Mint Cash

A Bitcoin-backed, permissionless and price-stable payments and savings currency system

Shin Hyojin 신효진 (hyojin@mintca.sh)
version mentha-0 (prerelease)
September 2023

Abstract. We present Mint Cash, a system that achieves currency value stability against various fiat currencies without relying on a centralized banking system that these fiat currencies depend on. While there are multiple different approaches to representing fiat currency on distributed ledgers like the blockchain, Mint Cash employs a unique approach of constructing two separate synthetic swap mechanisms that purely rely on Bitcoin to maintain buying power. Monetary stability models proven by contemporary currency regimes are tightly integrated into the system, from managing government spending, achieving yields, and adjusting interest rates to avoid interest arbitrage resulting in net value outflow. Interest powered by liquid staking collateral is adjusted against external interest rates and real money demand, providing a consistent, yet highly efficient yield source for Cash holders. Support for multiple currencies outside of the U.S. Dollar provides an effective hedge for the system as a whole; synthetic swaps and borrows enable new opportunities that can compose non-U.S. Dollar currencies with decentralized finance (DeFi) protocols predominately valued in the U.S. Dollar. The authors believe Mint Cash is a critical value add to Bitcoin by providing stability in addition to censorship and inflation resistance properties it provides, potentially serving as the world's largest decentralized currency built for a decentralized economy, ready for mass adoption.

I. Previous Work

1. Stabilizing Foreign Exchange Rates

Even though blockchain technology and cryptocurrencies only became possible after the introduction of Bitcoin[1], the fundamental economic concepts for achieving value stability against one or multiple external currencies are not new. Modern fiat currencies heavily depend on monetary policies as set forth independently by R. A. Mundell[2] and J. M. Fleming[3], commonly known as the Mundell-Fleming or IS-LM-BP model. Unlike the IS-LM model[4] that have described a mostly closed economy with negligible levels of imports and exports, IS-LM-BP introduces foreign exchange rates of currencies as another parameter impacted by domestic monetary policy under a free market with frequent international trade across different countries with independently managed currencies.

As a refresher on how Keynesian economics described economic equilibrium, this section reviews two basic models defined by Keynes as an alternative to classic economics: IS-LM and AD-AS.

The IS-LM model describes the relationship between **investment savings** and **liquidity money**, where the intersection of these curves represents economic equilibrium. The investment savings (IS) curve is represented as

Definition I.1.1. The investment savings (IS) curve.

$$Y = C(Y - T(Y)) + I(r) + G + NX(Y)$$

where:

- Y equals income
- $C(Y - T(Y))$ equals customer spending minus taxes levied (T(Y))
- $I(r)$ equals business investment moving in inverse to the interest rate parameter (r)
- G equals government spending
- $NX(Y)$ equals net exports, i.e. exports minus imports

As $I(r)$ represents lower interest rates leading to higher investments (and vise versa), this curve means **lower interest rates result in higher net income, and higher interest rates mean lower net income**, assuming $Y = AD$ (where AD is aggregate demand).

The liquidity money (LM) curve is represented as

Definition I.1.2. The liquidity money (LM) curve.

$$\frac{M}{P} = L(i, Y)$$

where:

- $\frac{M}{P}$ equals the amount of real money
  - M equals the amount of nominal (non-adjusted) money
  - P equals the current price level

  thus representing the amount of money value in circulation adjusted by inflation.
- L is a function of i (the interest rate) and Y (real income) that represents **real demand for money**

As money supply $\frac{M}{P}$ is completely independent from both i and Y, being under complete control of the central bank (and ultimately the government), this means

- from a **monetary policy** standpoint:
  - more money supply being introduced means lower interest rates and higher income, shifting the LM curve to the right
  - less money supply means higher interest rates and lower income, shifting the LM curve to the left

- from a **fiscal policy** (i.e., deficit government spending) standpoint:
  - more deficit government spending (G) may increase total income while not impacting savings rates, as this shifts the IS curve to the right, and vice versa

To properly calculate the effects of price levels (P) on equilibrium income defined by the IS-LM curve, the AD-AS model is used. AD-AS represents the relationship between **aggregate demand** and **aggregate supply**, which in turn calculates how economic upsides and downturns affect money demand and, consequently, price levels.

The aggregate demand (AD) curve is an expansion of the IS curve at different price levels, defined as:

Definition I.1.3. The aggregate demand (AD) curve.

$$Y = Y^d\left(\frac{M}{P}, G, T, Z_1\right)$$

where:

- Y equals real GDP (gross domestic product)
- M equals the amount of nominal money
- P equals the current price level
- G equals government spending
- T equals taxies levied at real money levels
- Z_1 equals other miscellaneous parameters that affect the location of the IS curve, i.e. any other forms of spending

This means:

- A higher $\frac{M}{P}$ value — real money supply — implies higher aggregate demand, and vice versa
- A higher G value — government spending — implies higher aggregate demand, and vice versa
- A higher T value — higher taxation — implies lower aggregate demand, and vice versa
- Any other form of spending implies higher aggregate demand and vice versa

The aggregate supply (AS) curve is usually described to be:

- heavily influenced by **price level** P in the short term,
- heavily influenced by **real GDP** Y in the long term,
- and influenced by both parameters in the middle.

The Mundell-Fleming model, also known as the IS-LM-BP model — as an extension of the IS-LM model — adds another parameter called **balance of payments (BP)**, which defines flow of foreign currency and assets relative against a nation state's sovereign currency. Mundell-Fleming also adds foreign interest rates and foreign GDP as factors determining value of money, as interest arbitrage affects value flow to and from a particular currency.

