The Fundamentals for Creating a Stable Crypto Asset

By Caleb Clark & Blake Byrnes

Version 0.18

Abstract. Stablecoins are cryptocurrencies designed to solve the volatility of Bitcoin by pegging to a reference asset, most commonly the dollar. However, the current crop of stablecoins are fundamentally broken. By pegging to fiat they absorb all the same inflationary debasement issues that are undermining fiat currencies around the world.

Worse still, many stablecoins have depegged, death-spiraling into catastrophic failure. The ones that haven't are at constant risk of doing so. Their solution for providing price stability has created a brittleness, a ticking time bomb of instability.

This paper introduces a novel approach for using unrestrained profit incentives to create a fully decentralized stablecoin, one that doesn't rely on centralized assets or fiat pegging. More importantly, it is the first stablecoin immune to death spirals. Even if Argon loses 99.9999% of its value, it will bounce back to its target price within days.

Within the Argon is a secondary mechanism called Dual Signature Time Lock (DSTL) that facilitates trustless and efficient cross-chain asset locking between Bitcoin and another heterogeneous blockchain like Argon. DSTL is not only faster but significantly cheaper and more secure than existing cross-chain mechanisms such as HTLC, XCLAIM, XCC or Babylon.

Table of Contents

Introduction

This is the second in a series of stablecoin whitepapers. Our first, *On The Stabilization of Collateral-Backed Stablecoins*[1], explores the history of currency, the current state of stablecoins, the many challenges faced by the crypto industry, and the move of governments into Central Bank Digital Currencies (CBDCs).

The entire spectrum of money is in disarray. Debt and inflation are plaguing fiat[2] while death spirals and depegs are threatening stablecoins[3].

This paper introduces a novel algorithmic stablecoin called the Argon. It is the first stablecoin to function as a form of commodity-money, and it requires zero “collateral" for stabilization. It uses basic economic principles to create Unrestrained Profit Incentives (UPIs) that sit on both sides of the stablecoin’s target price. This allows for minor fluctuations while achieving long-term stability through rational self-interest and profit maximization. These profits are realized via blockchain-native synthetic derivatives that are exogenous to the stablecoin and functionally isolated from fluctuations in market sentiment.

The result is a self-balancing system where the further Argon 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. There are only two scenarios in which this stablecoin could collapse. The first requires 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. The second requires a complete collapse of crypto, including the entirety of Bitcoin’s market value.

The final half of this paper lays out the proof behind Argon’s stabilization mechanism. Even if it loses 99.999% of its value, it will still rebound back to its target price within days. Further, it requires no external capital for its re-stabilization. This capability distinguishes Argon from all other crypto stablecoins.

The History of Currency

Let’s start with some context. Argon is only the latest in a long line of currencies with commodity-money being the earliest. Each subsequent evolution successfully solved the primary weakness of its predecessor, while at the same time, inadvertently introducing a new weakness.

- **Commodity-Money**. In 3000 BCE, grain began being used as a medium of exchange[4]. It was a huge improvement over bartering. Its value was durable, divisible, and had a relatively stable value. Precious metals soon replaced grain as it had even better durability and long-term stability[5]. However, all forms of commodity-money suffer from significant transferability issues, particularly in large quantities over long distances[6].

- **Representative-Money**. Paper IOUs came into existence during the Tang dynasty of 617 - 907 AD[7]. They represented commodity-money’s value without requiring the physical movement of heavy assets. It was a huge leap forward in transmissibility, and yet it created an entirely new weakness. Whoever holds the gold can quietly print more paper and debase the currency at will. Inflation and banking panics (death spirals) entered the world[8].

- **Fiat-Money**. Every form of representative-money has eventually succumbed to overprinting. The results are either complete collapse or a forced conversion to fiat. In 1971, the dollar arrived at such a moment. Nixon did what every government has done when faced with such a challenge: convert the currency to fiat by force of decree[9]. In moving off the gold standard, Nixon saved the United States from a national banking panic, and in doing so, he exacerbated the problem of inflation. Fiat imposes zero printing limitations, and as a result, every fiat system in history has imploded.

- **Bitcoin-Money**. Satoshi designed Bitcoin to be immune from overprinting or inflationary debasement[10]. As such, it operates independent of fiat, and its digital nature provides unsurpassed transmissibility and durability. However, it has one major weakness: extreme pricing volatility. This volatility renders it unusable as a stable medium of exchange in everyday commerce.

- **Algorithmic Stablecoins**. The first stablecoin was launched ten years ago[11]. It sought to create a stable-priced cryptocurrency that would be as fully decentralized as Bitcoin. Multiple algorithmic stablecoins have launched since then[12]. All have shutdown or imploded due to one of two issues. Either their endogenous token structure created a self-perpetuating destruction loop or their underlying decentralized assets exhibited too much volatility to be financially viable.

- **"Collateral-backed" Stablecoins**. "Collateral-backed" requires quotes because these stablecoins have no "collateral" that matches any known financial definition of the word. Issuers basically accept unsecured loans from their users and earn interest off their users' money. They operate as fractional reserve banks without being regulated as banks. This adds huge risk to their users without offering FDIC insurance guarantees. A simple investigation of these stablecoins makes it clear they're a single black swan event away from complete collapse[13].
- **Central-bank Digital Currencies**. CBDCs are touted as the final evolution of digital money. They remove the underlying instability of stablecoins by using force of fiat. However, they also bring huge dangers to society because of the totalitarian control they offer over political dissidents or anyone else who steps out of line[14].

On The Stabilization of Collateral-Backed Stablecoins provides a more detailed analysis of the history outlined above. In short, we believe the current stablecoin industry is at a dead end.

A growing body of research indicates that fully decentralized stablecoins are economically impractical if not wholly unfeasible[15]. They show that stablecoins carry a high risk of death-spiraling unless they use exorbitant levels of over-capitalization, which becomes financially insoluble when applied on a global scale. However, this body of "research" has also only examined "collateral-backed" stablecoins and/or the very limited set of previously tried algorithmic models.

Notwithstanding the failure of past algorithmic stablecoins, we believe algorithmic stablecoins are the ideal structure for a successful global currency. However, the previous ideas do not work, and a fundamental rethink is required.

A. BASIC PRINCIPLES

Four core beliefs underlie many of Argon's design decisions. This section briefly summarizes them.

A.1 - Bad Currencies Don't Make Good

Wrapping fiat currency with a crypto token does not eliminate fiat's underlying issues. It merely adds extra complexity and risk.

Over 99.9% of stablecoins are pegged to fiat currencies, primarily the dollar[16]. Regardless of whether they're synthetic or "collateral-backed" stablecoins, as the dollar is debased so is the stablecoin. Today's stablecoins are basically representative-money with fiat underlying it. As history has shown, representative-money never holds more long-term value than the asset backing it. It's always worth less. This is because representative-money carries risk that the issuer might not redeem its IOU (I owe you).

There are numerous reasons why the promise to redeem might fail. A coding bug could exist in the stablecoin protocol allowing for theft or other havoc, there could be fraud among management who drains the coffers, or there could be issues at the banking custodians who hold the "collateral." Regardless of the probabilities, when you account for all the entities and algorithms that must be trusted for a stablecoin to operate, it's obvious that holding a stablecoin carries significantly more risk than holding a physical dollar.

The deeper issue is that the dollar itself is not a sound financial asset. Over the last one hundred years, the dollar has lost 96% of its value[17]. By pegging to the dollar, stablecoins are inheriting the same inflationary debasement issues as the dollar, while at the same time, stacking it with the additional aforementioned risks of protocol bugs, management fraud, and custodian problems.

So why is $166B[18] in capital sitting in these stablecoins? It's because stablecoins are the "most stable" of the extremely price volatile crypto markets. The market overwhelmingly uses them as temporary trading conduits for moving in and out of crypto trades. However, existing stablecoins have little to no fundamental properties that fix the dollar's problems.

No dollar-pegged stablecoin can ever hope to become a major world currency because it can never outrun the inflationary debasement and stability concerns of the fiat to which it's pegged. The larger it grows, the more dollars it holds in reserve. This creates a situation where increased growth creates increased risk of a collapse impacting the broader financial system, and therefore it stands a greater chance of being swallowed into a government CBDC. And the moment it's swallowed into a CBDC is the moment it ceases to be fiat-pegged. It become fiat itself.

We believe the only way to fix the mounting issues of debt and inflation around the world is to create a stablecoin that can remain stable without needing fiat. The worlds needs a truly sound digital currency, one that's an alternative to fiat, not one that compounds the existing problems.

A.2 - Central Points of Failure Ensure Failure

Many stablecoins describe themselves as decentralized because they allow 3rd parties to participate in network activities. However, at the core of their networks are centralized entities that, if disabled, would cause the entire system to break. One of the most obvious is "collateral" custodians. Custodians are centralized entities the hold the physical assets and requires trust. Shutting down the custodians shuts down the stablecoin.

Centralized stablecoins like USDC and USDT obviously use centralized custodians, but so do seemingly decentralized protocols like MakerDao and Frax[19]. Instead of direct custodianship of physical dollars, these decentralized protocols hold 3rd-party tokens which custodian the physical dollars.

Regardless of who serves as custodian, the life and death of these stablecoins reside in the trustfulness of the custodians. They become the central point of failure, and they become the central lever by which these stablecoins can be controlled.

As Murphy's Law dictates, given enough time, everything that can go wrong will go wrong. When you tokenize a physical asset, such as fiat currency, there is no onchain guarantee that the physical asset actually exists. Custodians can say one thing and do another. Even more concerning, future governments could exploit these assets to impose oppressive controls and threaten individual freedoms.

One reason Bitcoin has stood the test of time is because it operates as a true independent currency. It is not an IOU for another asset. It stands as its own unit of value, as currency, collateral and commodity.

We believe the world needs a stablecoin without centralized "collateral" custodians or any other type of centralization in its core stack. Only by creating a stablecoin with no centralized point of failure can a durable digital currency be guaranteed to last beyond the lifetime of any single nation-state.

A.3 - Great Currencies Operate As Rubber Bands

Only subservient currencies rely on pegging; independent currencies do not. Pegging ties a currency to an anchor by locking its exchange rate in a rigid grip. The primary benefit of pegging is it offloads the complexities of currency management to its anchor. As outlined in our first whitepaper, pegging creates a brittleness that sets the stage for banking panics and death spirals. Pegged currencies either maintain their peg or they don't, and when they don't, they often implode[20]. The most well-known implosion was the British pound in 1992, when George Soros famously "broke" the Bank of England[21].

A significant percentage of the currencies in operation today are pegged to an anchor currency, with most of them pegged to the dollar. Nearly all stablecoins use pegging.

Targeting is very different from pegging. Targeting allows a currency to fluctuate within flexible pricing bands that follow the natural movements of economies. It provides the governing authority with the freedom to enact policies that influence the currency toward specific pricing targets without limiting possibilities. This is how the United States dollar operates. The Japanese yen, the Eurozone euro, and the Swiss franc also follow this approach.

We believe targeting is the most viable approach for an algorithmic stablecoin with global ambitions. Only by operating outside the confines of the dollar can a stablecoin avoid the inevitable conclusion of being assimilated into a CBDC[22].

A.4 - The Best Currencies Are Served Hard

In the world of currency, "hard" means no inflation or deflation. In contrast, Argentina's peso is the poster child for a soft currency — it has experienced runaway inflation of more than 40% a year for the last five years running[23].

Throughout history, all currencies have had inflation, even gold[24]. Every time an ounce of gold is mined, it inflates the circulation. Nevertheless, gold has one of the lowest inflation rates of all the world's currencies, which is one of the primary reasons it has been held in high esteem over millennia.

Inflation is a problem because someone is profiting at the expense of the rest. Inflation erodes one of the fundamental properties of money, which is that it should be a safe store-of-value for everyone who holds it.

We believe a properly designed algorithmic stablecoin has the potential to do what no other currency has done before (not even gold): become the world's first truly hard currency with zero inflation or deflation.

Note: This paper only addresses the properties needed for stabilizing to a target price. It does not seek to determine what that that price should be. Those details — such as measuring inflation and implementing an inflation index — are beyond the scope of this paper. Please see our third whitepaper, *Bootstrapping a Global Currency*.

B - BASIC ARCHITECTURE

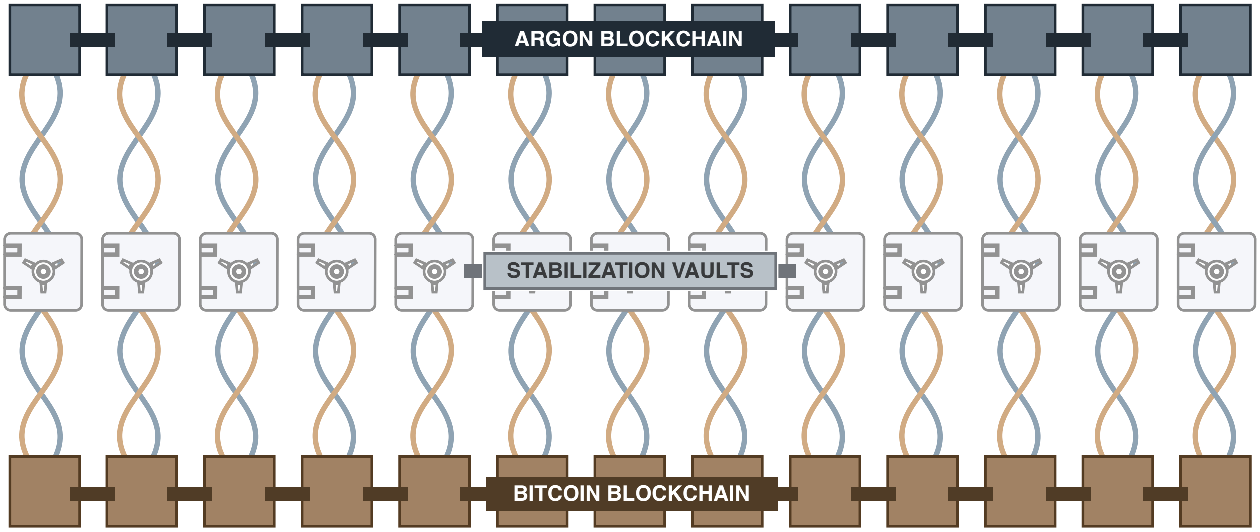
This section presents some of the broad architectural elements of Argon. It's not meant to address the technical details but merely to communicate some of the high-level concepts that are helpful in setting a proper context for understanding our stabilization mechanisms.

B.1 - Two Blockchains

Argon is a fully independent, useful-proof-of-work blockchain. It does not require an existing Bitcoin Layer 2 (L2) network. Instead, it directly integrates into Bitcoin through a series of Stabilization Vaults using our novel Dual Signature Time Lock (DSTL) protocol. See Section D.

Stabilization Vaults lock bitcoins on the Bitcoin blockchain. In doing so, they mint argons on the Argon blockchain. This helps stabilize Argon's price, and it provides bitcoins with full hedging from any downside risk.

FIGURE B.1.1 — THE ROLE OF VAULTS IN LINKING THE BLOCKCHAINS



B.2 - Three Crypto Tokens

Argon uses a three-token structure:

Argon Stablecoin. Argon is the network's stablecoin token and primary unit of measurement. Each unit is divisible up to six decimal places (one one-millionth of an argon), the smallest of which is a microgon. Argon will initially be valued at $1.00, but as it is targeted to an inflation index, its value will continuously appreciate against the dollar as inflationary debasement of the dollar progresses.

Ownership Tokens. These are earned through participation in running the network, and their supply is capped. Similar to Bitcoin, Ownership Tokens are mined at a rate that halves approximately every 1,458 days, and their total quantity is forever capped at 21,000,000. The token's fundamental value comes from exclusive rights to participate in the network’s mining and minting of new argons. Whenever demand for argons increase, Ownership Tokens, together with bitcoins, gain the right to mint new ones.

Bitcoin Tokens. Bitcoins serve as the core store-of-value within the Argon network. They integrate into the Argon blockchain through Stabilization Vaults, and they serve two purposes. Whenever demand for argons increase, bitcoins, along with Ownership Tokens, are awarded the right to mint new ones. Second, all vaulted bitcoins naturally short the Argon, and if the currency ever drops below its target price, bitcoins have the right to cover their shorts and earn profits by burning excess argons from circulation.

