol behind our proof-of-work blockchain, p2p settlement fees, and more.

The most up-to-date version of our whitepapers can be found at https://argonprotocol.org. Feel free to email us at caleb@argonprotocol.org or blake@argonprotocol.org with any questions or suggestions.

Acknowledgments

A huge thanks to Martin Underwood and Alvin Townley for reading countless drafts, giving invaluable feedback and sometimes even rewriting entire paragraphs — without the two of you, our ideas would not be as crisp nor the writing as clear. It's also proper to give a shoutout to Nader Al-Naji, Josh Chen, and Lawrence Diao who inspired us early in our journey through their Basis whitepaper. Last but not least, a note of appreciation to the writing and work of Chris Dixon who opened our minds to possibilities beyond the obvious.

---

[1] CoinMarketCap, 2024. Available online: at https://coinmarketcap.com/currencies/bitcoin/ (accessed on January 12, 2024)

[2] Yianni Doumenis, Javad Izadi, Pradeep Dhamdhere, Epameinondas Katsikas, and Dimitrios Koufopoulos. 2021. A Critical Analysis of Volatility Surprise in Bitcoin Cryptocurrency and Other Financial Assets. Risks by MDPI.

[3] Anton Badev, Cy Watsky. 2023. Ripple Effects from the Terra Collapse. Federal Reserve Board, Washington, D.C, Finance and Economics Discussion Series. Available online at https://www.federalreserve.gov/econres/feds/files/2023044pap.pdf

[4] BitShares Whitepaper released in 2014. Available online at https://blog.bitmex.com/wp-content/uploads/2018/06/173481633-BitShares-White-Paper.pdf

[5] The opening sentence of Satoshi's whitepaper: https://bitcoin.org/bitcoin.pdf

[6] The Bitcoin whitepaper was first published on October 31, 2008 on what was known as, "The Cryptography Mailing List."

[7] Kane Pepi. How Many People Use Bitcoin. https://www.techopedia.com/cryptocurrency/how-many-people-use-bitcoin (accessed on January 25, 2024).

[8] [8] CoinMarketCap, 2024. Available online: at https://coinmarketcap.com (accessed on January 12, 2024)

[9] Statista, November 6, 2022

[10] October 20, 2022 report by Fundera on Companies That Accept Bitcoin

[11] BitPay, Coinbase, and Paypal

[12] CryptoNews: https://cryptonews.com/guides/will-bitcoin-ever-be-stable.htm

[13] Mitsutoshi Adachi, Alexandra Born, Isabella Gschossmann and Anton van der Kraaij. 2021. The Expanding Functions and Uses of Stablecoins. European Central Bank. https://www.ecb.europa.eu/pub/financial-stability/fsr/focus/2021/html/ecb.fsrbox202111_04~45293c08fc.en.html

[14] CoinGecko, 2023. Available online: https://www.coingecko.com/en/categories/stablecoins (accessed on October 10, 2023)

[15] SafeCoin, BitUSD, DigitalDollar, NuBits, CK USD, and TetherUSD to name a few.

[16] Muyao Shen. 2022. How $60 Billion In Terra Coins Went Up In Algorithmic Smoke. Bloomberg. https://www.bloomberg.com/graphics/2022-crypto-luna-terra-stablecoin-explainer/

[17] Christian Catalini and Alonso de Gortari. 2021. On the Economic Design of Stablecoins. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899499

[18] a16z Crypto Policy Team. 2023. Considerations for the Regulation of Algorithmic Stablecoins. https://api.a16zcrypto.com/wp-content/uploads/2023/04/Considerations-for-the-Regulation-of-Algorithmic-Stablecoins.pdf

[19] CoinMarketCap. 2024. https://coinmarketcap.com/view/stablecoin/ (accessed on January 12, 2024)

[20] Arijit Sarkar. USDC depegs as Circle confirms $3.3B stuck with Silicon Valley Bank. https://cointelegraph.com/news/usdc-depegs-as-circle-confirms-3-3b-stuck-with-silicon-valley-bank

[21] CoinMarketCap. 2024. https://coinmarketcap.com/currencies/usd-coin/ (accessed on January 12, 2024)

[22] Signed into law by President Dwight D. Eisenhower on May 9, 1956. https://www.govinfo.gov/content/pkg/COMPS-252/pdf/COMPS-252.pdf

[23] As reported by the stablecoin issuers themselves: https://tether.to/en/tether-q3-attestation-reveals-highest-percentage-of-cash-and-cash-equivalent-reserves-over-330m-reduction-in-secured-loans-and-maintains-726b-exposure-in-us-t-bills/ and https://www.circle.com/blog/how-the-usdc-reserve-is-structured-and-managed