The IS curve under Mundell-Fleming is defined as:

Definition I.1.4. The expanded investment savings (IS) curve under the Mundell-Fleming model.

$$Y = C\big(Y - T(Y), i - E(\pi)\big) + I(i - E(\pi), Y_{t-1}) + G + NX(e, Y, Y^*)$$

where:

- $E(\pi)$ equals expected rates of inflation. Total customer spending C is adjusted by interest rates minus inflation.
- Y_{t-1} equals gross domestic product (GDP) of the previous fiscal period. Business investment I is adjusted by interest rates adjusted by expected inflation and previous GDP data.
- e equals the nominal exchange rate (the value of foreign currency valued in domestic currency), and Y^* equals the combined GDP of all foreign countries that this nation conducts trade with. Net exports NX is affected by all three parameters e, Y (GDP) and Y^*.

The balance of payments (BP) curve consists of:

Definition I.1.5. The balance of payments (BP) curve.

$$BP = CA + KA$$

where BP equals balance of payments, CA equals the current account surplus (net foreign assets), and KA equals the capital account surplus (net flow of currency entering an economy for investment).

IS-LM-BP assumes:

Definition I.1.5-1. Current account surplus.

$$CA = NX$$

i.e. current account only consists of foreign currency flows being used for imports and exports, and:

Definition I.1.5-2. Capital account surplus.

$$KA = z(i - i^*) + k$$

where:

- k equals purely external factors for capital flow
- z equals capital flow affected by interest rates
- i^* equals the foreign interest rate

The function $\frac{d}{dx}z(x)$ represents the degree of capital mobility, i.e., how much effect interest rate delta between domestic and foreign economies will have on total capital account cashflow.

Because existing assumptions under IS-LM only holds when BP is at perfect capital mobility, it is well known only two of the following three economic factors may be achieved:

- a **stable exchange rate** against one or more foreign currencies
- a **sovereign monetary policy**, i.e. being able to set independent interest rates
- **free capital flows**, i.e. no imposed capital controls on foreign exchange markets

This is also known as the **impossibility trinity**. Most contemporary currency regimes choose to employ all three factors, but only partially — this allows for central banks to have *some* flexibility over their monetary policy while not being forced to choose between either a highly fluctuating exchange rate, or complete control over capital flows (which would, consequently, block foreign investments to bootstrap GDP).

2. Existing Stablecoin Implementations

While Bitcoin and blockchain technology have enabled truly borderless, peer-to-peer payments over the World Wide Web, a core problem with cryptocurrencies built on top of public blockchains has always been **stability against existing, government-issued fiat currencies.** Cryptocurrencies are simply not a viable option for every-day payments and savings if their extreme volatility of value against foreign fiat currency from speculative demand continues.

Multiple forms of **stablecoins**, a type of cryptocurrency that are designed to maintain a fixed or relatively stable exchange rate against fiat currencies, have been proposed and are in circulation, especially on the Ethereum blockchain.

There are three types of stablecoins currently available for users of public blockchains:

- **A. Fiat and asset-backed stablecoins.** Those include stablecoins that are 1:1 backed by U.S. bank deposits and/or government bonds, like USD Coin (USDC) minted by Circle; and stablecoins backed by other traditional assets that can be used to buy back underlying U.S. Dollars, like Tether (USDT). While stablecoins of this class are usually considered to be the safest to hold, they still have operational concerns, including but not limited to the following:

    - **Heavy dependencies on traditional financial infrastructure**: while stablecoins facilitate faster international settlements of fiat currencies backing them, they may lose on-chain value when there is a black swan event within the traditional financial system that peer-to-peer settlements were supposed to avoid in the first place.

      USDC temporarily de-pegged from its US$1 market value in early 2023 when Silicon Valley Bank (SVB), one of USDC issuer Circle's major banking partners, suffered from a bank run event and was unable to redeem funds from SVB to buy back USDC panic sells with actual U.S. Dollars. While the de-peg was ultimately resolved with federal intervention to restore SVB's deposit balances and emergency funding out of Circle's corporate assets, this incident serves as a reminder that **completely depending on traditional financial systems to custody**

collateral may bring over and amplify certain economic problems that blockchain technology was meant to solve.

  - **Trust and transparency issues with collateral assets held off-chain**. This is especially of concern with Tether (USDT), where instead of backing stablecoins with U.S. bank deposits and government bonds, the company actively conducts investments into illiquid and often unstable assets — such as bonds and equity issued by private companies — with assets that are supposed to back USDT and hold its peg with the U.S. Dollar. Tether Limited does conduct periodic audits of its asset portfolio backing USDT, however its legitimacy and accuracy is often questioned by critics of Tether and its stablecoin products.

    This means collateral assets backing stablecoins may be used as leverage liquidity against active, and often risky, investments, which is exactly what cryptocurrencies tried to avoid; perhaps this is closer to an unauthorized offshore bank or even a hedge fund than an accurate representation of the U.S. Dollar on the blockchain.

- **B. Overcollateralized, cryptocurrency-backed stablecoins**. Unlike fiat and asset-backed stablecoins, overcollateralized stablecoins are a type of synthetic asset, meaning they are effectively tokenized loans backed by cryptocurrency collateral that are often valued much higher than the market value of stablecoins being minted. Examples of these stablecoins include DAI, a stablecoin minted by the MakerDAO (MKR) protocol, and Synthetix USD (sUSD), a synthetic asset pegged to the U.S. Dollar issued by Synthetix (SNX); more recent implementations may have higher capital efficiency and lower borrow rates — sometimes even close to zero — at the cost of fluctuating exchange rates, including Liquity (LUSD) and Reflexer Finance (RAI).

  While, arguably, these are much more decentralized solutions than completely depending on off-chain collateral held by centralized custodians, overcollateralized stablecoins do have their own problems:

- **Capital inefficiency**. As overcollateralized stablecoins are effectively defined as liquid loan positions against non-stable, on-chain collateral, most of them require depositing more assets than its resulting stablecoin mint value that are also often subject to liquidation when collateral value goes down than the value of borrowed stablecoins. This capital inefficiency creates a liquidity crisis where, without external, centralized actors that have vested interest in the stablecoin system, controlling available supply of these stablecoins may be difficult, which limits the system's ability to maintain a constant value peg against external assets.