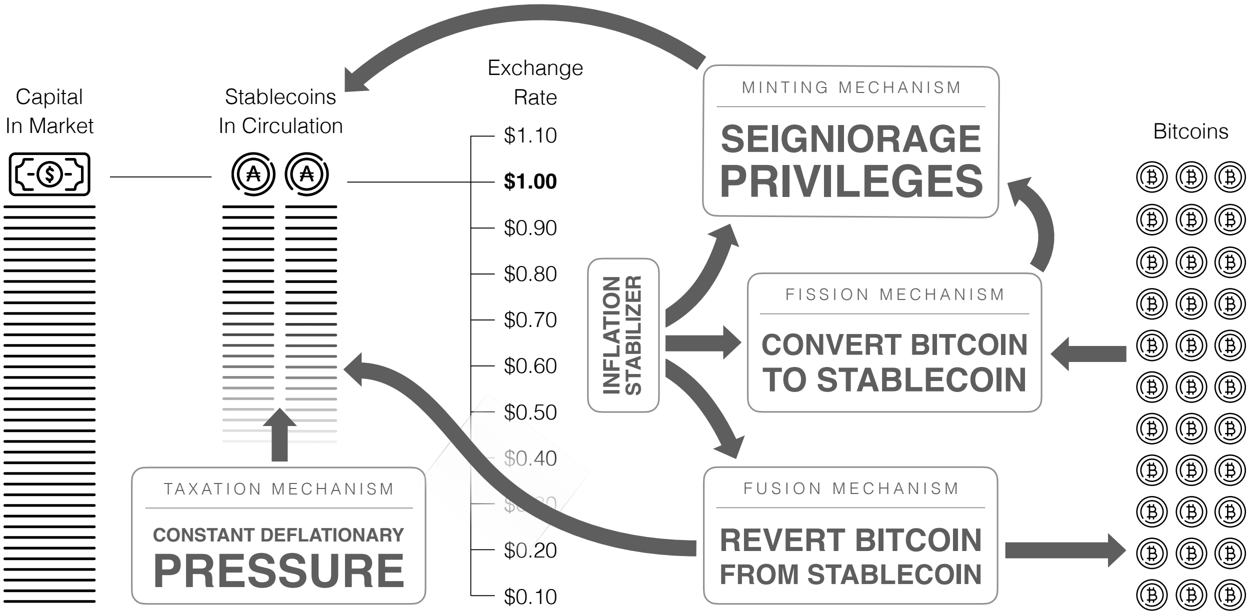
B.3 - Four Stabilization Mechanisms

Argon has four stabilization mechanisms that operate as Unrestrained Profit Incentives to keep the currency at its target price. Two are triggered when the price increases above target; two are triggered when it drops below target. The further argon deviates from its target, the greater the opportunity.

All four stabilization mechanisms are exogenous to Argon’s ability to stabilize, meaning no participant is required to hold endogenous tokens or otherwise entertain the risk of whether argon re-stabilizes.

The following illustration shows a high-level overview of the basic components.

FIGURE B.3.1 — THE FOUR STABILIZATION MECHANISMS



Fusion Mechanism. Fusion is the process by which a Bitcoin is locked into a Stabilization Vault and is then split into two assets: newly minted argons + a Bitcoin Option. It doing so, the bitcoin owner is able to fully hedge their downside risk. See Sections C (Embracing the Law of Supply & Demand) and D (Bitcoin Endosymbiosis).

Fission Mechanism. Fission is the process by which a bitcoin is unlocked from a Stabilization Vault and handed back to its original owner. In doing so, argons are burned from circulation. Depending on Argon’s market price relative to its target price, the quantity of argons burned could be as high as 27,000,000% greater than the value the bitcoin being unlocked. See Sections C (Embracing the Law of Supply & Demand) and D (Bitcoin Endosymbiosis).

Minting Mechanism. Minting is the algorithm that ensures Ownership Tokens and Bitcoin Tokens share a 50/50 split in the creation of new Argon stablecoins. Read more in Section E (Seigniorage Privileges).

Taxation Mechanism. Taxation exerts a constant upward pressure on Argon’s price. It uses internet-native economic networks and cryptographical authorities to enforce the tax and burn the argons from circulation. See Section F (Constant Deflationary Pressure)

All four of these mechanisms work in harmony, and they're independent of whether the market believes the Argon will ever hold a stable value. This is because all four mechanisms depend on exogenous assets and profit incentives external to the stablecoin. In short, no future black swan event affecting the stablecoin can trigger a death-spiral. Participants will realize their profits regardless of whether Argon's price ever rebounds to its target — these two events are mutually exclusive.

C. EMBRACING THE LAW OF SUPPLY & DEMAND

Supply and Demand (S&D) is a fundamental concept of economic theory. It describes how, in a competitive market, the unit price for a particular good will vary until it settles at a point where the quantity demanded by consumers will equal the quantity supplied by producers, resulting in market equilibrium. This section lays out the basic premise for how Argon's stabilization mechanisms leverage the law of Supply and Demand to create price balance.

C.1 - Fluctuations Are Inevitable

The first rule of stablecoins is that they are never truly stable. Although they're designed to maintain stability, fluctuations naturally occur as capital flows in and out. The formula below illustrates the fundamental price at which a market will ultimately settle, assuming all other variables remain constant: price equals demand divided by supply.

Formula for Determining Price Based on the Law of Supply and Demand

$$P = D / S$$

In this formula:

P := The market price of the stablecoin

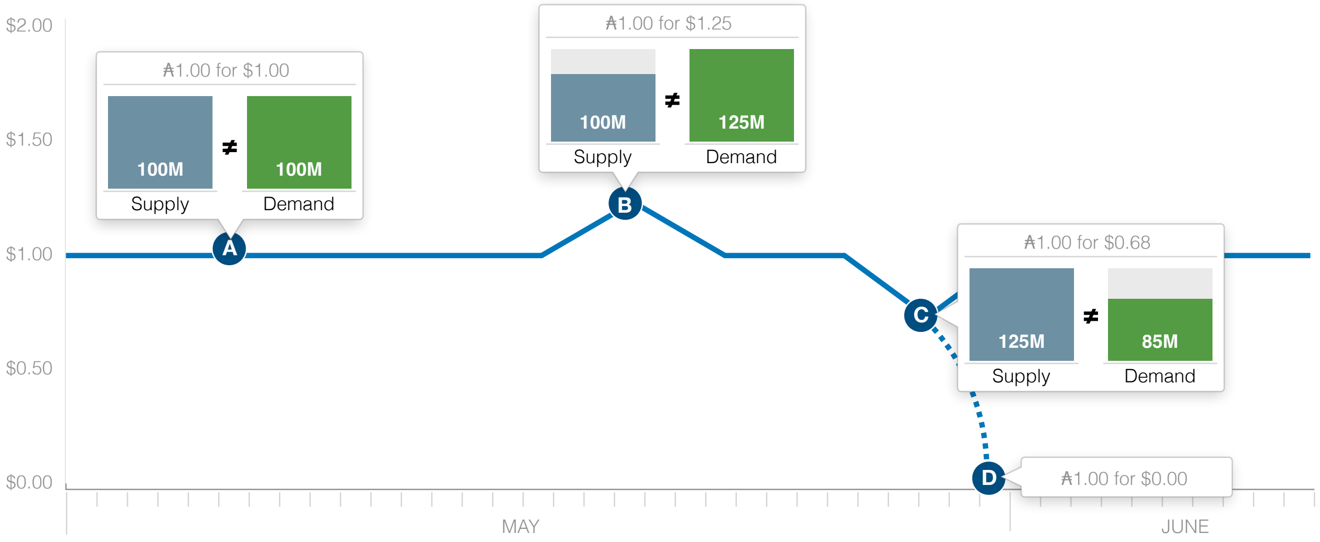
D := The total amount of capital driving demand in the market

S := The total supply of stablecoin tokens

The true measure of a well-designed stablecoin is its ability to withstand black swan events because, given enough time, black swan events are going to happen[25].

Figure C.1.1 shows the four basic pricing positions of a stablecoin: stable, over-priced, under-priced and dead. The market price naturally floats based on the balance (or lack of balance) between supply and demand.

Figure C.1.1 — The Fluctuation of Price Based on the Law of Supply and Demand



Position A shows a stable price, in this case, one argon for one dollar. It means the Law of Supply and Demand is in balance — the same quantity of argon tokens have been created (supply) to match the amount of capital that has moved in (demand).

Position B is a stablecoin whose price has risen too high. The market is demanding more units of currency than exists in circulation, which drives the dollar-to-stablecoin price above target. The solution is to mint more currency, 25M to be exact. In the world of digital, it's as simple as incrementing an integer. Injecting this new currency into the market increases circulation and drives the price back down to target.

Position C shows demand dropping below supply. The Law of Supply and Demand asserts that there are only two ways to regain the token's target price: a) increase demand by convincing more outside capital to enter the market and "catch a falling knife" or b) remove excess supply by burning tokens. If neither of those happen, the market will begin to lose confidence in the stablecoin as a stable currency. If the stablecoin is "collateral-backed" then in all likelihood the currency will quickly enter a death spiral and fall to worthless.

Position D is a stablecoin at the end of its death spiral. All demand has left the market.

Managing the Law of Supply and Demand is complicated within currencies, especially when supply exceeds demand (i.e., as in Figure C.1.1.C). Convincing more capital (demand) to move in when the stablecoin has already depegged is expensive, and the opposite approach of reducing supply is equally complicated — few one want a centralized entity, or even a decentralized entity for that matter, to "fix" the imbalance by reaching into users' accounts and reducing their net worth.

Governments use the Law of Supply and Demand to adjust currency, but they do so in ways that are rarely visible to the general populace. For example, instead of reaching into users' bank accounts, the Federal Reserve uses Treasury bonds to manipulate the supply lever and interest rates to restrict/ease the demand lever[26].

C.2 - Four Ways to Stop a Death Spiral

There are four basic ways to stop a stablecoin from death spiraling:

1. **Guarantee Abundance of Reserves**
   This is a critical requirement for "collateral-backed" stablecoins. It ensures liquid reserves with a total value equal to or greater than the total value of stablecoin tokens in circulation. However, supplying enough reserves to reduce the probabilistic occurrence of a death spiral is costly, to the point of being financially untenable at a global scale. Regardless of the quality or quantity of its underlying reserves, one can never predict when a black swan event will cause theft or loss of reserves, but when it spirals out of control, another level is required.

2. **Raise Emergency Capital**
   When a "collateral-backed" stablecoin is free-falling and user redemptions are outstripping cash reserves, additional outside capital must be funneled in to replenish the reserve gap. USDC faced this exact scenario during the Silicon Valley Bank collapse of March 2023. USDC's issuer, Circle, experienced a reserve shortfall of nearly $4B[27]. They called an emergency halt of USDC redemptions[28] while they explored capital options. Lucky for them, the government stepped in to guarantee SVB's depositors[29], which brings us to the force of fiat.

3. **Leverage the Force of Fiat**
   This suspends the Law of Supply and Demand. It's what Nixon did in the summer of 1971 when he stopped a possible run on the dollar by nationalizing gold holdings and decreeing the dollar as fiat. It's also similar to what the U.S. government did March of 2023 when they saved Silicon Valley Bank and with it, the USDC stablecoin[30]. Continued use of fiat force creates a natural move towards CBCDs which creates authoritarian-control risks for society as outlined in our first whitepaper.

4. **Implement Oppositional Market Forces**
   It's possible to setup derivative-like financial triggers that effectively function as calls, puts and shorts in order to stabilize a currency. The result is a currency where the greater it deviates from its target price, the greater its profit incentives force it back into line. The challenge is that engineering an economic system to fully hedge all possible risks usually consumes as much capital as simply guaranteeing an overabundance of reservers.

The rest of this paper will explore the details of using oppositional market forces to stabilize a stablecoin.

C.3 - Oppositional Market Forces

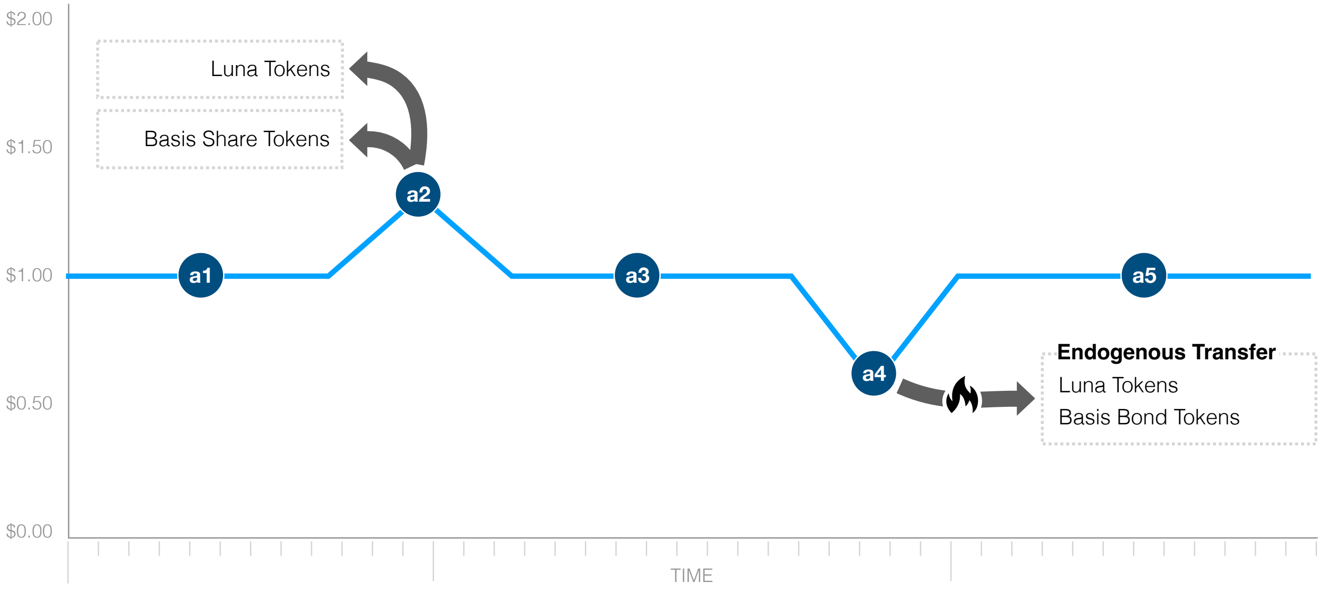
Setting up oppositional market forces to counterbalance a stablecoin's price fluctuation isn't new. All previous algorithmic stablecoins have attempted this to some extent. Argon's novelty lies in the way it flips one key component (step a4 of Figure C.3.1). To help explain, let's briefly explore two prior stablecoins.

The Endogenous Mistake of Basis and Terra

Basis and Terra are two of the more prominent algorithmic stablecoins from the last ten years. Basis was announced in 2017 with a $133M investment from Andreessen Horowitz, Bain Capital Ventures, and others[31]. It shut down on December 13, 2018[32]. Terra launched in 2020[33] and imploded in May of 2022[34].

Both stablecoins made the mistake of using endogenous incentives to reward those who participated in its stabilization mechanisms. Figure C.3.1 shows their basic flow.

Figure C.3.1 — The Stabilization Flow of Basis and Terra



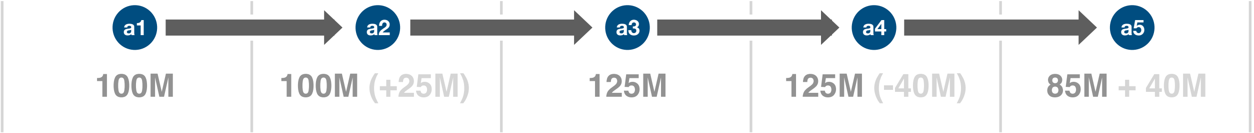
- a1 Basis and Terra worked great when the price was stable.
- a2 Basis and Terra worked great when prices rose above target. Basis transferred the value of new stablecoins to its Share Tokens by directly minting and selling new stablecoins on the open market. Terra used a more complicated process to indirectly transfer value to Luna holders. Regardless, no stablecoins have ever failed as their prices increased.
- a3 Basis and Terra had no issues in bringing their price upswings back down to target.
- a4 The downswing is where Basis and Terra went awry. Their mechanisms for removing stablecoins from circulation used endogenous tokens. At first glance they appeared to reduce the supply, however, in reality they merely shifted the excess circulation from one internal ledger to another. Although the second token appeared to be separate, it was still part of the stablecoin's protocol, and as such, the excess circulation was merely shifted to a new name.

In 2021, Professor Christian Catalini published a detailed analysis on endogenous loops within algorithmic stablecoins[35]. He showed that once the price dips below a certain threshold, the benefits flips, and endogenous capital incentives stop acting as death-spiral prohibitors and begin acting as accelerants. One year later Catalini was proven correct during Terra's stunning collapse.

Figure C.3.2 shows the stablecoins in circulation during the various steps of Figure C.3.1. For example, during step a2, 25M tokens are added to satisfy demand, which brings the total circulation to 125M. However, in step a4, the

40M burn is an endogenous transfer. As a result, 125M total (endogenous + stablecoin) token value still exists in step a5 even if technically there are only 85M stablecoins.