[24] Gary B. Gorton and Jeffery Y. Zhang. 2021. Taming Wildcat Stablecoins. University of Chicago Law Review, Vol. 90. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3888752

[25] John Williams. 2023. Stablecoin Issuer Argues Crypto Regulation Could Stifle Innovation. https://techbullion.com/stablecoin-issuer-intervenes-in-sec-v-binance-case-arguing-crypto-regulation-could-stifle-innovation/

[26] Dan Awrey. 2021. Bad Money. Cornell Law Review. https://live-cornell-law-review.pantheonsite.io/wp-content/uploads/2021/02/Dan-Awrey-Bad-Money.pdf

[27] Gerald P. Dwyer Jr.. 1996. Wildcat Banking, Banking Panics, and Free Banking in the United States. Federal Reserve Bank of Atlanta. https://www.atlantafed.org/-/media/documents/research/publications/economic-review/1996/12/vol81nos3-6_dwyer.pdf

[28] Discounts were tracked and published in banknote reporters such as Thompson's Bank Note Reporter: https://curiosity.lib.harvard.edu/american-currency/catalog/66-990094886070203941

[29] Warren E. Weber. 2015. Lessons for E-Money from the U.S. Experience with Bank Notes. Federal Reserve Bank of Atlanta. https://www.atlantafed.org/cenfis/publications/notesfromthevault/1505

[30] The National Bank Act was passed by congress on February 25, 1863. https://fraser.stlouisfed.org/title/national-bank-act-1863-1111

[31] The banking panics of 1873, 1884, 1893, and 1896, to name just a few.

[32] The Federal Reserve Act signed by President Woodrow Wilson on December 23, 1913: https://www.senate.gov/artandhistory/history/minute/Senate_Passes_the_Federal_Reserve_Act.htm

[33] The Banking Act of 1933 created the FDIC and with it, federal deposit guarantees, which took affect on January 1, 1934: https://www.fdic.gov/bank/historical/brief/brhist.pdf

[34] Silicon Valley Bank's troubles started on March 8, 2023 when they announced a $1.8B loss on their bond portfolio. That started a domino affect that ended two days later when federal regulators closed it for good on March 10, 2023.

[35] Douglas Garbutt. 1984. Significance of Ancient Mesopotamia In Accounting History. Accounting Historians Journal: Vol. 11. Available at: https://egrove.olemiss.edu/aah_journal/vol11/iss1/5

[36] Yang, Lien-sheng. 1971. Money and Credit in China (2nd edition). Cambridge, Massachusetts: Harvard University Press.

[37] According to the Federal Reserve Bank of New York, the stablecoin market hit $180B in 2022: https://libertystreeteconomics.newyorkfed.org/2023/07/runs-on-stablecoins/

[38] Circle terms of use for USDC: https://www.circle.com/en/legal/usdc-terms

[39] Samuel Haig. 2022. MakerDAO May Execute Emergency Shutdown If Sanctions Hit DAI. The Defiant: https://thedefiant.io/tornado-impact-makerdao-dai

[40] Ray Dalio. 2021. Principles for Dealing with the Changing World Order. Published by Simon & Schuster.

[41] U.S. Federal spending jumped 40% in four years, from $4.45 trillion in 2019 to $6.21 trillion in 2023: https://www.cbo.gov/system/files/2023-02/58848-Outlook.pdf

[42] U.S. National Debt as of January 13, 2024: https://www.pgpf.org/national-debt-clock

[43] As of January 14, 2024, the Atlantic Council lists 5 CBDCs as having launched with another 15 in active pilots. https://www.atlanticcouncil.org/cbdctracker/

[44] Morton, W. Scott, China: Its History and Culture (New York: Lippincott, 1980)

[45] Christine Dean. 2014. Making Money (1st edition). Published by Oxford University Press.

[46] The Bank Charter Act 1844 (7 & 8 Vict. c. 32), sometimes referred to as the Peel Banking Act of 1844. Available online: https://www.ledr.com/bank_act/1844032.htm

[47] Sharon Ann Murphy. 2017. Other People's Money: How Banking Worked in the Early American Republic. Published by Johns Hopkins University Press.

[48] The Coinage Act of 1873 was signed by President Ulysses S. Grant on February 12, 1873: https://fraser.stlouisfed.org/title/coinage-act-1873-1095/fulltext

[49] Yi Wen and Brian Reinbold. 2020. The Changing Relationship between Trade and America's Gold Reserves. Available online at https://www.stlouisfed.org/publications/regional-economist/first-quarter-2020/changing-relationship-trade-americas-gold-reserves

[50] Allan H. Meltzer. 2005. Origins of the Great Inflation. https://files.stlouisfed.org/files/htdocs/publications/review/05/03/part2/Meltzer.pdf

[51] David Frum. 2000. How We Got Here. Published by Pereus Books Group.