- **Lack of incentives to arbitrage**. Overcollateralized stablecoin systems and CDPs (collateralized debt positions) require borrowers to constantly borrow and repay their loans to arbitrage a stablecoin's value back to its intended value peg. However, there is close to zero incentives for borrowers to constantly manage their positions, as (i) capital put up as stablecoin collateral is already worth more than the value of its corresponding loan position, and (ii) arbitrage requires even more capital to buy or sell stablecoins to restore its market value at its intended peg against an external fiat currency.

  Because it can be difficult to persuade users to mint new stablecoins by taking collateral liquidation risk (and effectively longing the asset), some protocols offer a relatively low minimum loan-to-value (LTV) ratio or borrow interest rates (sometimes even being sub-zero) to address the stablecoin supply problem. As stablecoins must follow interest rates of external currencies in some form to avoid a significant de-peg event, however, **having a low interest rate factor while external interest rates are generally high may cause the stablecoin to fall below its intended peg even when the system has more than enough assets to back them at peg.**

  This is because there isn't enough demand for external actors to buy and hold the stablecoin at the expense of liquidating other forms of assets, and the only actor within the system that can correct the de-peg are borrowers, which require additional capital to buy back and repay their loan position for the arbitrage to work as intended (as $i - i^* \leq 0$, therefore the BP curve represents a negative slope (BP^{-}) and sub-zero net capital flows — $KA = z(i - i^{*}) + k$).

- **Liquidations & collateral risk.** There is also significant risk of incorrect and/or mismanaged liquidations under a CDP-based stablecoin model, which may result in a cascading loop of bad debt that the protocol cannot independently handle. Even if liquidations are correctly handled, synthetic asset liquidations have an additional risk vector where **implied price volatility of said debt tokens increases exponentially when the market value of their underlying collateral is also highly volatile.** Liquidators are disincentivized to buy back debt tokens (stablecoins) during collateral auctions, as liquidations may result in a loss for the liquidator, even at a high liquidation premium ratio.

  This is in contrast with money market liquidations, where loans are denominated in assets and not debt tokens, and thus implied volatility is an independent variable for both deposits and borrows — not intertwined.

- **C. "Algorithmic" stablecoins**. These types of stablecoins solely rely on market demand for assets to maintain stability; the general idea is that, when there is more demand for stablecoins, their supply can simply increase, and when there is less demand, the protocol can decrease supply — maintaining peg while not affecting the entire asset pool.

  The concept of using algorithms based on supply and demand to adjust stablecoin peg was first pioneered by Basis, which was shut down by the Securities and Exchange Commission (SEC) in 2017 due to concerns its Shares tokens might be unregistered securities — as any expansions in Basis stablecoins (seigniorage) are distributed to Shares holders, and that constitutes the definition of a security as a form of dividends.

  During the 2020 DeFi boom, multiple attempts at algorithmic stablecoins have emerged; perhaps the most well-known implementation is Terra[5], initially built in 2018 but collapsed with a so-called death spiral event on May 2022.

Terra stablecoins are purely based on swaps to and from another token known as Luna to maintain its peg against multiple fiat currencies. As a reminder, the concept with Terra was that every unit of Terra stablecoin would be swappable to Luna equal in value with the same number of units of the base fiat currency the Terra stablecoin would be pegged with, and vice versa. For instance, every 1 UST (TerraUSD) is swappable to 1 U.S. Dollar worth of Luna, and 1 U.S. Dollar worth of Luna is swappable to 1 UST (TerraUSD). When the value of 1 UST is above 1 U.S. Dollar, anyone can buy 1 U.S. Dollar worth of Luna, swap it to 1 UST, and sell it at more than 1 U.S. Dollar, earning a profit. When the value of 1 UST is below 1 U.S. Dollar, anyone can buy 1 UST with less than 1 U.S. Dollar, swap it to 1 U.S. Dollar worth of Luna, and sell them on the market, also earning a profit.

The problem with this mechanism was that when everyone wants to sell both Terra stablecoins and Luna, and there is no demand for buying Luna, even if 1 UST were to be swapped to 1 U.S. Dollar worth of Luna following its intended mechanism, **there would be no buy pressure for Luna that would enable that additional Luna minted to be sold back to *actual* U.S. Dollars**. This would result in Luna infinitely being printed to compensate for that loss of value without being able to restore UST peg properly, as seen with the May 2022 crash.

While algorithmic stablecoins are mostly considered to be experimental and not suitable for holding value long-term especially after Terra's near-complete collapse, there are unique advantages to this approach despite its flaws:

- **High capital efficiency**. Unlike CDP-based stablecoins, algorithmic stablecoins are capital efficient because there are no additional insurance parameters to protect a collateralized loan position against liquidations. Additionally, since algorithmic stablecoin protocols do not depend on interest rates for adjusting supply, standard interest rate adjustment models seen with existing fiat currencies may be used for controlling demand for said stablecoin.

- **Liquidity for non-U.S. Dollar stablecoins**. Most value on decentralized finance (DeFi) is denominated in U.S. Dollars, and the absolute majority of stablecoins pegged to a fiat currency are also pegged to the U.S. Dollar. While this is efficient from a liquidity management standpoint — as supporting more currencies inevitably results in liquidity fragmentation and management overhead — only supporting U.S. Dollars as the sole fiat currency represented on the blockchain takes away choice for users outside of the U.S. that do not use the USD as their primary currency.

As algorithmic stablecoins are synthetic assets and allow for synthetic swaps between different asset types, **they can support multiple currencies without having to provide additional liquidity.** Algorithmic stablecoins also can, in theory, support existing U.S. Dollar-based used cases with stablecoins pegged to another fiat currency.