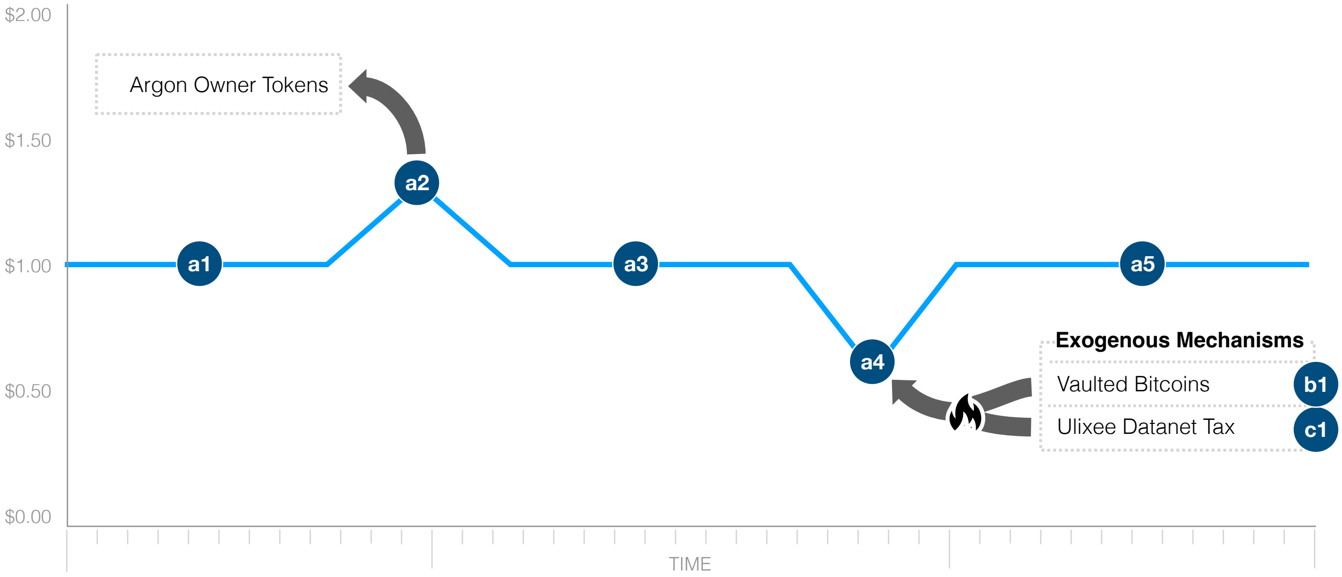
Figure C.3.2 — The Circulation Fluctuations of Basis and Terra



The Exogenous Design of Argon

Argon flips the endogenous transfer of step a4 in Figure C.3.1 to an exogenous mechanism as shown in C.3.3. This completely burns the excess stablecoins from existence, and in doing so, the death-spiral inducing loops of Basis and Terra becomes a death-spiral impossibility in Argon.

Figure C.3.3 — The Circulation Flow of Argon

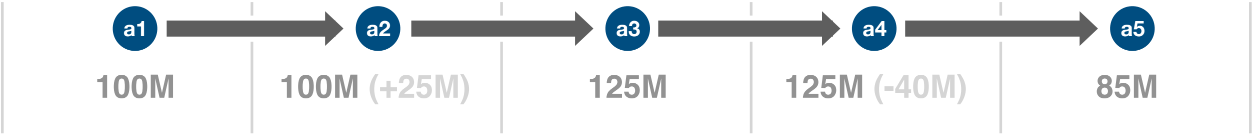


Argon is very similar to Basis in step a2 in that it uses a direct minting mechanism to transfer economic value to Ownership Tokens and Bitcoins (see Section E).

The key to Argon's exogenous mechanisms is that they're not just conduits into exogenous assets. They have a much more compelling property in that their incentives operate independently of the stablecoin's stabilization needs. For example, the market has reason to vault bitcoins (see Section D.10, Understanding Bitcoin Economics) and participate in the Ulixee Data Network (see Section F.3, Ensuring Effective Burn) regardless of any belief in the stablecoin itself. Therefore none of Argon's stabilization mechanisms rely on the stablecoin's probability of success or the market's belief in it. Stabilization is driven purely by external profits.

Figure C.3.4 shows the number of argons in circulation as supply and demand fluctuate. The final step looks very different from Basis and Terra (see Figure C.3.2). With Argon, none of the 40M burned tokens are moved into an endogenous bucket. Instead they are completely deleted. Gone from circulation.

Figure C.3.4 — The Circulation Fluctuations of Argon



D. BITCOIN ENDOSYMBIOSIS (FISSION + FUSION MECHANISMS)

Bitcoin has a special relationship with the Argon whereby Argon eats Bitcoin by converting it into a stablecoin. Simultaneously, Bitcoin becomes the underlying store-of-value and foundational bedrock of the Argon. Within this process of endosymbiosis, Bitcoin's downside pricing risk is hedged, creating opposing market forces: as Argon's value falls, the profit incentives increase, accelerating its return to target price.

D.1 - Liquid Locking

Argon's integration with Bitcoin exhibits economic properties akin to liquid staking. As with staking, bitcoins are used as an underlying representation of value on the Argon chain, and in doing so, they are able to earn profits from their assets. They're also able to receive full liquidity at their bitcoin's current market price in the form of secondary tokens, the Argon stablecoin. However, Argon implements none of the penalties that are commonly associated with staking. Bitcoins are simply locked into Stabilization Vaults with no possible penalties and with a guaranteed ability to unlock whenever the owner desires.

Stabilization Vaults are special lightweight anonymous software entities within the Argon ecosystem that ensures bitcoin locking and unlocking rules are followed. Instead of using risky bridges or centralized custodians to connect the chains, Stabilization Vaults use a profoundly simpler mechanism called Dual Signature Time Locks (DSTL). It guarantees that bitcoins remain cryptographically non-transferrable on the Bitcoin blockchain while they are actively engaged within Argon. See D.6 for details.

D.2 - Mechanism Triggering

Fission and Fusion are the two stabilization mechanisms that activate when Argon's market price rises or falls outside its target price.

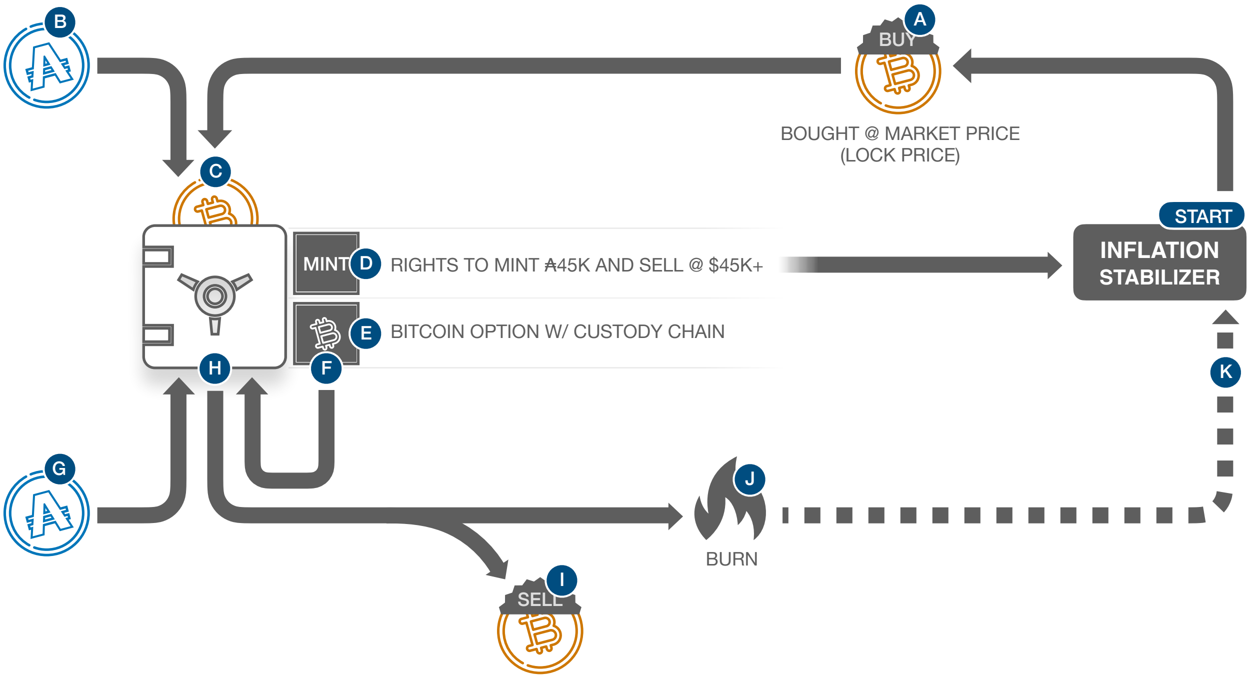
When Argon exceeds its target price, the Fission Mechanism enables bitcoins to be moved into Stabilization Vaults, which splits the bitcoin into multiple assets, including the minting of new argons. These new argons helps satisfy market demand, which brings the price back down to target. It also gives bitcoins an ability to short the argon if it ever drops below target.

When Argon falls below target price, bitcoins held in Stabilization Vaults can profit by covering shorts against the argon. This process is called Fusion since it recombines the assets that had previously been Fissioned. Doing so results in a rapid, large-scale burning of excess argons from circulation, helping bring the price back up to target.

D.3 - A High-Level Flow

Let's walk through the story of a single Bitcoin as it goes through the process of locking into a Stabilization Vault (Fission) and unlocking (Fusion).

Figure D.2.1 — Fissioning and Fusioning a Bitcoin



The flow begins with the Inflation Stabilizer (START). Whenever argon's market price has risen above the target price (i.e., more supply is demanded by the market), anyone who has a bitcoin (A) can submit their bitcoin into a Stabilization Vault (C). The Inflation Stabilizer is beyond the scope of this whitepaper (see our 3rd paper for more details), but the short summary is that it uses an oracle mechanism to measure inflation.

A security fee (B) is required. This fee ensures the honesty of the Vault, and it provides an insurance guarantee for bitcoin owners. More on this in Section D.8, Understanding Vault Security.

Transferring a bitcoin into the vault requires moving it to a new address on the Bitcoin network using a custom multisig script. At its most basic, the multisig requires two keys for unlocking: one key is held by the Vault, the other by the bitcoin owner (see Section D.6, Dual Signature Time Locks).

Once the bitcoin (A) and security fee (B) are inserted into the Vault (C), the bitcoin owner receives two things.

First is the right to mint a new batch of argons (D) equal in value to the current market price of bitcoin as determined at the moment of locking. These newly minted argons are unencumbered, meaning they can be transacted, held or sold as the owner wishes. Since bitcoins are only allowed to vault during moments when the Inflation Stabilizer shows Argon demand is outstripping supply, these argons have a ready market.

By selling their argons, the owner fully hedges their bitcoin's downside risk. They now have the cash equivalent in hand and are therefore indifferent to Bitcoin's price falling. Selling argons also helps stabilize the market by increasing supply and bringing the price back down to target.

The second asset is a Bitcoin Option (E), which allows the owner to unlock their bitcoin (no change of custody) at any time within the following year so long as the requisite number of argons are inserted back into the Vault. It is important to note that bitcoin owners must explicitly unlock (and relock if they choose) at year's end. Vaulting each year might seem onerous, but it's similar to keeping your internet domain name registered — it requires only a few seconds of work, and it's key to ensuring the operational and security guarantees of the system. We expect a plethora of productized services to emerge in the marketplace to assist in this process. However, users who fail to participate in unlocking and/or relocking at the end of each year have no negative affect on the system itself. They are simply allowing others to step in and take their spot.

Bitcoins can be reclaimed at any time by inserting the Bitcoin Option (F) and required argons (G) back into the Vault. The number of argons required is specified in Section D.5 (The Details of Unlocking a Bitcoin), but basically it's the current market price of Bitcoin capped at the market price of when it was originally vaulted. So if a bitcoin was vaulted at $45k and the market drops to $35k, then only $35k worth of argons are needed to unlock it. The extra

$10k is retained by the bitcoin owner. Similarly, if it was vaulted at $45k but the prices rises to $90k, then only $45k worth of argons are needed. This fluid movement between the dollar and argon does not negate or diminish the value of the argon or the effectiveness of Argon's stabilization capabilities. It merely mixes argon custody.

Once the Bitcoin Option and argons have been inserted into the vault (H), the bitcoin is unlocked and full control is transferred back to the owner (I). The inserted argons are then burned (J). This act of burning ensures excess argons are completely destroyed from circulation. This helps drives the price back up (K), making room for other bitcoins to vault.

D.4 - The Details of Locking a Bitcoin

Locking bitcoins into a Stabilization Vault is relatively straightforward. The following steps assume you already own one. The minimum that can be vaulted in a single transaction is one satoshi. There is no maximum.

Note that four different actors are described within these steps: the Bitcoin Owner (Owner), the Stabilization Vault (Vault), the Argon Mainchain (Mainchain), and the Bitcoin Blockchain (Bitcoin).

Step One Owner finds a Vault they want to use. Anyone can setup and run Vaults on the network, and each sets their own Security Fee (see Section D.8, Understanding Vault Security). There is no technical hard limit to the number of vaults that can exist in the system.

Step Two Owner submits a vaulting transaction to the Mainchain, which includes the public key they will use for locking their Bitcoin, the number of satoshis that will be locked, and the Mainchain account where their soon-to-be-minted argons will be deposited.

Step Three Mainchain and Vault process the incoming transaction, which includes the following steps: a) the current market price of Bitcoin is determined and set as the Lock Price, b) public keys that the Vault will use for the Bitcoin multisig are published, c) the required Security Fee is taken from the Owner's Mainchain account, and d) argons equivalent to the Bitcoin's market value is taken from the Vault and locked into the Mainchain as collateral.

Step Four Mainchain begins monitoring Bitcoin for a cosign script_pubkey matching the expected movement of satoshis being locked. This can be independently determined. This is because each node can build the miniscript with the public parameters to determine the script_pubkey, and all transactions submitted to Bitcoin are public.

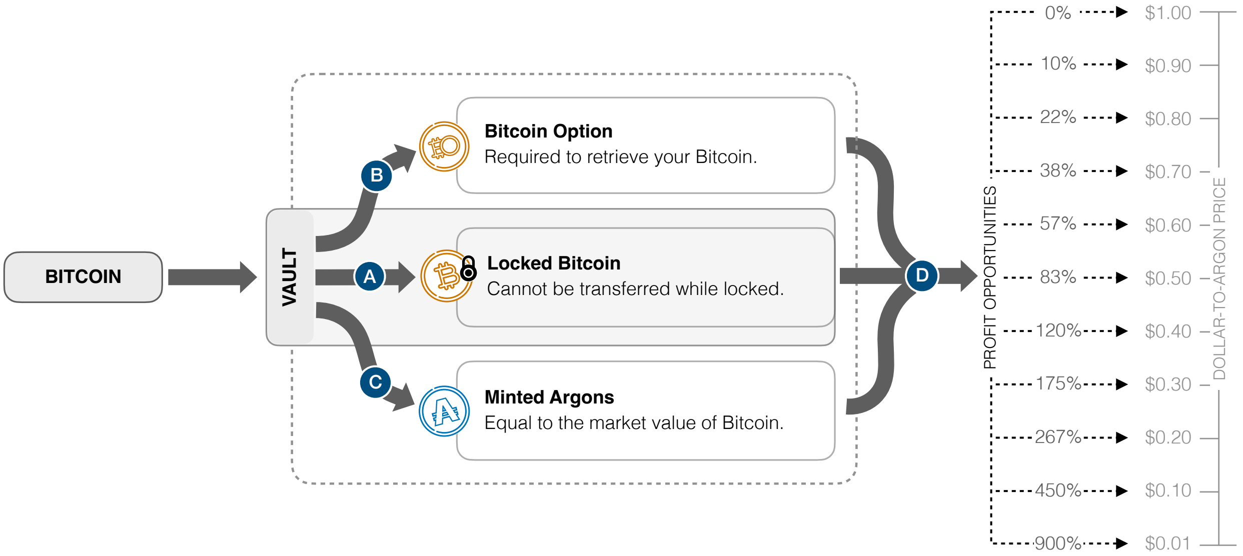
Step Five Owner sends their committed satoshis to the script_pubkey on Bitcoin. There is no time limit on when they must do so, except that the process can proceed until they do so, which means the Owner will not receive any argons or other value from locking.

Step Six Mainchain confirms the locking of satoshis on Bitcoin and adds the corresponding argons needed for minting to the Minting Queue (see E.3).

Step Seven Whenever Argon minting is allowed (see Section E), the newly minted argons are added to the Owner's Mainchain account.

The above steps are collectively referred to as the Fission Mechanism because it splits a bitcoin into three separate assets as shown in Figure D.3.1.

Figure D.3.1 - Fission Spliting Bitcoin Into Three Parts



A **Locked Bitcoin**. The original bitcoin is cryptographically and economically locked so that it cannot be moved or transferred except under certain circumstances (see Section D.5, The Details of Unlocking a Bitcoin).

B **Bitcoin Option**. This is a special virtual token that allows the owner to unlock their original bitcoin when certain conditions are met (see Section D.5, The Details of Unlocking a Bitcoin).

C **Minted Argons**. These newly minted argons are equal in value to the current market price of the Locked Bitcoin. They are free and clear to be spent, transferred, or used however the owner wishes.

D **Profit Opportunities**. Stabilization Vaults give bitcoin owners three profit opportunities. First, it provides full liquidity through the creation of newly Minted Argons — these can be converted into other investments or held as inflation-resistant assets. Second, it opens up low-risk opportunities to profit from Bitcoin market volatility. Finally, the value of Locked Bitcoins can be applied as a short against any future drop in Argon pricing.

Fission's locking mechanism closely resembles collateral that is commonly bound to loans. In fact, thinking of newly minted argons as a loan is perhaps the easiest way to understand the process. Imagine you have a bitcoin with a market value of $45k. You place this asset into the Vault and receive an Argon "loan" equal in value to $45k. The Locked Bitcoin sitting in the Vault is your "bound collateral," and the Option to Unlock is your "collateral receipt." The analogy isn't perfect, but in many ways, you're creating an unencumbered, term-less, non-interest bearing loan that can be redeemed whenever you wish. This should not be confused with the collateral that Vaults are required to pledge (see D.8, Understanding Vault Security).