[52] Jeffrey Garten, former Dean of Yale University's School of Management. 2001. Three Days at Camp David. Harper Collins. https://insights.som.yale.edu/insights/how-the-nixon-shock-remade-the-world-economy

[53] U.S. Secretary of State, Office of the Historian. Nixon and the End of the Bretton Woods System. https://history.state.gov/milestones/1969-1976/nixon-shock

[54] Michael J. Graetz. 2016. A "Barbarous Relic": The French, Gold, and the Demise of Bretton Woods. Columbia Law School Faculty Publications.

[55] Derived from FRED's Currency in Circulation Data. Available online at https://fred.stlouisfed.org/series/CURRCIR

[56] Derived from FRED's Federal Debt Data. Available online at https://fred.stlouisfed.org/series/GFDEBTN

[57] As of January 14, 2024, the Atlantic Council lists 15 CBDCs designed for retail commerce as already being in active pilot status: https://www.atlanticcouncil.org/cbdctracker/

[58] Although there has been no direct statistics published on the comparison rates of stablecoin failures versus bank failures, the rate of stablecoin failures is astronomically high (estimated over 20% failure during last 8 years): https://www.americanbanker.com/opinion/paypals-stablecoin-plan-poses-a-grave-threat-to-financial-stability and https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022008.ashx

[59] An example is The Federal Reserve taking a 79.9% stake in AIG's equity: https://www.newyorkfed.org/aboutthefed/aig

[60] Tao Zhang, "Central Bank Digital Currency" (keynote address at the Conference on China's Trade and Financial Globalization, London, March 19, 2020); John Kiff et al., "A Survey of Research on Retail Central Bank Digital Currency," IMF Working Paper no. 2020/104, June 26, 2020; Andrew Ackerman, "Fed Prepares to Launch Review of Possible Central Bank Digital Currency," *Wall Street Journal*, October 4, 2021; and John Kiff and Jonas Gross, "CBDCs for the People? Where the Current State of Digital Currency Research Leads," CoinDesk, December 3, 2021.

[61] Over 97% of money in circulation is now in electronic form (Ajay S. Mookerjee, 2021, Harvard Business Review, https://hbr.org/2021/10/what-if-central-banks-issued-digital-currency); According to a Gallup poll from July 5-26, 2022, the number of Americans who are cashless has doubled over the last five years; a similar growth was registered by the European Central Bank on February 6, 2023

[62] The Federal Reserve spends nearly a billion dollars annually on the design and minting of paper money (https://www.federalreserve.gov/faqs/currency_12771.htm). According to McKinsey & Company, the additional expense of handling this cash accounts for at least five to ten percent of all bank operating costs and this cost continues to grow (https://www.mckinsey.com/industries/financial-services/our-insights/attacking-the-cost-of-cash).

[63] Many CBDCs risks communicated in this paper were inspired from research by the Cato Institute's Policy Analysis No. 941, April 2, 2023.

[64] Howard Anglin, "In Our Cashless Society, We Need to Take Digital Jail Seriously," The Hub (Canada), February 22, 2022.

[65] Alan Zibel and Brent Kendall, "Probe Turns Up Heat on Banks," *Wall Street Journal*, August 7, 2013.

[66] Nicholas Anthony, "How Canada Made the Case for Cryptocurrency, Not CBDCs," *Cato at Liberty* (blog), March 2, 2022.

[67] Barton Gellman of The Washington Post was the first journalist to report on Snowden's revelations: https://en.wikipedia.org/wiki/Edward_Snowden

[68] The FED has been actively exploring CBDCs since at least mid-2020. https://www.federalreserve.gov/cbdc-faqs.htm + https://www.federalreserve.gov/newsevents/pressreleases/other20200813a.htm + https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx + https://www.bostonfed.org/news-and-events/press-releases/2022/frbb-and-mit-open-cbdc-phase-one.aspx

[69] Board of Governors of the Federal Reserve System. 2022. Money and Payments: The U.S. Dollar in the Age of Digital Transformation. https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf

[70] Although not officially acknowledged by the government, the evidence is overwhelming: https://www.reuters.com/article/idUSKBN27D1DO/

[71] Gold's supply increases 1% to 2% per year according to the World Gold Council: https://www.gold.org/goldhub/research/gold-demand-trends/gold-demand-trends-full-year-2022/supply

[72] There is no agreed upon model for determining the annual loss rate, however everyone agrees that it's a problem: https://news.bitcoin.com/analyst-1500-bitcoins-lost-every-day-less-than-14-million-coins-will-ever-circulate/

[73] Bitcoin's market cap as of August 11, 2024 is $60,277.59 per token with 19.79M tokens in circulation.