II. Desired System Properties

1. No Centralized Collateral Risk

Mint Cash should have zero dependencies on external, centralized banking systems; i.e. **anyone that can accept Bitcoin payments should also be able to accept Mint Cash payments, regardless of who they are.**

While actors like Circle (USDC) and Tether (USDT) may blocklist and arbitrarily burn stablecoins held with a wallet, Mint Cash currencies fundamentally cannot be censored — as the system is not bound to legacy financial systems.

The value add for Mint Cash is to **bring monetary stability to everyone that has access to Bitcoin and its peer-to-peer transaction network, in addition to censorship resistance properties that Bitcoin already provides.**

2. High Capital Efficiency

Mint Cash should be swappable to and from its collateral asset similar to synthetic asset swaps, and should not require loan positions to mint new stablecoins. This is because:

- **Mint Cash should be able to control its own interest rates against each and every fiat currency the system is targeting.** As stablecoin supply is governed by borrow interest rates under an overcollateralized model, low rates are a prerequisite for providing enough stablecoin liquidity for users to trade on the market.

  This may result in a dilemma in monetary policy, where low rates reduce demand for holding stablecoins as an asset, therefore requiring additional capital in addition to loan collateral; and rate adjustments may be required as part of a forex stability policy — while higher rates reduce stablecoin supply, making it difficult to properly perform expansions for said stablecoin to stay on peg.

- **Additional capital may be required to keep overcollateralized stablecoins on peg.** For instance, when a user opens a loan position to mint stablecoins and liquidates them on the market — which should be incentivized behavior to provide enough stablecoin liquidity — there is no way for these users with loan positions to rebalance stablecoin market value to be back on peg, unless additional capital is used to buy back stablecoins and liquidate their positions.

  While overcollateralized stablecoins may seem like they should not de-peg from its intended value because they are backed by more collateral than their face loan value — which equals the amount of stablecoins minted — **market value does not equal the value of collateral locked within a synthetic asset protocol.** This means these loan position tokens should be bought to repay the loan position in order for the collateral to *actually* take effect, excluding liquidations.

3. A Monetary Policy Resilient to External Price Shock

Mint Cash should be able to dynamically adjust monetary and fiscal policy to absorb both short-term and long-term price shock on the open market. These policies are based on the Mundell-Fleming model and related research on forex rate stabilization, with a focus on multiple forms of modern currency regimes.

The Mint Cash system should be designed to minimize the range of value fluctuation against a stablecoin's corresponding fiat currency, and not enforce a hard one-to-one peg. Some monetary policy considerations of Mint Cash currencies include:

- **Interest rate decisions** against fiat currency interest rates a Mint Cash currency is designed to track
- **Capital flow limits** both for Treasury shares and collateral assets
- A **peg fluctuation tolerance range**, which is indirectly defined by virtual swap liquidity

Some economic policy factors require an expedited governance process that should be able to make decisions within hours; how Mint Cash orchestrates protocol governance for adjusting these monetary and fiscal policy levers are described with later sections of this paper.

4. Liquid Non-U.S. Dollar Stablecoins and Deposits

Mint Cash should be able to support multiple currencies outside of the U.S. Dollar, and also be able to actively maintain peg against these currencies. This is critical for a few reasons:

- Support for multiple currencies bring in demand for transactions that mostly are conducted outside of the United States; considering regulatory uncertainty around decentralized finance (DeFi) applications within the United States, it makes sense for stablecoins to support more currencies outside of the U.S. Dollar.

- From a monetary stability standpoint, **supporting multiple currencies act as a hedge between different external interest rate regimes**, as **interest rate factors greatly impact value of fiat currencies** — and Cash currencies designed to track their market value are also affected.

Mint Cash is the **only stablecoin system that can achieve scalability for multiple currency systems at scale**, without having to provide onchain liquidity for every single currency pair. This greatly improves composability between Cash currencies pegged to different fiat currencies, as they do not explicitly require liquidity to be swapped to and from one another — which greatly simplifies user experiences for applications that do not primarily target the U.S. market.

III. Mint Cash: System Design

Mint Cash is implemented on top of a heavily modified version of Terra Core (renamed Terra Classic after TerraUSD's depeg event), a Cosmos SDK based blockchain that once served the Terra stablecoin protocol[5].

While Terra as an algorithmic stablecoin has catastrophically failed, **the Terra stablecoin design and codebase had some significant advantages that the authors believe are worth revisiting**:

- **No centralized collateral risk.** If the Terra system worked correctly as intended, the Terra family of stablecoins would have been one of the most censorship resistant stablecoin implementations while also remaining stable against market value of multiple fiat currencies. MakerDAO's DAI, for instance, holds more than half of its collateral backing DAI in USDC at the time of writing, a stablecoin issued by a U.S. entity (Circle) that may get shut down by a U.S. based financial institution at any time.

  This is to mitigate some of the issues mentioned with overcollateralized stablecoins mentioned with previous sections of this paper, although this does **expose the protocol to centralized collateral risk**, which may result in certain wallet addresses getting sanctioned or shut down to comply with government orders — as not complying with these orders may result in not being able to redeem significant portions of stablecoin collateral.

- **High capital effeciency.** The Terra stablecoin system was one of the only synthetic asset based stablecoins that did not require loan positions to mint new stablecoin units into circulation. This was because Luna, Terra's native mining token, was assumed to have sufficient buying power to contract Terra supply at all times, therefore never requiring additional collateral or external buybacks to keep Terra stablecoins on peg.

While it turned out Luna did *not* have sufficient buying power to properly contract Terra supply at all times, this system may still be very efficient if the death spiral problem is properly addressed with — i.e. as long as said collateral can sufficiently contract stablecoin supply without relying on a token that can be infinitely minted.

- **Support for non-U.S. Dollar stablecoins.** One feature of the Terra protocol that even its developers failed to sufficiently recognize was its ability to instantly add support for any currency, as long as (i) the currency is liquid enough to be traded against Luna, (ii) price oracles against that currency can be reliably established, and (iii) enough information is available to the public on that currency so that economic parameters for that currency may be properly set without disturbing the stability mechanism for other stablecoins.