D.5 - The Details of Unlocking a Bitcoin

This section assumes a Bitcoin is already locked into the Vault. Unlocking requires three steps.

Within these steps are four different actors: the Bitcoin Owner (Owner), the Stabilization Vault (Vault), the Argon Mainchain (Mainchain), and the Bitcoin Network (Bitcoin Network).

`Step One`	Owner submits an unlocking transaction to the Mainchain. This includes the public key the Owner wants the Bitcoin moved to along with the base transaction fee that will be submitted to the Bitcoin Network. Additionally, the specified quantity of argons required for unlocking must be included (see Dynamic Unlocking Formula below).
`Step Two`	Vault has ten days to create a Partially Signed Bitcoin Transaction (PSBT) and publish their public key and signature from the PSBT back to the Mainchain. Failure to do so results in the Vault losing their security collateral, plus extra extra penalties (see Section D.8, Understanding Vault Security). Once the Vault has responded and Mainchain has validated, the Vault is freed from penalties.

`Step Three`	Owner collects the Vault's PSBT data from the Mainchain, creates the final transaction, then cosigns and submits to the Bitcoin Network. At this point, the bitcoin is unlocked and the Owner is back in full control.

The number of argons required for unlocking is determined by our Dynamic Unlocking Formula (DUF), which is shown below. It is designed to incentivize network participation, particularly in conditions where the Argon has deviated from its target price.

Dynamic Unlocking Formula

$$\text{ArgonsNeeded}(r, b) = \begin{cases} b & \text{if } r \geq 1 \\ b\left(20r^2 - 38r + 19\right) & \text{if } 0.90 \leq r < 1 \\ b\left(\frac{0.5618r + 0.3944}{r}\right) & \text{if } 0.01 \leq r < 0.90 \\ \frac{b}{r} \cdot (0.576r + 0.4) & \text{if } r < 0.01 \end{cases}$$

Where $r := \dfrac{A_c}{A_t}$ and $b := \min(B_c, B_v)$. Here

A_c := The current market price of Argon

A_t := The target price of Argon

B_c := The current market price of Bitcoin

B_v := The market price of Bitcoin at its time of vaulting

Let's breakdown DUF into its discrete parts.

The first condition of the formula is applied when the current market price of Argon is greater than or equal to the target price of Argon ($\text{if } r \geq 1$):

$$b := \min(B_c, B_v)$$

As shown above, when Argon is stable, the quantity of argons required for unlocking a bitcoin is the current market price of Bitcoin but capped at the market price from when it was originally locked. So if a bitcoin was locked when the market price was $45k then it will never cost more than $45k worth of argons to unlock it, regardless of how high Bitcoin rises. However, if Bitcoin's market price drops below $45k then only the lesser amount is required.

The second condition uses a rational-quadratic expression that is applied whenever Argon's market price drops below its target price but remains within a 99% drop window ($\text{if } 0.01 \leq r < 1$):

$$b\left(20r^2 - 38r + 19\right)$$

This scales the quantity of argons required for unlocking based on the current market price relative to its target price.

When Argon's value is barely below its target price, this multiplier ensures the number of argons required for unlocking is less than what would normally be required, which encourages Bitcoin owners to participate. For example, if Argon's price falls 1%, the profit collected by participating bitcoins is 2% (not 1%).

As Argon further deviates below target, the multiplier increases the number of Argons needed for unlocking, thereby allowing for a higher bitcoin-to-argon burn ratio while still ensuring bitcoin owners receive robust profits.

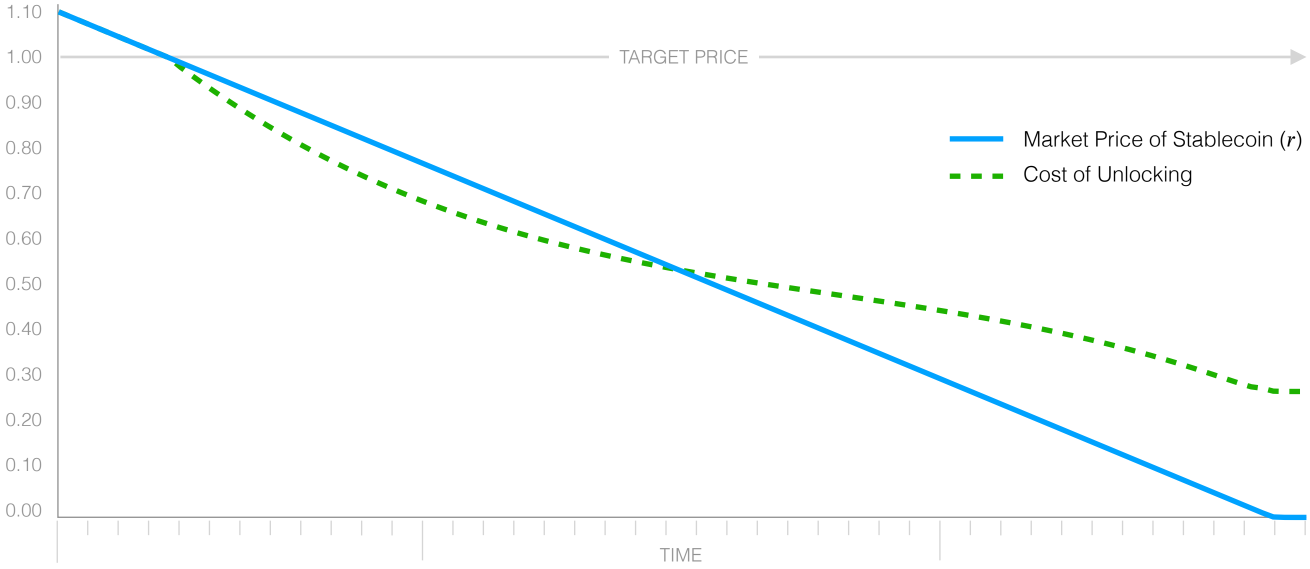
$$\frac{b}{r} \cdot (0.702r + 0.274)$$

When Argon's price drops more than 99% (if $r < 0.01$), the function flips to a rational-linear expression to maximize the burn slope and cap the profits at 265%:

This expression maximizes the burning of argons at the expense of great bitcoin profits (already at 265%) to ensure that even in the event of a complete collapse, if only a small handful of bitcoins are left in the vault, the entire circulation of excess argons can still be purged.

The following chart shows the cost of unlocking a bitcoin (green dotted), which is a combination of how many argons are required by DUF for unlocking as well as the cost to acquire them on the market. A second line (solid blue) shows the current market price of Argon as defined in the r variable above. The first 47% in price drop enhances the investment return for bitcoin owners at a rate greater than the actual drop. This incentivizes rapid participation and therefore rapid re-stabilization. As the price continues to fall below 50%, DUF begins prioritizing circulation burn, although vaulted bitcoins still maintain a healthy profit.

Figure D.5.1 - Relationship of Argon Market Price to the Cost of Covering Short



Most stablecoins that experience a 70%+ drop in value would be considered to be in a full-on death spiral with no hope of recovery. DUF creates the opposite scenario. The formula creates pricing leverage whereby a small handful of bitcoins can burn the entirety of excess circulation.

The following table shows the result of DUF at various Argon pricing levels (the first line shows how the formula works above target price). The price is shown in dollar denominations with the target price being set at $1.00, but this is only done for readability. Obviously, as an inflation-resistant stablecoin, the Argon's target price will rise over time relative to the dollar, but because of the r variable used within DUF, the ultimate outcome can never change.

Current ($)	BTC Price ($)	Argons Needed	Cost ($)	Profit	BTC Participation	BTC Leverage
1.10	45,000	45,000	45,000	0.00%		100%
...	...	...	...	...	...	...
1.00	45,000	45,000	45,000	0.00%		100%
0.99	45,000	44,550	44,105	2.03%	1.01%	99%
0.98	45,000	44,190	43,306	3.91%	2.04%	98%

0.97	45,000	43,845	42,530	5.81%	3.08%	97%
0.96	45,000	43,515	41,775	7.72%	4.14%	97%
0.95	45,000	43,200	41,040	9.65%	5.21%	96%
0.94	45,000	42,900	40,326	11.59%	6.29%	95%
0.93	45,000	42,615	39,632	13.55%	7.39%	95%
0.92	45,000	42,345	38,957	15.51%	8.50%	94%
0.91	45,000	42,091	38,302	17.49%	9.62%	94%
0.90	45,000	41,852	37,666	19.47%	10.75%	93%
0.89	45,000	41,628	37,049	21.46%	11.89%	93%
0.88	45,000	41,420	36,450	23.46%	13.04%	92%
0.87	45,000	41,228	35,868	25.46%	14.19%	92%
0.86	45,000	41,051	35,304	27.46%	15.35%	91%
0.85	45,000	40,891	34,757	29.47%	16.51%	91%
0.84	45,000	40,747	34,227	31.47%	17.67%	91%
0.83	45,000	40,619	33,714	33.48%	18.83%	90%
0.82	45,000	40,507	33,216	35.48%	20.00%	90%
0.81	45,000	40,412	32,734	37.47%	21.16%	90%
0.80	45,000	40,334	32,267	39.46%	22.31%	90%
...	...	...	...	...	...	...
0.70	45,000	40,510	28,357	58.69%	33.33%	90%
...	...	...	...	...	...	...
0.60	45,000	42,611	25,567	76.01%	42.24%	95%
...	...	...	...	...	...	...
0.50	45,000	47,055	23,528	91.26%	47.82%	105%
...	...	...	...	...	...	...
0.40	45,000	54,677	21,871	105.75%	49.38%	122%
...	...	...	...	...	...	...
0.30	45,000	67,424	20,227	122.47%	46.72%	150%
...	...	...	...	...	...	...
0.20	45,000	91,153	18,231	146.84%	39.49%	203%
...	...	...	...	...	...	...
0.10	45,000	155,251	15,525	189.85%	26.09%	345%
0.09	45,000	168,929	15,204	195.98%	24.24%	375%
0.08	45,000	185,904	14,872	202.58%	22.27%	413%
0.07	45,000	207,593	14,532	209.67%	20.16%	461%
0.06	45,000	236,364	14,182	217.31%	17.90%	525%
0.05	45,000	276,500	13,825	225.50%	15.46%	614%
0.04	45,000	336,612	13,464	234.21%	12.83%	748%
0.03	45,000	436,974	13,109	243.27%	9.99%	971%

0.02	45,000	639,364	12,787	251.91%	6.90%	1,421%
0.01	45,000	1,264,546	12,645	255.86%	3.52%	2,810%
...	...	...	...	...	...	...
0.001	45,000	12,361,590	12,362	264.03%	0.36%	27,470%
...	...	...	...	...	...	...
0.0001	45,000	123,331,590	12,333	264.87%	0.036%	274,070%
...	...	...	...	...	...	...
0.00001	45,000	1,233,031,590	12,330	264.95%	0.0036%	2,740,070%
...	...	...	...	...	...	...
0.000001	45,000	12,330,031,590	12,330	264.96%	0.00036%	27,400,070%

The BTC Participation column shows the maximum number of vaulted bitcoins that have room to participate at each price level. As Argon's price barrels toward $0.00001 the percentage allows to participate shrinks considerably. This triggers a binary first-mover race whereby every bitcoin is competing to participate, creating a situation where the further Argon falls the faster it will rebound. After all, who wouldn't want to collect a 264% return at basically zero percent risk? It's zero because covering the short requires zero concern for whether the argon ever rebounds.

D.6 - Dual Signature Time Locks

In this section we introduce Dual Signature Time Locks (DSTL), a novel mechanism for binding two heterogeneous blockchains. By utilizing owner-guaranteed multisigs with a three-layered sign-off process on Bitcoin, DSTL decouples locked assets from issued assets. This approach enables full liquidity on the Argon blockchain while eliminating the need for centralized custodians, risky atomic bridges, or extreme over-collateralization.

We expect there may be multiple use-cases for DSTL, however this paper is focused exclusively on DSTL's implementation within Argon. We will defer any efforts of generalizing it into a more broadly defined protocol..

DSTL was designed to ensure that bitcoins held in Stabilization Vaults are cryptographically and economically guaranteed to remain locked on the Bitcoin blockchain until the proper unlocking process is complete. This prevents bitcoins from being double-used on both chains simultaneously.

Existing Cross-Chain Technologies

The concept of transferring assets across blockchains dates back to at least 2013, when Tier Nolan proposed the idea of atomic swaps[36]. His approach allowed tokens to be exchanged between different blockchains without the need for an intermediary, such as a centralized exchange.

Broadly speaking, cross-chain integrations can be categorized into two main types: swapping and staking.

Swapping is the most common method of leveraging assets across blockchains. While many swaps are facilitated by centralized exchanges like Coinbase and Binance, several decentralized bridging protocols have been developed and tested over the years, including HTLC[37], XCLAIM[38], tBTC[39], and XCC[40]. However, according to data from crypto aggregator Token Terminal, over 50% of DeFi hacks occur on decentralized bridging protocols[41]. These hacks often exploit the extensive attack surface produced by the inherent complexity of such protocols.

Cross-chain swaps on Bitcoin are even more challenging due to its lack of Turing-completeness. As a result, the majority of wrapped bitcoins rely on centralized authorities, which creates its own set of challenges. An example of the risks introduced by centralized custodians is the recent upheaval surrounding WBTC[42], which highlights the uncertainty these entities can bring to an ecosystem.

Staking is simpler than swapping. It eliminates the need for transferability on the receiving chain since tokens are simply locked up and then returned to their original owners at the end of the commitment. Despite this reduction, the technical requirements for implementing effective slashing mechanisms remain significant. As indicated in Babylon's litepaper[43], it seems cryptographically possible to achieve trustless staking on top of Bitcoin; however, the inherent complexities retain a substantial risk of vulnerable exploitations.

The Strategic Sacrifice of Transferability and Slashing

A secure Bitcoin integration is fundamental to Argon's stability as a currency, and any substantial risk of cross-chain exploits is unacceptable. The invention of DSTL emerged from the realization that two prominent features of decentralized swapping and staking contribute nearly all of their complexity, and yet, they add no value to Argon. In fact, eliminating these features enhances Argon's economic model.

Transferability: For most swapping protocols, the ability to transfer assets within the receiving chain is non-negotiable. Imagine transferring a wrapped bitcoin to Ethereum, only to find that it cannot be used or traded within the Ethereum ecosystem. Such a limitation would render the asset undesirable. WBTC, with its $10 billion market capitalization[44], owes its value to its transferability within Ethereum and other ecosystems. Argon operates differently. The inability to exchange wrapped bitcoins—or what we call Bitcoin Options—is not a limitation but an immensely valuable feature for Argon. It ensures that bitcoin owners retain their chain of custody back to Bitcoin, which is allows the the creation of hedging derivatives to protect against Bitcoin's downside risks, and enables vaulted bitcoins to act as a wall of shorts in case of downward movement in Argon's price.

Slashing: In the Argon ecosystem, bitcoins are not used for staking, which makes slashing irrelevant. For example, the majority of Babylon's protocol is dedicated to penalizing funds on Bitcoin's chain in a trustless and non-exploitable manner. Argon has no need for such penalties, allowing us to sidestep all the complexities of *accountable assertions*[45], *finality gadgets, Bitcoin convenant emulation*, and *Bitcoin timestamping*[46].

Argon's locking protocol is so simple it can hardly be considered a protocol. It's essentially just a two-part multisig.

Our Absurdly Simple Bitcoin Script

The following miniscript is the complete implementation of DSTL in Bitcoin:

```
or(
    thresh(3,
        pk({owner_pubkey}),
        pk({primary_vault_pubkey}),
        thresh(5,
            pk({secondary_vault_pubkey_1}),
            pk({secondary_vault_pubkey_2}),
            ...
            pk({secondary_vault_pubkey_10})
       )
    ),
    and(
        pk({primary_vault_pubkey}),
        thresh(8,
            pk({backup_vault_pubkey_1}),
            pk({backup_vault_pubkey_2}),
            ...
            pk({backup_vault_pubkey_10})
        ),
        after({vault_period})
    )
)
```

Implementing this script as Taproot will increase privacy and reduce transaction costs. As you can see from the code, only two multisigs are required.

The first multisig (thresh 3) requires the Owner, Primary Vault, and five of ten Secondary Vaults to participate.

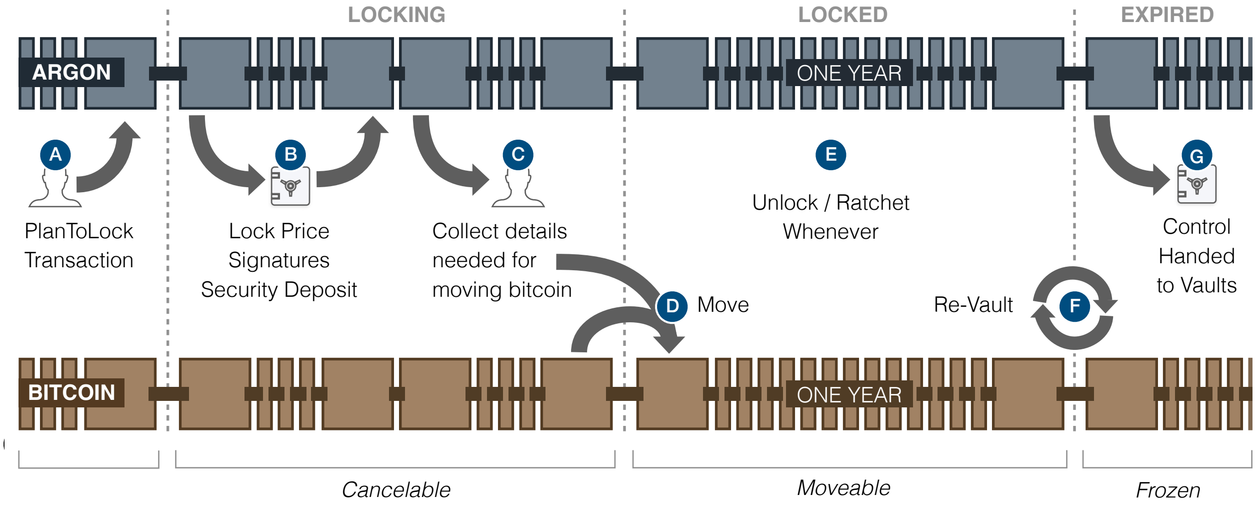
The second multisig is only allowable after the one-year vaulting period has expired. It allow for edge-cases where the Owner has disappeared. Without this second multisig, the Primary Vault would be unable to retrieve their Security Collateral (see D.8, Understanding Vault Security).

DSTL works because participating Vaults (Primary, Secondary, and Backup Vaults) have nothing to gain and everything to lose by failing to fulfill their obligations. The miniscript provides zero capability to steal the bitcoin, and the system exacts penalties far greater than any potential gain if the Vault fails to assist the Owner in a legitimate transfer and/or conspire with the Owner in any type of illegitimate transfer. See Sections D.8 (Understanding Vault Security) and D.9 (Understanding Vault Economics).

A More Detailed Breakdown

The following diagram shows the process of locking from both the Bitcoin and Argon touch points. Additional details are included below.

Figure D.5.1 - The Process of Implementing a Dual Signature Time Lock



The process starts with a bitcoin Owner wanting to vault — the bitcoin can start from a central custodian or self-custodian wallet.

A Owner chooses a Stabilization Vault as their Primary Vault and submits a PlanToLock transaction to the Mainchain, which includes the details listed in D.4, Step Two.

B Primary Vault sees the incoming PlanToLock, identifies Secondary Vaults based on a predetermined XOR algorithm, gathers relevant signatures for the upcoming Bitcoin transaction, and submits a response back to the Mainchain (see D.4, Step Three).

C Owner collects the signature and other details supplied by the Vault (see D.4, Step Five).

D Owner submits their UTXO transaction to Bitcoin, which includes the miniscript listed above as part of its output rules. Once this transaction is accepted by the Bitcoin network, the Owner can no longer spend any output without following Argon's unlock rules (see D.5, The Details of Unlocking a Bitcoin).

E Owner can unlock and/or ratchet (see D.7, Ratcheting a Locked Bitcoin) whenever they wish. There are no time locks or other latency delays enforced by the protocol, and nothing can happen without full sign-off by the Owner. Primary and Secondary Vaults can be counted on to participate in all valid transactions because of their inability to profit from, and the massive penalties levied them, if they fail to do so (see D.8, Understanding Vault Security).

F If Owner wishes to remain vaulted for a second year, they should re-vault before the year end expiration. Re-vaulting is simply the combined act of unlocking and relocking. Failure to either unlock or re-vault before the expiration risks forfeiting their bitcoin to the vaults. See next step.

G Upon the expiration of year's end, Primary Vaults are able to reclaim all collateral still being held against them for bitcoins that previously unlocked or re-vaulted. From this point forward, the vaults are free to use their collateral however they wish. Also, any abandoned bitcoins can now be captured by the Primary Vault through use of the second DSTL signature. However, vaults still have an incentive to work nicely with the Owner since capturing the forfeited bitcoin is a financial wash. The vault loses argon collateral equal to the market value of their captured bitcoin the moment they claim it. The beauty of this balance is that both parties have more to gain by following the rules than not.

DSTL is a major leap forward because it greatly reduces the surface area for an attack. It's almost impossible to create a simpler integration between two heterogeneous blockchains. Most of the complexity has been moved from cryptographical/coding structures to basic economic incentive structures. For more details see D.8 (Understanding Vault Security) D.9 (Understanding Vault Economics), and D.10 (Understanding Bitcoin Economics).

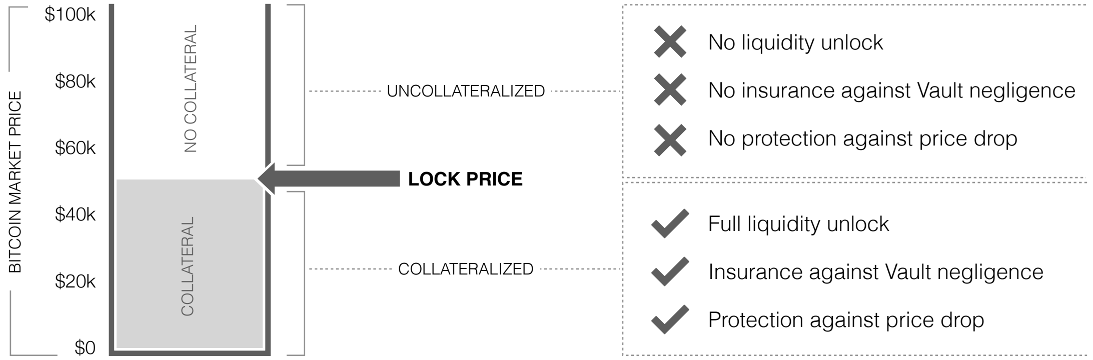
D.7 - Ratcheting a Locked Bitcoin

Ratcheting allows an Owner to increase or decrease their bitcoin's Lock Price as the market changes. It's similar to unlocking and then immediately re-locking. The primary difference is, it doesn't require the Owner to submit another transaction to Bitcoin, and it doesn't require Vaults to do a full re-collateralization of the bitcoin's value.

When Bitcoin's Market Price Rises

The following illustration shows a single bitcoin that was initially vaulted at $50k but now has a Market Price of $100k. It has never been ratcheted so its Lock Price is still set at $50k. This means the Vault only has collateral risk of $50k. Ratcheting up the bitcoin delivers three main benefits: it unlocks another $50k in liquidity to the Owner, it increases bitcoin's insurance against Vault negligence, and it protects against any market drops below $100k.

Figure D.6.1 - An Under-collateralized Bitcoin

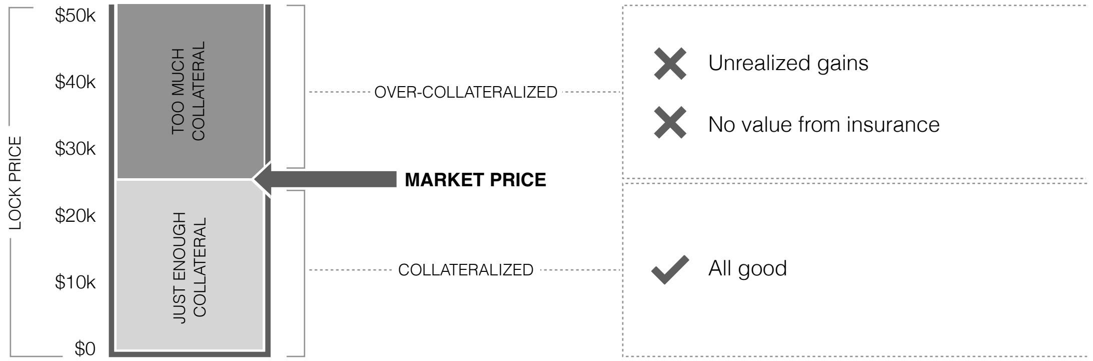


Ratcheting is a beneficial improvement over unlocking and relocating because it avoids paying another transaction fee on the Bitcoin network.

When Bitcoin's Market Price Drops

The following illustration is an inversion of D.6.1. The x-axis is now set at the Lock Price instead of the market price, and it's now over-collateralized instead of under-collateralized. The market price is now half the Lock Price. Ratcheting the Lock Price back up to full market value allows the Owner to capture the entire spread between the Lock Price and the current Market Price as a fully realized gain (see D.10, Understanding Bitcoin Economics).

Figure D.6.2 - An Over-collateralized Bitcoin



Note: ratcheting at a lower price requires inserting the same quantity of argons as unlocking (see the Dynamic Unlocking Formula in D.4). In the example show, this would require 25k argons, which lets the owner keep the remaining 25k of 50k argons that had been minted during the initial lock. Minting rights would then provide another 25k argons, which depending on the Argon's Inflation Index, might sit in the queue for an undetermined amount of time (see Section E.3, A Minting Queue).

In both of the examples — both when ratcheting the price up and when ratcheting down — the amount of time remaining on the one-year lock does not change. If there are three months remaining before the ratchet, there will be three months remaining after the ratchet.

What Happens When a Vault Has No Collateral Capacity

Ratcheting up requires the Primary Vault to have argons available for use as additional collateral. This is never guaranteed. In a situation where the Vault does not have capacity for handling an up-ratchet, the Owner has two options: wait to ratchet until there is capacity or move to another Vault.

One improvement of the protocol might be to penalize Primary Vaults that lack spare collateral. For example, they could be forced to hand over the Security Fee they collected during initial lock in order to help smooth the new Vault transition. Regardless, it is improbable for Security Fees to be in affect for at least the first five to ten years (see D.9, Understanding Vault Economics), which makes the issue of spare collateral of little consequence.

D.8 - Understanding Vault Security

Stabilization Vaults are the ultimate gatekeepers of bitcoin within the Argon network. Through their use of DSTL multisigs, Vaults hold the final authority over unlocking requests, making it imperative that their incentives are correctly aligned to ensure the integrity and security of the network.

One of the challenges is that Argon is fully open and decentralized. It has no identification processes, certifications, or selection mechanisms to limit who can join. Anyone can create and connect a Vault, and there could be hundreds or even thousands of them. Since there are no centralized authorities to distinguish between good and bad actors or to control who is allowed to join, the protocol must be designed to assume that all Vaults are untrustworthy and to ensure that even untrustworthy Vaults are rendered harmless.

Two Types of Malfeasance

While Vaults have no power to unilaterally steal bitcoins, they do possess the capability to break the rules in two other ways:

Collude with Bitcoin Owners: Vaults can collude with bitcoin owners to unlock bitcoins without the proper burning of argons. If allowed, this undermines the integrity of the broader network.

Ignore Legitimate Requests: Vaults can ignore legitimate transfer requests from bitcoin owners. If allowed, this harms both the targeted bitcoin owners and the broader network.

Argon's solution to prohibit this malfeasance is collateral. Unlike the collateral used in "collateral-backed" stablecoins, this collateral is real — assets will be forfeited if there are any breaking of rules. The genius of collateral is that, when applied correctly, any ill-gotten gains can be neutralized, and in doing so, the financial incentive to break rules can be eliminated.

Pledging Security Collateral

Vaults must pledge argons equal to a minimum of 110% of the market value of the bitcoins in their custody. The amount is determined at the moment of locking, and it's held for a minimum of one year. The collateral is used both to insure its own actions and that of other Vaults in the network. If Vaults engage in any misconduct, their argons are immediately forfeited.

Vault Collateral Formula

$$\text{Collateral} = 1.10L_b$$

In this formula:

$Collateral$:= The number of argons that Vault must pledge

L_b := The argon market price of Bitcoin at the moment of locking

The following rules are enforced:

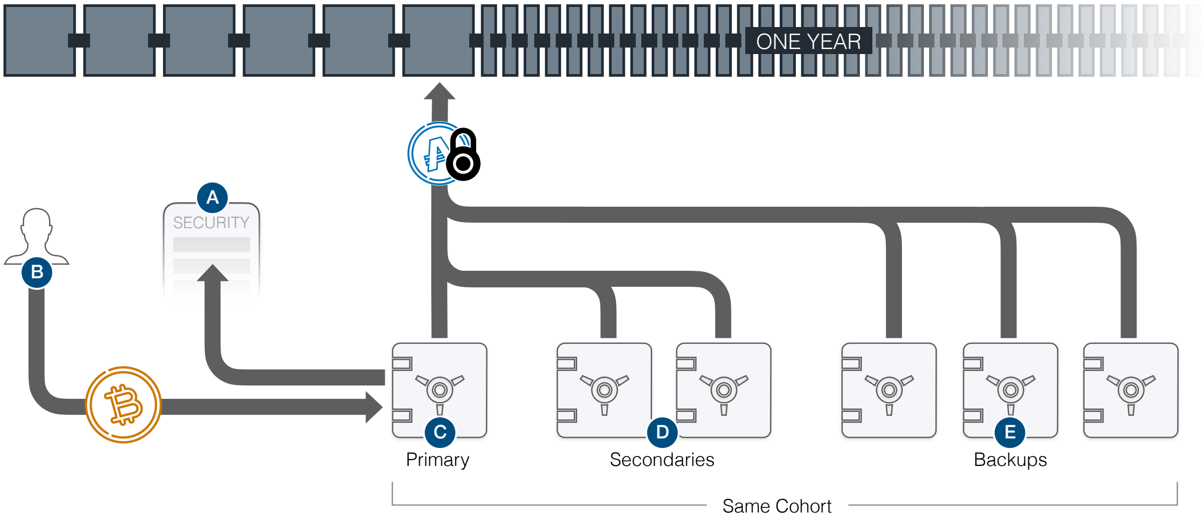
Vault forfeits an amount equal to the Lock Price of the bitcoin if they fail to respond to legit unlocking requests.

Vaults forfeits an amount equal to the Lock Price if the bitcoin moves without a valid unlocking request. This is true both during the vaulting year and for all time thereafter.

Vault forfeits 10% of their collateral if they do not respond to legitimate Secondary and Backup signature requests.

The amount required to be held as collateral remains steady throughout the length of the vaulting period regardless of fluctuations in Bitcoin's market price. The only exception is when a Ratcheting Transaction is submitted. In that case, the collateral will relock at the new market price and remain so until another Ratcheting Transaction occurs.

Figure D.8.1 - Pledging Security for a Bitcoin



(A) All Vaults must publicly communicate how much bitcoin space is open (i.e., how many argons are available for collateralizing) as well as the Security Fee being charged.

(B) Owner submits a bitcoin to the Vault of their choosing (hereafter referred to as Primary Vault), which triggers a process on the Mainchain that locks the required security collateral and selects Secondary and Backup Vaults.

(C) The Primary Vault is a signer on both multisigs and therefore has primary responsibility for ensuring the bitcoin remains locked unless a legitimate unlocking transaction is submitted. If the bitcoin moves outside the process then 100% of the Lock Price will be forfeit by the Primary Vault.

(D) Secondary Vaults are selected using XOR from a listing of vaults within the same commitment timeframe (cohort) as the Primary Vault. This ensures all vaults in a multisig can be counted on to remain active during the full year. Half of the Secondary Vaults are required to co-sign along with the Primary Vault to ensure Owners are correctly following the rules.

(E) The Secondary Vaults also serve as Backup Vaults. Backup Vaults are only activated in the case where a bitcoin is abandoned within a vault. In order to claim the bitcoin, the Primary Vault is required to get 80% of the Backup Vaults to co-sign their transaction. This ensures no foul play by the Primary Vault.

Because of the quantity of argons locked as Security Collateral in each vault, vaults are incentivized to follow the rules both to avoid penalties and also to maintain the value of their own argons being held as collateral.

Additionally, vaults are heavily incentivized in the economic success of the broader network through their partnership with = miners (see D.9, Understanding Vault Economics).

Six Possible Scenarios

DSTL multisigs has two sides (Owner + Vaults), which means there are only six possible combinations of collusion, cooperation, and/or subversion.

1. Owner and Vault Legitimately Work Together

In this first scenario both parties follow the protocol rules for locking and unlocking and both parties earn their respective rewards. See D.9 (Understanding Vault Economics) and D.10 (Understanding Bitcoin Economics).

2. Owner and Vault Illegitimately Collude Together

Owners and Vaults can conspire to unlock bitcoins without burning the required Argons since they collectively control the full multisig needed for Bitcoin network transactions. This collusion might occur due to an existing relationship or because the Owner and Vault are the same entity. Since anyone can create a vault, and the Owners choose which vaults to use, the potential for collusion is always present. Although it is not possible to algorithmically guarantee against this, it is possible to economically ensure that no perpetrator can gain by cheating and also that no innocent party can lose.

For example, a bitcoin owner might lock their bitcoin in a colluding vault, mint argons equal to the bitcoin's market value, sell those argons, and then attempt to move the bitcoin fraudulently. By bypassing Argon's Mainchain, they avoided burning the required argons. Or did they? By burning the Vault's Security Collateral, any possible gains from the collusion are more than offset by a greater loss.

If the bitcoin's Lock Price was 50k, the parties might avoid the 50k locking fee, but they will lose a minimum of 105%, or 52.5k. This includes the Primary Vault's 50k and an additional 2.5k to 5k from Secondary or Backup Vaults, depending on whose signatures were on the output. Mainchain miners track all UTXO hashes of bitcoins locked in Vaults. The moment a bitcoin moves without a corresponding locking transaction, the colluding Vaults have their Security Collateral forfeited.