  Terra's focus on TerraUSD (UST) may have made sense from a business perspective, but this was at the expense of almost completely abandoning one of its key features with Terra's original intended design.

  Considering a vast majority of decentralized finance (DeFi) users come from outside the United States due to regulatory uncertainty around security regulations, it makes sense for stablecoins to provide more options to users outside of the U.S. Dollar, while retaining compatibility with existing DeFi protocols denominated in the U.S. Dollar.

Using the Cosmos SDK technical stack to implement the Mint Cash protocol has several additional advantages:

- **Secure cross-chain asset bridging and messaging over IBC (Inter-Blockchain Communication).** Mint Cash relies on collateral types that are not native to any chain supporting smart contracts. Such assets require a reliable and decentralized asset transport solution that can scale across many different consensus algorithms and smart contract VMs, and the only production-ready solution for achieving these goals as of the time of writing is IBC.

Exports of Mint Cash currencies to other blockchains is also critical to achieving economies of scale, and IBC can transport native Mint Cash assets for use outside of the Mint Cash ecosystem securely — without fears of being sanctioned by a central entity.

- **Vertical integration between technical and economic systems of the protocol.** There are certain features of the Mint Cash protocol that requires vertical integration between the actual execution environment smart contract code and transactions are processed and economic policies, such as taxation policies and staking returns.

  Versatility offered by the Cosmos SDK allows for these features to be implemented directly at the protocol level, without having to resort to smart contract level hacks that may expose potential security vulnerabilities.

Mint Cash aims to continue working on what Terra set out to do initially, but in a completely transparent and — most importantly — sustainable manner: **a decentralized economy needs decentralized money that is stable enough and sufficiently censorship-resistant**.

1. Macroeconomic Assumptions

Mint Cash is built on modern currency stabilization theories and concepts. **This includes, but not limited to, the following macroeconomic assumptions**:

1. **The impossibility trinity set with the Mundell-Fleming model also stands true with transactions between cryptocurrencies and fiat currencies**. This means decentralized currencies face the exact same dilemma that plagues central banks and governments: that (i) independent monetary policy, (ii) stable exchange rates, and (iii) free movement of capital cannot be perfectly achieved at once — only two out of three policies may be chosen at a time.

   Most modern governments and their currencies choose to partially achieve all three policies instead of perfectly achieving two and completely abandoning the remaining policy choice. However, as policy goals of the Mint Cash system is focused heavily on maintaining macroeconomic stability instead of having a sovereign savings rate (unlike what TerraUSD and Anchor tried to do), we significantly reduce the independent monetary policy factor and increase the stable exchange rate factor, albeit not being at perfect value equilibrium.

2. **There will be very little native spending demand for calculating spending and GDP under traditional macroeconomic models on the blockchain for the foreseeable future.** Mass adoption have been discussed within the cryptocurrency industry for more than a decade, but the only viable use case for on-chain primitives has mostly been speculative demand — trading, investing or earning yield.

   While expansion of the Mint Cash economy will be achieved through more DApps being built on the platform, more transaction fees/taxes accumulating with more users, and cashflow from fees acting as fiscal policy for even more DApps — initial entry onto the platform should be driven primarily by novel application constructions only available on Mint Cash, including Anchor savings rates, trading opportunities, and forex hedging features.

3. **Perfect capital control cannot be achieved with purely on-chain systems, and any form of direct and indirect capital control implemented on the blockchain must be purely driven by code and economic incentives.** Under traditional macroeconomics models, capital control is usually achieved through law enforcement and military forces that governments can leverage to force its citizens into taking financial positions that normally will not happen under assumptions of a perfectly free market.

   On the blockchain, however, there is no enforcement of action other than passively invoked code that defines a set of conditions on how exactly coins can and should be spent. This means **no one will voluntarily enter a system with economic penalties when potential losses are evident,** if additional economic incentives to do so are not given.

4. **Economic efficiencies achievable with blockchain technology may build an advantage in interest rates without draining net value from the system.** The value-add for a lot of stablecoins is that they can earn additional returns from holding those stablecoins instead of depositing their money with traditional financial institutions; Anchor's 20% yearly returns on TerraUSD stablecoins was the primary growth factor for Terra stablecoins, for example. As illustrated above, however, increased rates against the external, global interest rate parameter inherently results in net capital outflow due to interest arbitrage between multiple currencies, assuming free capital flows. **This will affect a system's ability to maintain value peg of its native currency valued against multiple external currencies.**

   To achieve net economic growth — i.e., a higher GDP value — without significantly increasing transactional demand for domestic currency in the traditional sense will require higher economic incentives for external value to enter the system, which means providing higher yield at least in the short run. **This is an economic dilemma not yet solved by any other on-chain economic system.**

   A potential solution to this is to leverage economic efficiencies of fully automated financial systems built on the blockchain to provide a yield advantage over other systems by increasing **interest utilization efficiency**. While effective deposit interest rates will still reach equilibrium with the global interest rate in the long run, the system can fuel enough transactional demand before that equilibrium is met to be self-sustainable, as we will demonstrate with later sections with this paper.

5. **Fiscal spending and seigniorage is limited by assumption 1, and any debt incurred by the system must either be completely backed by decentralized and trustworthy assets to have sufficient buying power, or explicitly expressed as deficit spending within the protocol**. Deficit spending also should not exceed more than a given percentage of the protocol's entire accounting pool.

Accounting functions should be implemented such that the current state of total assets and liabilities is clearly shown, and the Treasury should be able to take corrective measures, either through automated procedures or governance, once liabilities start exceeding a pre-set value enforced by the protocol.

2. Synthetic Swaps, Liquidity and Collateral Construction

As mentioned earlier, Mint Cash builds on the Terra Core stablecoin system[5] to implement its core monetary stability mechanisms. This section explains how Mint Cash addresses core design issues with Terra's stablecoin system while still retaining some of its promised major benefits.