3. Vault Try to Steal the Bitcoin

One or more Vaults might attempt to sign the multisig without the Owner's knowledge in order to move it to a Bitcoin address they control. This is impossible as both DSTL multisigs require the Owner's signature for any transaction to be valid. If a Vault attempts to unlock a bitcoin for itself, the transaction will fail on the Bitcoin network, and when caught by Argon miners, the participating Vaults will forfeit all their related collateral thereby ensuring zero gain and full loss.

4. Vault Ignore Owner's Legitimate Requests

Vaults cannot be physically forced to sign legitimate unlocking requests, and there are an infinite number of reasons these requests could be ignored. It might simply be that the Vault operator has died.

Regardless of the reason, so long as the Owner's unlocking request was cryptographically valid, all vaults that do not sign the first request (whether Primary or Secondary) ultimately lose their Security Collateral. The collateral is used to make the Owner whole. The Backup Vaults are then designated to block any unlocking request by the Primary Vault after one year. So long as the owner has been Ratcheting up after major value increases, any potential loss will be fully covered. The Primary Vault loses 100% of their collateral.

5. Owner Tries to Steal the Bitcoin

Owner might try to move the bitcoin to another address without first submitting a valid unlocking request to the Mainchain. However, unless the Owner has colluded with the Vaults (see #2 above), the Owner will be unable to succeed. Vaults enforce the rules through their half of the DSTL multisig, which ensures that users cannot retrieve their assets without first fulfilling their obligations.

6. Owner Ignores Vault's Legitimate Responses

After submitting a valid unlocking request to the Mainchain, Owner might ignore the Vault's signing response. They are free to do so, however, the only loser is the Owner. Everyone in the Argon network will be able to validate the Vault's signing response and therefore the Vault is at no risk of losing their Security Collateral.

Because of DSTL's dual signature design, any user who decides to ignore their vaulted bitcoin (i.e., refuses to unlock and/or relock at the end of the year) is only harming themselves. Argons equal to the value of the vaulted bitcoin is still burned from circulation by the Primary Vault (with assistance from Backup Vaults), and the bitcoin is then free to be relocked in the vaults. The system continues as usual.

In summary, Argon ensures that any participant who disregards the rules, whether intentionally or unintentionally, will lose more than they gain.

D.9 - Understanding Vault Economics

To grasp the economics of Vaults, it's essential to first understand their costs. The operational demands of Vaults are basically to serve as simple multisig cosigners. Their responsibility is to store private keys in a hardware wallet and sign a handful of transactions each year. Vaults have up to 10 days to respond to signing requests, so the demands are not strenuous.

The primary cost for Vaults is the argons they must hold as collateral for bitcoins in their custody. This can be calculated as the time/value cost of money.

Vaults have two primary revenue sources:

Yield from Security Collateral

Vaults generate revenue by charging bitcoin owners a Security Fee, which reflects both the market value of the bitcoin and the duration (one year) for which the collateral is locked. For example, a 3% fee would be considered highly favorable for bitcoin owners since, as discussed in Section D.9, the volatility of bitcoin and therefore the potential upside of hedging far exceeds 3%.

It's important to note that from a dollar-denominated perspective, the Vault's yield is even higher than 3%. Since Argon is an inflation-resistant currency, the Vault's dollar-denominated return comprises its yield plus the dollar's inflation rate over the given year.

Yield from Bonded Argons

The major profit opportunity for Vaults, particularly in the first five to ten years, is in the loan services they offer to mining operations. Bonded Argons are a special type of by-product produced by Vaults, and these Bonded Argons are crucial to mining operations. Only Vaults have the authority to create them, and the mining and minting of argons are not possible without these Bonded Argons.

Vaults lend these Bonded Argons to miners, allowing Vaults to earn a share of the mining rewards. The amount of Bonded Argons that a Vault can generate is capped only by the market value of the bitcoins it holds. While the full details will be covered in our next whitepaper, suffice it to say that, given the mechanics of Bonded Argons and their role in mining operations, it is virtually guaranteed that a Vault will generate a minimum of 30% annual yield for at least the first five years.

In summary, the profit from Bonded Argons will likely generate far more revenue than what is possible from Security Fees. Vaults may even be incentivized to offer negative rates (paying bitcoin owners to join) in order to generate more Bonded Argons

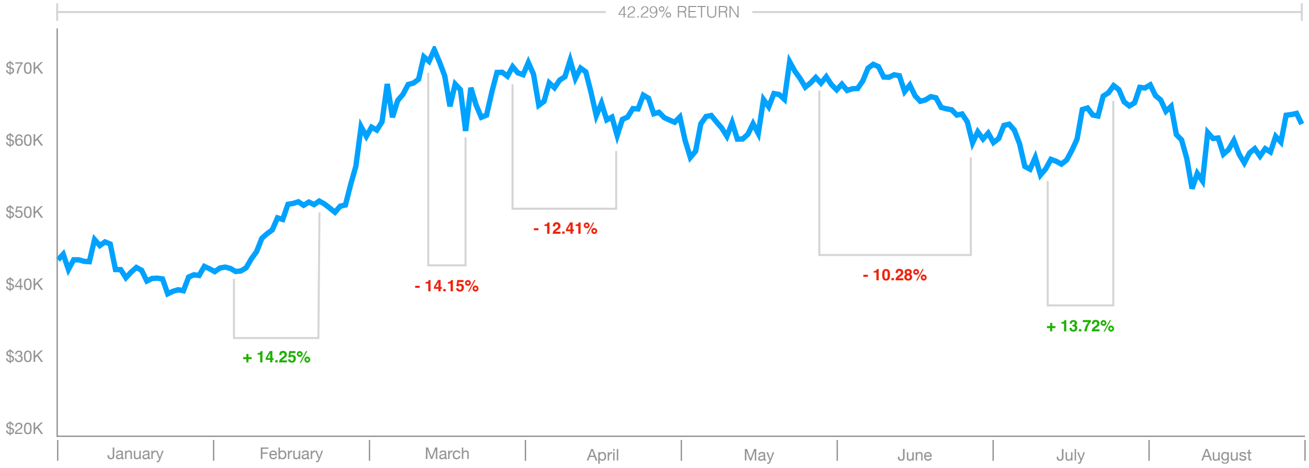
D.10 - Understanding Bitcoin Economics

This section addresses the uncertainty regarding whether there will be enough vaulted Bitcoins within the Argon ecosystem to have a material effect on Argon's stabilization mechanisms. The fundamental question is what benefits would encourage bitcoins to be vaulted.

The primary benefit is the ability to unlock the liquid market value of a bitcoin. Additionally, vaulting bitcoins allows for a full hedge against downside pricing risk. Beyond this, there is a much larger opportunity: as Bitcoin's market price fluctuates, the Lock Price can be ratcheted up and down to align with these price movements. This ratcheting mechanism creates powerful new trading tools for Bitcoin owners.

To illustrate this, historical modeling in the chart below shows that a Bitcoin HODLer would have realized a 42.29% gain as its price increased from $44,176 to $62,858 between January 1 and August 26 of this year[47].

Figure 12 - Bitcoin Price from January 1, 2024 to August 26, 2024



Vaulting bitcoin between January 1, 2024, and August 26, 2024, however, would not have improved the returns, which would have remained at 42.29%. While the vault would have protected against potential losses, there were no losses to mitigate, so it did not impact the result.

How would ratcheting have changed this? It would have allowed what are essentially zero-cost Bitcoin hedges to protect the price drops and cleanup the upswings. For example, by implementing a simple strategy of blindly ratcheting every time Bitcoin's price changes 10% either direction, the results would have been significantly better.

In 2024, this simple strategy would have required ratcheting fourteen times. To ensure a conservative model, let's consider the worst-case scenario where each ratcheting required moving to a new vault with enough capacity, which would have incurred additional Bitcoin transaction fees for updating the miniscript. Even with these worst-case costs factored in, the returns would have surged from 42.29% to 146.12%.

The following table shows the details of each ratchet. It uses the average Bitcoin transaction price for each date.

Date	Previous	Current	BTC Fees	Liquidity	Vaulting Profit	Hodler Profit
Jan 1, 2024		$44,176	$14.77	$44,161	-0.03%	0.00%
Jan 22, 2024	$44,176	$39,505	---	$44,161	-0.03%	-10.57%
Feb 7, 2024	$39,505	$44,319	$7.57	$48,968	10.85%	0.32%
Feb 12, 2024	$44,319	$49,958	$8.19	$54,599	23.59%	13.09%
Feb 27, 2024	$49,958	$57,075	$7.09	$61,709	39.69%	29.20%
Mar 3, 2024	$57,075	$63,168	$7.56	$67,794	53.46%	42.99%
Mar 11, 2024	$63,168	$72,121	$7.51	$76,740	73.71%	63.26%
Mar 19, 2024	$72,121	$61,919	---	$76,740	73.71%	40.16%
Mar 25, 2024	$61,919	$69,963	$6.14	$84,777	91.91%	58.37%
Apr 17, 2024	$69,963	$61,281	---	$84,777	91.91%	38.72%
May 20, 2024	$61,281	$71,443	$2.01	$94,937	114.91%	61.72%
Jun 21, 2024	$71,443	$64,096	---	$94,937	114.91%	45.09%

Jul 4, 2024	$64,096	$57,034	---	$94,937	114.91%	29.11%
Jul 15, 2024	$57,034	$64,860	$1.55	$102,761	132.62%	46.82%
Aug 4, 2024	$64,860	$58,116	---	$102,761	132.62%	31.56%
Aug 23, 2024	$58,116	$64,082	$0.79	$108,726	146.12%	45.06%
FINAL		**$62,858**		**$108,726**	**146.12%**	**42.29%**

It wasn't only the first eight months of 2024 that would have benefited from ratcheting. The following goes back twelve years to 2013. It uses the same strategy as the previous table, which is to ratchet every time bitcoin deviates 10% or more. There is no year where vaulting would have lost money.

Year	Starting	Ending	BTC Fees	Liquidity	Vaulting Profit	Hodler Profit
2024	$44,176	$62,858	$63.18	$108,726	146.12%	42.29%
2023	$16,614	$42,250	$45.80	$51,239	210.00%	154.31%
2022	$47,763	$16,527	$16.88	$77,891	63.08%	-65.40%
2021	$29,394	$46,250	$329.82	$151,305	414.75%	57.34%
2020	$7,176	$28,983	$84.52	$36,879	449.34%	303.90%
2019	$3,856	$7,168	$26.63	$17,236	347.01%	85.91%
2018	$13,375	$3,738	$137.87	$29,955	124.70%	-72.05%
2017	$997	$13,796	$250.72	$28,885	2,914.85%	1,283.25%
2016	$435	$965	$2.96	$1,331	217.77%	121.93%
2015	$315	$431	$0.90	$895	188.75%	36.87%
2014	$749	$321	$2.00	$1,756	134.42%	-57.16%
2013	$14	$732	$8.49	$2,229	16,389.23%	5,314.20%

To answer the opening question of this section, the incentive for bitcoins to participate in Argon's Stabilization Vaults is quite high, especially considering the additional profit opportunities that arise when Argon falls below its market price. (see table in Section D.5 – The Details of Unlocking a Bitcoin).

Note: The above returns are not compounded, meaning the profits earned from ratcheting are taken off the table instead of being reinvested into more bitcoins. Compounding would have an even more profound effect.

Additional Note: One cost that isn't included in these ratcheting models is Security Fees. This is because we believe it is improbable for Vaults to charge Security Fees for at least the first five to ten years. However, even if they do, it is unlikely those fees will have a material difference on the outcome.

The full historical data and coding logic used to generate these models have been published to our github.com/argonprotocol/whitepaper-models repository[48].

D.11 - Let's Talk About the Losers

One way to think of Argon is as a currency backed not by military power but by the power of balanced profit tensions. The tensions result from countervailing economic incentives designed into both sides of Argon's price.

When you understand that these incentives always create a simple value transfer — for instance, from Bitcoin to Argon and vice versa — it becomes clear that the only loser in Argon's stabilization process is the person who sells their Argon below market value due to fear or panic. In that case, the value transfer is a zero-sum scenario where Argon buyers inevitably gain the value forgone by the sellers. This dynamic serves as a deterrent to panic-selling, but if panic-selling ever does happen, Argon's bitcoin mechanisms will happily absorb the excess tokens. To use a dollar analogy: at some point, the "idiots" will stop selling a single $100 bill for two $20 bills.

D.12 - But They're Not Shorts

Throughout this paper, any reference to a "wall of shorts" should be interpreted as a representation of the profit potential for vaulted bitcoins when Argon trades below its target price (see the table in D.5, The Details of Unlocking a Bitcoin). These vaulted bitcoins are not actually short any instrument via traditional exchange-traded derivatives. As such, they do not carry unlimited loss potential from short squeezes, nor do they have any margin requirements or the need for market timing acumen.

D.13 - Acknowledging the Black Swan

Anomalous pricing action can lead to a slow erosion of Bitcoin's wall of shorts against the Argon. For example, if Bitcoin's price drops farther on a percentage basis than Argon's (e.g., BTC -60% vs. ARG -40%), then the following is technically possible:

1. Unlocking of Vaulted Bitcoins

All vaulted Bitcoins could unlock to take advantage of the short. This would burn a sufficient number of argons to re-stabilize at the target price, but in doing so, the vaults would be left completely empty.

2. Market Awareness

Before any new bitcoins can vault, the market notices that the vaults are empty, meaning the wall of shorts has disappeared. This could prompt a subsequent unmanageable sell-off of argons.

3. Pricing Plummet

Argon's price could then plummet into a death spiral, and with no bitcoins in the vaults, it might remain at a depressed level indefinitely.

For the scenario above to play out, 100% of the vaulted bitcoins would need to be unlocked in the same upswing with no new ones taking their place. However, if only a few bitcoins remain in the Stabilization Vaults, then those remaining bitcoins can fully consume and burn the excess argons once the price falls low enough. Presumably, a few profit-maximizing Bitcoin owners would seize this opportunity to stay in and clean up the entire gain from a re-stabilizing upswing, though in fairness, this would require some level of speculation.

While the situation described above seems improbable, it cannot be ignored. There are several ways to leverage the Minting Queue described in E.3 (Empowering Bitcoins with FIFO Queue) to encourage bitcoins to re-enter Vaults in the aftermath of such an event, even while the argon is still in a depressed death-spiral state. However, this introduces some probabilistic unknowns, especially within the context of a fully decentralized, free-market approach. The ultimate solution is to layer in a second stabilization mechanism that is unaffected by pricing anomalies. See Section F (Constant Deflationary Pressure) and Section G (Layering the Mechanisms).

E. SEIGNIORAGE PRIVILEGES (MINTING MECHANISM)

Argon's Minting Mechanism ensures the stablecoin never becomes a speculative asset. Whenever Argon rises above its target price, minting triggers the creation of new argons. Half these new argons are given to Ownership tokens; the other half to Bitcoin tokens. Selling those argons into the market helps rebalance supply and demand.

E.1 - The Formula for Minting

The Argon protocol has a built-in mechanism to prevent over-minting. New argons are only minted when the internal Inflation Index indicates demand has exceeded supply, which would have caused the trading price to rise above the target. The Minting Rights Formula shown below ensures that the supply of argons will only increase by the amount necessary to rebalance back to the target price.

Minting Rights Formula

$$\text{ArgonsToMint}(x, I) = \begin{cases} 0 & \text{if } I \geq 100 \\ \left| x \cdot \frac{(I - 100)}{100} \right| & \text{if } I < 100 \end{cases}$$

This formula uses:

I := Argon Inflation Index (base of 100, since launch of Argon)

x := The total supply of argons in circulation

The Argon Inflation Index is described in full detail in our third whitepaper, *Bootstrapping a Global Currency*, but for the sake of this paper, the Inflation Index uses a base of 100 starting at the launch of Argon.

E.2 - Limit Bitcoins to 50% Minting

Minting rules dictate that no more than 50% of argons in circulation can be minted by bitcoins. Argon Ownership tokens are given rights to mint the rest. This ensures sufficient profit incentives are retained to promote robust mining operations and foster continual network growth. For more details, see our third whitepaper, *Bootstrapping a Global Currency*.

E.3 - The Minting Queue

Bitcoin minting of new Argons occurs through a different process than that of Ownership Tokens and requires a special Minting Queue to ensure system fluidity. First, let us briefly explain the process for Ownership Tokens. When the price of Argon rises above its target price, new argons are awarded to Ownership Tokens. They are distributed pro-rata, and similar to dividends from public equities, Ownership Tokens continue to collect rewards as Argon circulation grows—these are recurring payments. Bitcoins, on the other hand, only earn minting rights when they perform specific actions, such as locking into Stabilization Vaults or ratcheting their Lock Price.

Recall that new argons cannot be minted unless Argon's market price is above the target. However, to facilitate bitcoins moving in and out of Stabilization Vaults whenever they wish (even when argon aren't being minted), a special Minting Queue exists. A bitcoin that earns minting rights is placed into this queue. The queue operates on a First In, First Out (FIFO) order, and this queue is prioritized over Ownership Tokens.