Unlike Terra, Mint Cash is a fully collateralized digital currency system — **all units of minted currency are backed by Bitcoin**, the world's largest, most scalable, and decentralized digital currency. Also unlike other collateralized stablecoin systems, however, **Mint Cash does not issue currency against loan positions**: **all units of currency are still minted as synthetic swaps.**

A major issue not yet addressed with collateralized stablecoin models is **liquidity construction**. For traditional currencies, central banks perform both liquidity provision and market making on forex markets against their native currency to facilitate trade and value flow to and from its own economy. Central banks also often act as a major forex transaction counterparty, absorbing forex transactional demand to either expand or contract monetary supply.

For assets built on automated smart contracts, however, **such a system simply does not exist yet**. This has often resulted in protocols either providing unsustainable token rewards to maintain market liquidity, or implementing a protocol-owned liquidity mechanism in an attempt to control asset redemption curves against minted currency (e.g., PAMMs).

Mint Cash mimics central bank policy of partially being involved with forex transactions and liquidity provision by implementing ***both*** **automated liquidity management and virtual automated market makers (vAMMs)**. Any user can deposit Bitcoin in exchange for **Mint**, a token equivalent to Luna under the Terra system. Mint can also be burnt and redeemed back to underlying Bitcoins.

As there no initial market liquidity is expected for Mint, **the protocol is required to both construct a market with sufficient trading liquidity** and **determine the exchange ratio between Bitcoins and Mint where Mint is issued and burned at**. For the purposes of implementing the Mint Cash protocol, we assume:

- **more demand** for Mint corresponds to:
  - a higher **exchange rate** between Bitcoin and Mint — i.e., more Bitcoin required per Mint and vice versa
  - more **effective market liquidity** between Bitcoin and Mint

- **less demand** for Mint corresponds to:
  - a lower **exchange rate** between Bitcoin and Mint — i.e., less Bitcoin required per Mint and vice versa
  - less **effective market liquidity** between Bitcoin and Mint

Under these assumptions, we further define the further limitations:

- total liquidity delta between any two given epoch checkpoints defined by the protocol **should not exceed a globally defined** *BaseCollateralLiquidity* **parameter**.
- as the protocol hits the total liquidity delta limit, i.e., the total number of Mint that can be minted or burnt by the system, Mint Cash **proactively applies virtual slippage** such that the effective execution price of Mint swaps is always much lower than the price set by the virtual liquidity maker curve.

We build upon the virtual liquidity maker curve first defined by Pilgrim[7] system and generalize certain trading functions to be suitable for minting synthetic assets.

Formally put:

Lemma III.2.1. Issued Mint when *n* satoshis are accepted as collateral.

$$MintIssued = \text{floor}\left\{\frac{1}{2} \cdot \frac{\log\left(1 + \frac{n + 2 \cdot InitialRounds + RoundUnit}{(InitialRounds + RoundUnit) \cdot InitialBase}\right)}{\log\left(\frac{InitialRounds + RoundUnit}{InitialRounds}\right)}\right\} \cdot RoundUnit$$

where n is a positive integer.

Lemma III.2.2. Burnt Mint when *n* satoshis worth of collateral is being returned.

$$MintBurnt = \text{floor}\left\{\frac{1}{2} \cdot \frac{\log\left(1 + \frac{n + 2 \cdot InitialRounds + RoundUnit}{(InitialRounds + RoundUnit) \cdot InitialBase}\right)}{\log\left(\frac{InitialRounds}{InitialRounds + RoundUnit}\right)}\right\} \cdot RoundUnit$$

where n is a positive integer.

Lemma III.2.3. Required Bitcoin in satoshis when $n \cdot RoundUnit$ Mint is issued.

$$RequiredBitcoinInSatoshis = \frac{(InitialRounds + RoundUnit)^{2n} - InitialRounds^{2n}}{(2 \cdot InitialRounds + RoundUnit) \cdot InitialRounds^{(2n-1)}}$$

where n is a positive integer.

Lemma III.2.4. Bitcoin being returned in satoshis when $n \cdot RoundUnit$ Mint is burnt.

$$RequiredBitcoinInSatoshis = \frac{(InitialRounds + RoundUnit)^{2n} - InitialRounds^{2n}}{(2 \cdot InitialRounds + RoundUnit) \cdot InitialRounds^{(2n-1)}}$$

where n is a positive integer.

The above was an illustration of the Mint virtual liquidity curve without the $BaseCollateralLiquidity$ parameter applied. Under a direct liquidity-to-price correspondence curve as shown from lemmas III.2.1 ~ 4, **a liquidity limitation is equal to a fixed price range applied to the virtual liquidity curve itself**, where price limit points are defined by $BaseCollateralLiquidity$ and $RoundUnit$.

Prior to calculating the number of returned tokens using formulas outlined above, **we first apply the constant-product (CP) price curve to all inputs and outputs with $BaseCollateralLiquidity$ as its liquidity product**, as defined with Uniswap v2[6]:

Definition III.2.1. The constant-product (CP) price curve

$$BaseSatoshis \cdot BaseCollateralInput = BaseCollateralLiquidity$$

Therefore, we use the following formulas with both the constant-product virtual liquidity function and base Mint issuance functions combined:

Theorem III.2.1. Issued Mint when n satoshis are accepted as collateral when $BaseCollateralLiquidity$ is given as the virtual liquidity limit.

From Lemma III.2.1 and Definition III.2.1:

$$MintIssued = \mathrm{floor}\left\{\frac{1}{2} \cdot \frac{\log\left(1 + \frac{\left(BaseCollateralInput - \frac{BaseCollateralLiquidity}{BaseSatoshis + n}\right) + 2 \cdot InitialRounds + RoundUnit}{(InitialRounds + RoundUnit) \cdot InitialBase}\right)}{\log\left(\frac{InitialRounds + RoundUnit}{InitialRounds}\right)}\right\} \cdot RoundUnit$$

Theorem III.2.2. Burnt Mint when n satoshis worth of collateral is being returned and $BaseCollateralLiquidity$ is given as the virtual liquidity limit.

From Lemma III.2.2 and Definition III.2.1:

$$MintBurnt = \mathrm{floor}\left\{\frac{1}{2} \cdot \frac{\log\left(1 + \frac{\left(BaseCollateralInput - \frac{BaseCollateralLiquidity}{BaseSatoshis - n}\right) + 2 \cdot InitialRounds + RoundUnit}{(InitialRounds + RoundUnit) \cdot InitialBase}\right)}{\log\left(\frac{InitialRounds}{InitialRounds + RoundUnit}\right)}\right\} \cdot RoundUnit$$

where *n* is a positive integer.

This system is referred to as the **base collateral pool**. Similar with the existing Terra `x/market` module specification[8], the Mint Cash system will attempt to *replenish* the liquidity gap between *BaseSatoshis* and *BaseCollateralInput* every *CollateralPoolRecoveryPeriod*. Unlike with the *BasePool* and *PoolRecoveryPeriod* parameters used for controlling synthetic stablecoin liquidity under the Terra system, however, Mint Cash collateral liquidity parameters are used for **both liquidity and capital controls**:

- When *BaseSatoshis* is extremely low against *BaseCollateralInput*, close to zero capital may exit the system due to very high virtual slippage until either when the base collateral pool is replenished, or when new collateral capital enters the system. This results in devaluation of Mint against its underlying Bitcoin collateral until there is enough base collateral pool liquidity for arbitrage recovered after the *CollateralPoolRecoveryPeriod*.

- When *BaseCollateralInput* is extremely low against *BaseSatoshis*, close to zero capital may enter the system due to very high virtual slippage until either when the base collateral pool is replenished, or when collateral capital exits the system. This results in overvaluation of Mint against its underlying Bitcoin collateral until there is enough base collateral pool liquidity for arbitrage recovered after the *CollateralPoolRecoveryPeriod*.

Therefore, **Mint acts as an asset buffer** to temporarily cover sudden systematic shocks that may be caused by collateral being deposited and withdrawn. This is similar with Treasury bonds, in the sense that they partially act as shares of a central bank while also partially representing collateral being managed by its currency system.

Mint may be swapped to and from multiple **Cash** currencies, each pegged to different fiat currencies. The flagship Cash currency is **CashSDR**, which aims to mirror the value of the IMF SDR; likewise, multiple variations of Cash currencies pegged to popular currencies may be minted, including **CashUSD**, **CashEUR**, **CashGBP**, and many others.

The relationship between Mint and Cash is similar with those of Luna and Terra stablecoins under the Terra system, with the exception that Mint must be explicitly collateralized while Luna is not. Mint Cash validators vote for the **current market price of Mint** and allows them to be synthetically swapped to and from Cash, under the `x/market` Cosmos SDK module[8].

Note that **Mint may be traded at a completely different value** from prices determined by the Bitcoin to Mint virtual liquidity maker. The value at Cash currency is minted is **based on this public market value**, and not by the initial Bitcoin vAMM. This is because **Mint does not directly represent underlying collateral**; rather, it is a **representation of the system's current state of value flow and accumulated debt**.

The fair market value of Mint is determined by the following factors:

- Value of total Bitcoin collateral locked
- Mint staking rewards
- Capital exit delay and premiums on Protocol-staked Mint
- Mint staking devaluation
- Total value of all Cash currencies minted, denominated in SDR (Special Drawing Rights)
- Moving average of the Anchor rate on all Cash currencies, denominated against the SDR, as a basket of currencies
- Anchor borrow rate and utilization ratio on all Cash currencies, denominated against the SDR
- Capital exit delay & premiums on Anchor-staked Cash currencies, currency utilization factor, and many other miscellaneous parameters
- Outstanding value inflow not arbitraged as new Mint supply with Bitcoin collateral due to the base collateral pool limit
- Outstanding value outflow not arbitraged as burnt Mint supply in exchange for underlying Bitcoin collateral due to the base collateral pool limit

Roughly put:

Conjecture III.2.1. Mint fair market valuation

$$MintFairMarketValue = MintNetValueAdd + CashDebtValue$$

Conjecture III.2.2. Mint net value add with basic Discounted Cash Flows

$$
\begin{aligned}
&MintNetValueAdd \\
&= \left\{ CollateralLocked \cdot \frac{(1 + StakingRewards)^{InterestEpoch}}{(1 + StakingDevaluation - StakingRewards)^{InterestEpoch}} \right\} \\
&\cdot StakingPremium(StakingRatio, UndelegationTime, SlashingRiskFactor) \\
&- \left\{ CashSupplyValue \cdot \frac{(1 + AnchorRate)^{InterestEpoch}}{(1 + LiquidationRisk(UtlilzationRatio) - AnchorRate)^{InterestEpoch}} \right\} \\
&\cdot CashPremium(StakingRatio, LockupTime, CurrencyUtilization) \\
&+ OutstandingValueIn \left(1 - \frac{CashMintedPerRecoveryEpoch}{BaseCollateralLiquidity}\right) \\
&- OutstandingValueOut \left(1 - \frac{CashBurntPerRecoveryEpoch}{BaseCollateralLiquidity}\right)
\end{aligned}
$$

It is assumed that *MintNetValueAdd* ≥ 0, due to capital control measures and incentive parameters that we will explain in depth with the following sections. Otherwise, under exceptional circumstances — including but not limited to sudden and large value loss of Bitcoin collateral, improper swap executions, etc — the system is considered undercollateralized and additional capital control or value inflow measures may be taken to properly contract system debt.