Whenever the Minting Rights Formula determines that new argons should be minted, the Minting Queue is checked. If it contains Bitcoin minting rights that have yet to be awarded, and if bitcoins have minted less than 50% of the current circulation (see E.2), then the First In (oldest) minting rights are popped off the Minting Queue and awarded. Legacy minting rights continue to be popped and awarded until a) no more Argons need minting, b) the queue has been emptied, or c) bitcoins have achieved their max minting of 50% circulation. Only after the Minting Queue is empty, or if bitcoins have reached their minting limit, are Ownership Tokens then awarded new argons.

E.4 - Wealth Transfer Through Seigniorage

Argon's Minting Mechanism is basically a seigniorage model. All capital entering the market to acquire argons accrues directly to vaulted Bitcoins and Ownership Tokens. Unlike "collateral-backed" stablecoins, incoming capital isn't required to be held in centralized custodians or treasury bonds. Instead, this capital is taken off the table as unencumbered profits. For more details, see our third whitepaper, *Bootstrapping a Global Currency*.

F. CONSTANT DEFLATIONARY PRESSURE (TAXATION MECHANISM)

The stability of any currency is contingent upon its ability to maintain a balanced supply in the market. To achieve this, Argon incorporates a unique taxation mechanism that exerts constant deflationary pressure, effectively creating an upward force on the stablecoin's price. This mechanism operates by levying a tax on all peer-to-peer transactions and then burning the collected taxes. This process continuously reduces the number of Argons in circulation, thereby increasing the scarcity and value of the remaining tokens.

F.1 - A Simple Tax Code

The following formula encapsulates Argon's complete tax code. Each transaction is charged a flat tax of ₳0.20 unless it qualifies as a micropayment, in which case the tax rate is 20% of the transaction total. Micropayments are covered in great detail in *Bootstrapping a Global Currency*, but for the sake of the following formula, micropayments are defined as transactions under ₳1.00.

Argon Taxation Formula

$$\text{Tax}(p, m) = \begin{cases} 0.2p & \text{if } m = 1 \\ 0.2 & \text{if } m = 0 \end{cases}$$

In this formula:

p *:= Price of Transaction Total (any payment settled between two parties)*

i := Is a Micropayment

F.2 - Taxes Must Burn

In traditional governments, taxes are reintegrated back into the economy through spending on societal programs, infrastructure, and bureaucratic functions[49]. However, in a decentralized network like Argon, this absence of a central authority allows for taxes to be completely burned, which removes them from circulation.

The benefits of burning are twofold:

During Inflation: It acts as a corrective force, driving the stablecoin's price back towards its target.

During Stability: It creates demand for new Argons to be minted (see Section E), thereby serving as a profit engine for Ownership Tokens.

While burn mechanisms are not new in the cryptocurrency world[50], Argon is pioneering their application in the stablecoin space. Stablecoins that have described themselves as burning, such as Basis and Terra, were more accurately just exchanging one token for another. They never burned in the sense of burning value. Argon burns.

F.3 - Ensuring Effective Burn

Although the perpetual burning of stablecoins ensures that the currency, at least in concept, can never enter a permanent death spiral—since, at some point, excess circulation will be burned—the practicality of such a system raises two critical questions.

1. Can the Economic Activity Survive Price Instability?

Argon's Taxation Mechanism relies on constant transaction flow, and during a price decline, currency usage must continue even when it is "underwater." Without ongoing usage, there will be no transactional volume from which to collect taxes. While the goal is for Argon to become a ubiquitous global currency, it is critical for the models to assume that most use cases will disappear if there are protracted periods of instability.

The ideal solution is to integrate Argon into a high-velocity, captive market that requires the use of the stablecoin regardless of its stability or broader appeal. This is where the Ulixee Data Network and its Datastores come into play. Ulixee is an open-source decentralized data platform built by the same team who built Argon. Datastores turn every website into an Argon-earning data API. They effectively create an internet-native business model that transforms web data into a marketplace of data blocks that developers can use to build new apps, websites, and AI engines. Argon is the native currency of these Datastores. It leverages Argon micropayments to facilitate a network that requires no user accounts or subscriptions. Data is charged on a per-query basis. In return for generating a steady transaction flow that leads to crucial tax burns, Ulixee Datastores earn up to 25% of the mining/minting rewards of the Argon network. For more details, see our third whitepaper, *Bootstrapping a Global Currency*.

2. Will the Economic Activity Carry Enough Burn Weight?

This is the core fundamental question. If Argon were to enter a death spiral, how long will it take for taxation to burn enough excess tokens to re-stabilize the currency back to its target price?

To set some context, imagine Argon circulation grows to one trillion and then loses 99.99999% of its value. Even if Argon processed Visa's global transaction volume of 212.6 billion transactions annually[51] and maintains this volume post-death-spiral, it will only burn ₳42.52 billion per year if taxed at a rate of ₳0.20 per transaction. At this pace, it will take 23.5 years for the Argon to burn through the one trillion stablecoin tokens and re-stabilize back to target. This obviously doesn't work.

The solution is our Wage Protector mechanism, a lever that amplifies the burn rate during inflationary periods. This mechanism allows taxation to absorb and burn a significantly greater quantity of excess Argons than the transactional volume alone would suggest. For example, in the previous scenario of Argon having one trillion stablecoins in circulation and losing 99.99999% of its value, Wage Protector will dramatically reduce the time to re-stabilize. For example, if the Ulixee Data Network has global gross revenue of only $50M annually — and even if everyone else deserts Argon, including bitcoins abandoning Stabilization Vaults — Argon is guaranteed to bounce back to stable in less than 30 days. Moreover, it will do so with zero negative effect on the commercial buyers or sellers participating in the Ulixee Data Network.

F.4 - Protecting the Wage

WageProtector is an extremely simple yet seemingly magical algorithm that gives the Taxation Mechanism its superpower. It keeps Argon fully decoupled from the dollar while ensuring that merchants who care about dollar-dominated value will always receive the dollar value they expect. The protocol achieves this by monitoring Argon's internal Inflation Index and adjusting prices accordingly. As a result, regardless of the stablecoin's price fluctuations, merchants consistently receive a stable dollar value for their goods and services.

Below is the WageProtector formula.

Formula D - WageProtector's Adjusted Price

$$\text{AdjustedPrice}(p, I) = \begin{cases} p & \text{if } I \leq 100 \\ p \cdot \left(1 + \frac{(I - 100)}{100}\right) & \text{if } I > 100 \end{cases}$$

In this formula:

I := Argon Inflation Index (base of 100, since launch of Argon)

p := Price of Transaction Total (any payment settled between two parties)

In traditional economies, price increases often lag inflationary policies by months or even years[52]. WageProtector triggers this increase almost instantaneously.

We expect WageProtector to be implemented as a simple coding function that developers can use in their apps and websites to wrap their transactional pricing. The following demonstrates a javascript implementation.

Code - Javascript Usage of WageProtector

```
import { WageProtectorForUSD } from '@argonprotocol/wage-protector';

const price = WageProtectorForUSD(10.00);
```

As internal inflation rises within the Argon due to circulation imbalance, the Wage Protector applies a multiplier to the amount of stablecoins burned. This is because taxes are calculated after the adjustment.

The following table shows the tax burn from a ₳1.00 purchase of at different stages of inflation. The Ulixee Data Network operates in micropayments so this creates a realistic tax percentage model.

Note: The table assumes a consistent dollar-to-argon exchange rate of $1.00 to ₳1.00. This will obviously change as time progresses and inflation of the dollar continues, but displaying even numbers is easier on the eyes, and regardless, the dollar-to-argon exchange rate has no effect on burn percentages.

Inflation Index	Tax Rate	$-to-₳	Purchase Cost (₳)	Purchase Cost ($)	Take Home ($)	Burn
100	20%	$1.00	₳1.00	$1.00	$0.80	20%
101	20%	$0.99	₳1.01	$1.00	$0.80	20%
102	20%	$0.98	₳1.02	$1.00	$0.80	20%
103	20%	$0.97	₳1.03	$1.00	$0.80	21%
104	20%	$0.96	₳1.04	$1.00	$0.80	21%
105	20%	$0.95	₳1.05	$1.00	$0.80	21%
106	20%	$0.94	₳1.06	$1.00	$0.80	21%
108	20%	$0.93	₳1.08	$1.00	$0.80	22%
109	20%	$0.92	₳1.09	$1.00	$0.80	22%
110	20%	$0.91	₳1.10	$1.00	$0.80	22%
111	20%	$0.90	₳1.11	$1.00	$0.80	22%
125	20%	$0.80	₳1.25	$1.00	$0.80	25%
143	20%	$0.70	₳1.43	$1.00	$0.80	29%
167	20%	$0.60	₳1.67	$1.00	$0.80	33%
200	20%	$0.50	₳2.00	$1.00	$0.80	40%
250	20%	$0.40	₳2.50	$1.00	$0.80	50%
333	20%	$0.30	₳3.33	$1.00	$0.80	67%
500	20%	$0.20	₳5.00	$1.00	$0.80	100%
1,000	20%	$0.10	₳10.00	$1.00	$0.80	200%
1,111	20%	$0.09	₳11.11	$1.00	$0.80	222%
1,250	20%	$0.08	₳12.50	$1.00	$0.80	250%
1,429	20%	$0.07	₳14.29	$1.00	$0.80	286%
1,667	20%	$0.06	₳16.67	$1.00	$0.80	333%
2,000	20%	$0.05	₳20.00	$1.00	$0.80	400%
2,500	20%	$0.04	₳25.00	$1.00	$0.80	500%
3,333	20%	$0.03	₳33.33	$1.00	$0.80	667%
5,000	20%	$0.02	₳50.00	$1.00	$0.80	1,000%
10,000	20%	$0.01	₳100.00	$1.00	$0.80	2,000%
...	...	...	...	...	...	...
100,000	20%	$0.001	₳1,000.00	$1.00	$0.80	20,000%
...	...	...	...	...	...	...

1,000,000	20%	$0.0001	₳10,000.00	$1.00	$0.80	200,000%
...	...	...	...	...	...	...
10,000,000	20%	$0.00001	₳100,000.00	$1.00	$0.80	2,000,000%
...	...	...	...	...	...	...
100,000,000	20%	$0.000001	₳1,000,000.00	$1.00	$0.80	20,000,000%

As the table shows, when the dollar-to-argon price falls to $0.01, the number of stablecoins transacted jumps by many orders of magnitude. However, the dollars paid by the customer remain steady, and the Take Home value for merchants is preserved. What really matters, at least for the re-stabilization of the currency, is the number of stablecoins burned as taxes, which skyrockets to 20,000,000% (20 million percent) above its normal rate.

To illustrate the power of this mechanism, let's briefly revisit the example in F.3 where Argon, as a one trillion stablecoin, loses 99.99999% of its value. When combined with an exogenous market like the Ulixee Data Network, Argon's Wage Protector significantly enhances its re-stabilization potential. Whether the Ulixee Data Network generates $10 million or $100 million in gross revenues, the key advantage lies in creating utility value for Argon within another market, independent of the stablecoin's stability. This integration allows Argon to maintain its functionality and provides a mechanism for recovering its value, even during periods of significant instability.

F.5 - Acknowledging Another Black Swan

The fundamental weakness of using taxation to stabilize Argon is that it's not rapidly responsive, especially during the early stages of a price drop. Until it falls far enough to trigger Wage Protector's outsized burns, Argon can seem stuck in an eternal neverland. Although it's burning, it's burning slowly.

This issue is especially relevant for an inflation-resistant stablecoin like the Argon. If the circulation grows faster than the taxation can keep up, the stablecoin can fall farther and farther behind in reaching its inflation-adjusted price target, until it finally falls far enough behind to take advantage of WageProtector. This dulls the promise of Argon as a wealth preserving currency.

The solution is to layer Taxation with a complimentary stabilization mechanism like Bitcoin Fusion.

G. LAYERING THE MECHANISMS

Death spirals have marked the downfall of many stablecoins. Their algorithms function well during periods of capital inflow — simply print more money to neutralize increased demand — but when prices dip, fear sets in. Some begin to liquidate, causing prices to fall further, which in turn generates more fear and uncertainty, eventually triggering a destructive spiral.

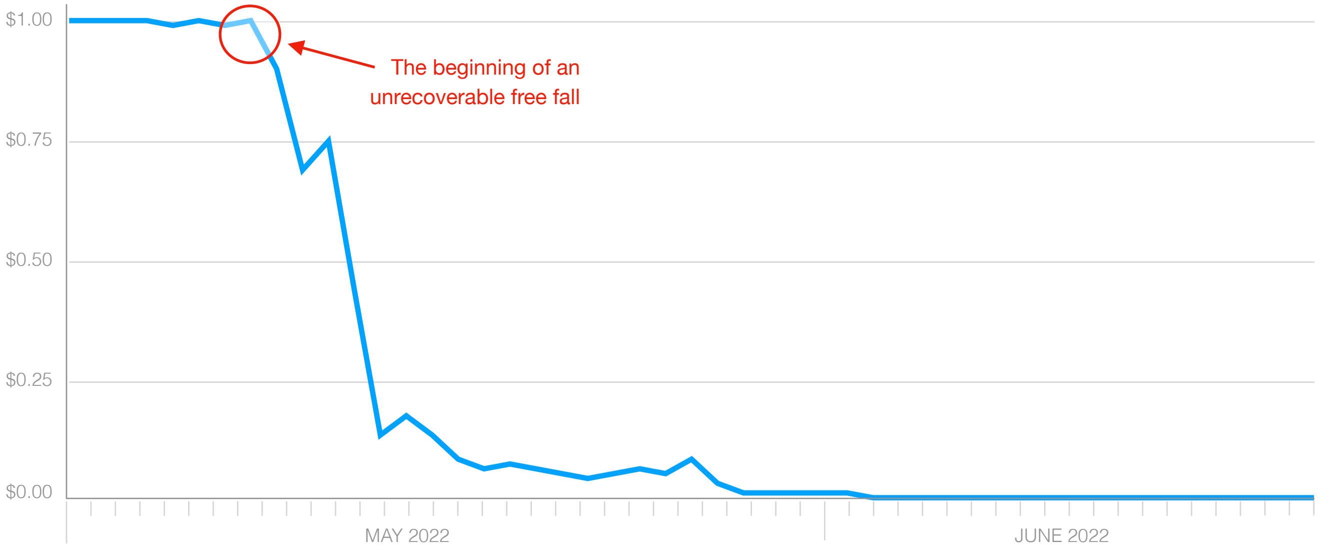
In this section, we explore how Argon is immune to death spirals and how the faster it falls, the faster it rebounds. Even a 99.99999% drop in Argon's value can't prevent the currency from bouncing back to its target price within days. It can do so even if all faith in the currency is lost and no external capital comes to its rescue.

G.1 - A Nightmare Scenario

One of the largest stablecoin collapses was Terra in late spring 2022. The chart below illustrates what happened in the days immediately before and after its death spiral. Despite several attempts to stop its free fall[53], Terra ultimately failed.

By the end of Terra's collapse, over $60 billion had evaporated[54], leaving the currency worthless; $18.7 billion was directly lost in the Terra stablecoin; the remainder was tied to the closely related Luna token.

Figure G.1.1 — The Epic Collapse of Terra



In this section, we replicate the Terra situation to create a worst-case scenario for Argon, fully testing its resilience in a simulated death spiral.

We start with the same metrics as Terra:

Stablecoins In Circulation	18,700,000,000
Starting Price	$1.00
Ending Price	$0.000001

As with Terra before its collapse, we assume the Argon ecosystem is running smoothly, unaware of the impending crisis. The vaults contain around 1.5% of all bitcoins in circulation, and the Ulixee Data Network operates at an annual volume of less than 0.1% of the Argons in circulation.

Vaulted Bitcoins	300,000
Ulixee's Annual Network Volume	$10,000,000

Despite the massive drop, Argon fully recovers to its target price of $1.00 in under 72 hours. We invite you to explore our models and give us feedback. The code is open-sourced at github.com/argonprotocol/whitepaper-assets.

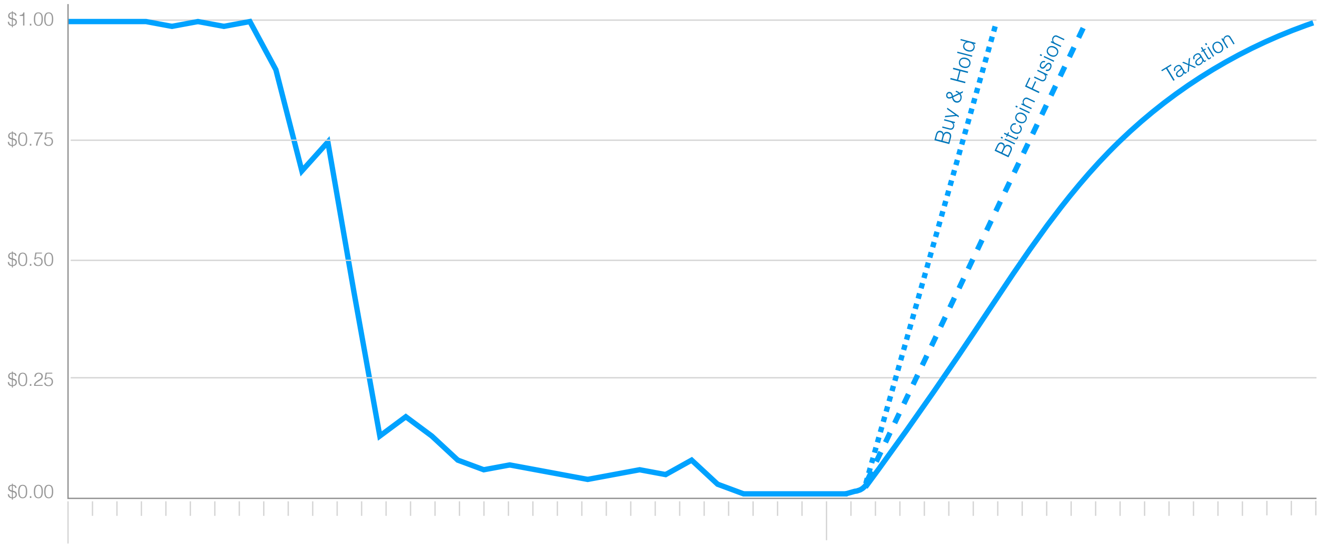
G.2 - Keep Calm and Burn On

Argon works due to the ability of its stabilization mechanisms to complement and counterbalance each other's weaknesses.

The Fusion Mechanism excels at rapid rebalancing while the the Taxation Mechanism ensures a guaranteed eventual rebalancing. Fusion is at its strongest near the top side of the target price, while Taxation performs exceptionally well in the death-spiral zone. Additionally, Fusion's risk of prematurely un-vaulting all the bitcoins is mitigated by Taxation's constant safety net.

These two mechanisms negate each other's black swan risks and amplify each other's strengths. Even better, both mechanisms operate independently of the stablecoin itself.

Figure G.2.1 — Replaying the Terra Scenario with Argon



Price drops that would spell disaster for any other stablecoin instead showcase Argon's remarkable resilience. The further Argon's price falls, the faster it rebounds — a stark contrast to how "collateral-backed" stablecoins operate. This creates a scenario where even if every Argon believer abandons the currency, it would still return to its pegged price within days, well, almost…

G.3 - Nothing Is Certain Except Death

There is one black swan scenario for which we have no solution. If it occurs, it will likely destroy Argon and any chance of its recovery. Three things must happen simultaneously:

1. Bitcoin drops to $0.000001
2. Argon drops to $0.000001
3. Ulixee's Data Network ceases to be used (i.e., annual activity of $0.00).

If all three occur at once, Argon's entire stabilization mechanism will likely implode with no chance of recovery. Of course, this situation hints at a larger apocalyptic problem for which we also have no solution.

IN CLOSING

We are readying the first public release of Argon. It will be open sourced and fully decentralized. A working codebase can be found at github.com/argonprotocol. We invite everyone to play around with our testnet (getting started instructions can be found at argonprotocol.org).

When Argon launches on the livenet, there will be no genesis blocks granting special tokens rights to founders, investors, pre-token holders, or anyone else. We believe a global currency should be owned by no one. The future should be an even playing field.

Next Steps

This whitepaper is the second in a series of three stablecoin papers. If you haven't already, we recommend going back and reading the first:

> *On the Stabilization of Collateral-Backed Stablecoins*. Our perspective on the history of stable currencies, the problem with today's stablecoins, and the future of Central Bank Digital Currencies (CBDCs).

The final whitepaper in this series will be published soon:

> *Bootstrapping a Global Currency*. This document outlines our strategy for bootstrapping the Argon from zero to one trillion. It covers the mining protocol behind our useful-proof-of-work blockchain, how our peer-to-peer settlement layer supports hundreds of thousands of transactions per second, and much 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 for reading countless drafts, giving invaluable feedback and in many instances even rewriting entire paragraphs — without your help 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] Clark, C., Byrnes B. (2024). *On The Stabilization of Collateral-Backed Stablecoins*. Argon Protocol. https://argonprotocol.org/on-the-stabilization-of-collateral-backed-stablecoins.pdf

[2] Schneider, F. (2017). Living in a fiat money world: The limits of monetary sovereignty. International Journal of Monetary Economics and Finance; Bassetto, M., & Galli, C. (2019). *Is inflation default? The role of information in debt crises.* American Economic Review, 109(10), 3556-3584. https://doi.org/10.1257/aer.20170721; Schreger, J., & Du, W. (2021). *Sovereign risk, currency risk, and corporate balance sheets.* SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3860465; Antipa, P. (2016). *How fiscal policy affects prices: Britain's first experience with paper money.* The Journal of Economic History, 76(4), 1044-1077. https://doi.org/10.1017/s0022050716000978.

[3] Thanh, B. N., Hong, T. N. V., Pham, H., Cong, T. N., & Anh, T. P. T. (2022). *Are the stabilities of stablecoins connected?* Journal of Industrial and Business Economics, 50(3), 515-525. https://doi.org/10.1007/s40812-022-00207-3; Galati, L., & Capalbo, F. (2023). *Silicon Valley Bank bankruptcy and stablecoins stability.* SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4437015.

[4] Davies, G. (1996). A history of money from ancient times to the present day (Rev. ed.). University of Wales Press.

[5] Goetzmann, W. N. (2016). Money changes everything: How finance made civilization possible. Princeton University Press.

[6] Kim, Y. S., & Lee, M. (2012). Return on commodity money, small change problems, and fiat money. *Journal of Money, Credit and Banking, 44*(2-3), 533-549. https://doi.org/10.1111/j.1538-4616.2012.00500.x; Gębarowski, R., Dróżdż, S., Górski, A. Z., & Oświęcimka, P. (2015). Competition of commodities for the status of money in an agent-based model. *Acta Physica Polonica A, 127*(3a), A-51-A-54. https://doi.org/10.12693/aphyspola.127.a-51

[7] Glahn, R. V. (2005). The origins of paper money in China. In *The origins of value* (pp. 65-90). https://doi.org/10.1093/oso/9780195175714.003.0005; Glahn, R. V. (2010). Monies of account and monetary transition in China, twelfth to fourteenth centuries. *Journal of the Economic and Social History of the Orient, 53*(3), 463-505. https://doi.org/10.1163/156852010x506047; Mao, Y. (2023). The influence of Tang dynasty's policies on Sogdian commercial networks. *Communications in Humanities Research, 4*(1), 614-620. https://doi.org/10.54254/2753-7064/4/20220927

[8] Ho, J. S. (2014). Monetary authority independence and stability in medieval Korea: The Koryŏ monetary system through four centuries of East Asian transformations, 918-1392. *Financial History Review, 21*(3), 259-280. https://doi.org/10.1017/s0968565014000213

[9] 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

[10] Nakamoto, S. (2009). Bitcoin Open Source Implementation of P2P Currency. The Cryptography Mailing List. https://satoshi.nakamotoinstitute.org/

[11] Larimer, D., Hoskinson, C., & Larimer, S. (2014). *BitShares whitepaper that first mentions BitUSD*. https://blog.bitmex.com/wp-content/uploads/2018/06/173481633-BitShares-White-Paper.pdf

[12] Bank for International Settlements. (2023). *Crypto and digital currencies: Unpacking policy issues* (BIS Paper No. 141). https://www.bis.org/publ/bppdf/bispap141.pdf

[13] Choi, J., & Kim, H. (2024). *Stablecoins and central bank digital currency: Challenges and opportunities.* Oxford Research Encyclopedia of Economics and Finance. https://doi.org/10.1093/acrefore/9780190625979.013.910; Klages-Mundt, A., & Minca, A. (2020). While stability lasts: A stochastic model of stablecoins. arXiv. https://doi.org/10.48550/arxiv.2004.01304; Abraham, M. (2024). *Crypto lending and stablecoin de-pegging: Key risks and challenges.* International Journal of Cryptocurrency Research, 4(1), 79-100. https://doi.org/10.51483/ijccr.4.1.2024.79-100; Arner, D. W., Auer, R., & Frost, J. (2020). *Stablecoins: Risks, potential and regulation.* SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3979495.

[14] Keister, T., & Sanches, D. R. (2019). *Should central banks issue digital currency?* Working Paper (Federal Reserve Bank of Philadelphia). https://doi.org/10.21799/frbp.wp.2019.26; Anthony, N., & Michel, N. (2023). *Central Bank Digital Currency: Assessing the Risks and Dispelling the Myths.* Cato Institute. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4638953.

[15] Klages-Mundt, A., & Minca, A. (2022). While stability lasts: A stochastic model of noncustodial stablecoins. *Mathematical Finance, 32*(4), 943-981. https://doi.org/10.1111/mafi.12357; Fu, S., Wang, Q., Yu, J., & Chen, S. (2024). Leveraging ponzi-like designs in stablecoins. *International Journal of Network Management, 34*(4). https://doi.org/10.1002/nem.2277

[16] CoinGecko. (2022). *Stablecoins Statistics Report*. https://www.coingecko.com/research/publications/stablecoins-statistics

[17] CPI Databases compiled by The U.S. Labor Department's Bureau of Labor Statistics: https://www.bls.gov/cpi/data.htm

[18] Stablecoin market cap as of September 3, 2024: https://coincodex.com/cryptocurrencies/sector/stablecoins/

[19] Rustgi, N. (2023). *Frax's shift to a fully backed stablecoin signals the end of DeFi's algorithmic experiment*. CoinTelegraph. https://cointelegraph.com/news/frax-s-shift-to-a-fully-backed-stablecoin-signals-the-end-of-defi-s-algorithmic-experiment

[20] Laboure, M. (2024). *What stablecoins can learn from history's currency pegs*. World Economic Forum. https://www.weforum.org/agenda/2024/07/what-stablecoins-can-learn-from-historys-currency-pegs/

[21] Ferguson, N., Schlefer, J. (2017). *Who Broke the Bank of England?* Harvard Business School Case Collection. https://www.hbs.edu/faculty/Pages/item.aspx?num=36754

[22] Bennet, C., Chan, R., Shah, M., Shetty, S. (2024). *Central Bank Digital Currencies: Building Block of the Future of Value Transfer*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/financial-services/bk/en-central-bank-digital-currencies.pdf

[23] Statista. (2024). *Inflation rate in Argentina*. https://www.statista.com/statistics/316750/inflation-rate-in-argentina/

[24] World Gold Council. (2024). *Gold Demand Trends*. https://www.gold.org/goldhub/research/gold-demand-trends/gold-demand-trends-full-year-2023/supply

[25] Diaconis, P., & Mosteller, F. (1989). Methods of studying coincidences. *Journal of the American Statistical Association*. https://www.stat.berkeley.edu/~aldous/157/Papers/diaconis_mosteller.pdf

[26] Svensson, L. E. O. (2014). How to weigh unemployment relative to inflation in monetary policy? *Journal of Money, Credit and Banking, 46*(S2), 183-188. https://doi.org/10.1111/jmcb.12158; Williams, J. C. (2013). A defense of moderation in monetary policy. *Federal Reserve Bank of San Francisco, Working Paper Series*, 01-29. https://doi.org/10.24148/wp2013-15; D'Amico, S., English, W. B., López-Salido, D., & Nelson, E. (2012). The Federal Reserve's large-scale asset purchase programmes: Rationale and effects. *The Economic Journal, 122*(564), F415-F446. https://doi.org/10.1111/j.1468-0297.2012.02550.x; English, W. B., López-Salido, D., & Tetlow, R. (2013). The Federal Reserve's framework for monetary policy: Recent changes and new questions. *Finance and Economics Discussion Series, 2013*(76), 1-70. https://doi.org/10.17016/feds.2013.76

[27] Galati, L. and Capalbo, F. (2023). Silicon valley bank bankruptcy and stablecoins stability. https://doi.org/10.2139/ssrn.4437015

[28] Dale, B. (2023). *Circle scrambles amid SVB fallout as USDC loses 1:1 peg*. Axios. https://www.axios.com/2023/03/11/circle-usdc-peg-svb

[29] Press Release (2023). *FDIC Acts to Protect All Depositors of the former Silicon Valley Bank*. https://www.fdic.gov/news/press-releases/2023/pr23019.html

[30] De, N. (2023). *USDC Stablecoin Regains Dollar Peg After Silicon Valley Bank-Induced Chaos*. CoinDesk. https://www.coindesk.com/business/2023/03/13/usdc-stablecoin-regains-dollar-peg-after-silicon-valley-bank-induced-chaos/

[31] Partz, H. (2018). *US Stablecoin Project Basis Raises $133 Mln From Major VC Firms*. CoinTelegraph. https://cointelegraph.com/news/us-stablecoin-project-basis-raises-133-mln-from-major-vc-firms

[32] Geron, T., Chernova, Y. (2018). *'Stablecoin' Project Basis Is Shutting Down After Raising $135 Million*. The Wall Street Journal. https://www.wsj.com/articles/stablecoin-project-basis-is-shutting-down-after-raising-135-million-11544730772

[33] Kwon, D. (2020). *Announcing TerraUSD (UST)— the Interchain Stablecoin*. Medium. https://medium.com/terra-money/announcing-terrausd-ust-the-interchain-stablecoin-53eab0f8f0ac

[34] Osipovich, A., Ostroff, C. (2022). *TerraUSD Crash Led to Vanished Savings, Shattered Dreams*. The Wall Street Journal. https://www.wsj.com/articles/terrausd-crash-led-to-vanished-savings-shattered-dreams-11653649201

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

[36] Nolan, T. (2013). *Alt chains and atomic transfers*. BitcoinTalk. https://bitcointalk.org/index.php?topic=193281.msg2003765#msg2003765

[37] Poon, J., Dryja, T. (2016). *The Bitcoin Lightning Network*. https://lightning.network/lightning-network-paper.pdf#page=30

[38] Zamyatin, A., Harz, D., Lind, J., Panayiotou, P., Gervais, A., Knottenbelt, W. (2018). *XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets*. Whitepaper. Imperial College London, SBA Research. https://eprint.iacr.org/2018/643.pdf

[39] Luongo, M. (2020). *A Decentralized Redeemable BTC-backed ERC-20 Token*. https://whitepaper.io/document/691/tbtc-whitepaper

[40] Bugnet, T., Zamyatin, A. (2022). *XCC: Theft-Resilient and Collateral-Optimized Cryptocurrency-Backed Assets*. https://eprint.iacr.org/2022/113.pdf

[41] Sun, Z. (2022). *Half of all DeFi exploits are cross-bridge hacks*. CoinTelegraph. https://cointelegraph.com/news/report-half-of-all-defi-exploits-are-cross-bridge-hacks

[42] Young, S. (2024). *BitGo Abruptly Pivots on Holders of WBTC Multi-Sig Keys Following Co*. UnchainedCrypto. https://unchainedcrypto.com/bitgo-abruptly-pivots-on-holders-of-wbtc-multi-sig-keys-following-community-outcry/

[43] The Babylon Team (2023). *Bitcoin Staking:* Unlocking 21M Bitcoins to Secure *the Proof-of-Stake Economy*. https://docs.babylonchain.io/papers/btc_staking_litepaper.pdf

[44] As of July 27, 2024: https://www.coingecko.com/en/coins/wrapped-bitcoin

[45] Ruffing, T., Kate, A., Schroder, D. (2015). *Liar, Liar, Coins on Fire*! Whitepaper. https://publications.cispa.saarland/565/1/penalizing.pdf

[46] Tas, E., Tse, D., Gai, F., Kannan, S., Maddah-Ali, M., Yu, F. (2023). *Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities*. Whitepaper. https://arxiv.org/pdf/2207.08392

[47] Bitcoin pricing data was retrieved from blockchain.com's API.

[48] The code used to generate these models have been open sourced at https://github.com/argonprotocol/whitepaper-models/designing-a-stabler-stablecoin/bitcoin-vaulting

[49] Soli, V. O., Harvey, S. K., & Hagan, E. (2008). Fiscal policy, private investment and economic growth: The case of Ghana. *Studies in Economics and Finance, 25*(2), 112-130. https://doi.org/10.1108/10867370810879438; Lawman, H. G., Bleich, S. N., Yan, J., LeVasseur, M. T., Mitra, N., & Roberto, C. A. (2019). Unemployment claims in Philadelphia one year after implementation of the sweetened beverage tax. *PLOS ONE, 14*(3), e0213218. https://doi.org/10.1371/journal.pone.0213218

[50] The first burning algorithm in cryptocurrency is generally credited to Counterparty, a protocol built on top of Bitcoin in 2014. Counterparty introduced the concept of "proof of burn" as a way to distribute its native token, XCP.

[51] Taken from Visa’s Annual Year End Report for 2023: https://annualreport.visa.com/financials/default.aspx

[52] Golosov, M. and Lucas, R. E. (2007). Menu costs and phillips curves. Journal of Political Economy, 115(2), 171-199. https://doi.org/10.1086/512625; Chin, K. (2018). New keynesian phillips curve with time-varying parameters. Empirical Economics, 57(6), 1869-1889. https://doi.org/10.1007/s00181-018-1536-2

[53] Browne, R. (2022). *$3 billion in bitcoin was sold in a last-ditch attempt to save UST stablecoin from collapse*. CNBC. https://www.cnbc.com/2022/05/16/what-happened-to-the-bitcoin-reserve-behind-terras-ust-stablecoin.html

[54] Shen, M. (2022). *How $60 Billion In Terra Coins Went Up In Algorithmic Smoke*. Bloomberg. https://www.bloomberg.com/graphics/2022-crypto-luna-terra-stablecoin-explainer/