Conjecture III.2.3. Cash debt value with basic Discounted Cash Flows

$$
\begin{aligned}
CashDebtValue = CashSupplyValue &\cdot \frac{(1 + AnchorRate)^{InterestEpoch}}{(1 + LiquidationRisk(UtlilzationRatio) - AnchorRate)^{InterestEpoch}} \\
&\cdot CashPremium(StakingRatio, LockupTime, CurrencyUtilization)
\end{aligned}
$$

Mostly determined by Anchor rates and interest monetary policy, as described with Section III.4. Following assumption III.1.2, this is in contrast with most modern currency regimes where *CurrencyUtilization* is the primary growth factor, while with our model demand is mostly driven by attractive interest rates.

Note that this does not mean *CurrencyUtilization* growth is irrelevant for the Mint Cash system, we are merely relying on attractive rates to drive initial adoption for Cash as a currency.

3. Implementing Capital Controls on a Permissionless System

Most currency models assume capital control as a *necessary evil* for maintaining relative monetary stability, largely enforced by legal frameworks that limit perfectly free value exchange of currency on the open market. Capital controls are also one of the three monetary policy goals required by Mundell-Fleming that cannot be perfectly achieved if all three economic policies were to be at least partially met. **However, since we are implementing the Mint Cash system on a permissionless blockchain, traditional methods of capital control by putting legal limitations on human action cannot be fully enforced**.

This section describes how Mint Cash handles value flow to and from the system to achieve similar desired effects with legally enforced capital controls, similar with legal currencies issued by central banks.

A. Liquidity Control Against Collateral

This was already discussed in depth with Section III.2: *BaseCollateralLiquidity* is an explicit limitation that controls how much collateral may enter or leave the system. This means if total capital outflows exceed a limit set by the constant-product price curve, Mint may only be traded with extremely high trade slippage before *CollateralPoolRecoveryPeriod* passes, which resets the liquidity limitation.

While any exiting capital will result in Mint market devaluation, as described with Conjecture III.2.2 this is accounted as protocol-accumulated debt. **This can be mitigated with III.3.B ~ C.**

B. Mint Native Staking Rewards and Undelegation Limits

As Mint Cash is built on the Cosmos SDK and, therefore, CometBFT (aka Tendermint) consensus, **Mint also acts as a native Proof of Stake token**. This combined with the fact that Mint may only be issued with Bitcoin collateral creates another opportunity for effective capital control.

Because Mint stakers that have delegated Mint to a validator cannot claim corresponding collateral before fully undelegating, **staked Mint is equivalent to Treasury and government bonds under a contemporary currency regime**, in addition to providing economic security for the network. In other words:

- **collateral backing staked Mint can be used to cover temporary protocol downfalls**, similar with an overcollateralized stablecoin model, without explicitly and equally penalizing everyone to take economic risks

- staking Mint implies taking those temporary monetary risks and being subject to potential slashing events, **while being compensated with a constant flow of staking rewards**

- staking rewards are funded with **transaction fees and taxation policies**, as described with Section III.5.

    - a higher tax rate leads to higher staking returns, which contracts supply back to collateral positions

    - a lower tax rate leads to lower staking returns, which burns Mint back to either its underlying collateral or Cash currency positions

Because staked Mint also contributes to monetary stability in addition to network security, **undelegations are subject to both a lockup and vesting period** — instead of returning the entire amount after being subject to a "cooldown" period. This policy prevents mass capital exits that may affect general monetary policy, even with sudden external shock.

C. Controlled Anchor Interest Rates on Cash Currencies

Higher Anchor interest rates may be given to those that choose to lock up their Anchor deposit positions for a predefined period, which is a strategy often employed by both central and commercial banks alike to guarantee borrow liquidity.

From a monetary policy standpoint, providing higher incentives for those that commit to provide liquidity for prolonged periods of time **often means increased aggregate demand for money**, as described with Section I. As Assumption III.1.2 implies there would be no spending to properly calculate GDP in the short term, increased savings rates for bootstrapping investment-savings is critical — we will discuss this in depth with Section III.4.

4. Yield Adjustments as a Stability Mechanism

Mint Cash repurposes Anchor[9], a savings protocol originally built on the Terra blockchain for providing high-yield savings accounts, as a component of monetary stability to adjust demand for Cash currencies.

Following the balance of payments (BP) curve, as defined with Definition I.1.5:

$$\underbrace{BP}_{\text{balance of payments}} = \underbrace{NX}_{=CA,\text{ current account surplus}} + \underbrace{z(i - i^*) + k}_{=KA,\text{ capital account surplus}}$$

Assuming $NX \approx 0$ in accordance with Assumption III.1.2, we are left with

$$BP \approx z(i - i^*) + k$$

Contemporary currency regimes assume that, if $i > i^*$, there would be net inflow of value to that currency system seeking higher interest rates — which means either exchange rates temporarily increase, or the central bank can mint more currency to compensate for that additional demand for value stability. However, in the long run, deposits will eventually match the global interest rate i^* due to continued value inflow. If there is no sufficient demand and investments denominated in that currency, capital will eventually leave the economy to liquidate any gains, resulting in lower exchange rates — if NX (net exports) cannot absorb that additional supply, this currency will continue to lose value.

With NX taken into consideration, a lot of economies choose to keep interest rates lower than the global interest rate — $i < i^*$ — to (i) bootstrap exports by keeping the value of domestic currency low, and (ii) decrease costs of leverage for additional economic investments under the IS curve, which in turn bootstraps GDP. As we are assuming close to zero native demand for currency initially, this quickly becomes a serious problem:

- for new capital to enter and utilize a new currency, there needs to be enough supply of currency to serve as trading liquidity on the markets
- additional supply can only make sense if interest rates are higher than the global interest rate — $i > i^*$ — and this requires increasing costs of leverage
- higher lending rates result in quicker net value outflow as there are close to zero native investments
- any gap in interest is either quickly arbitraged or lowered to compensate for additional deposit supply, and all net value will eventually leave the system

We believe this initial adoption problem can be solved by **loans with higher interest efficiency**: most interest rate models assume that there is significant operational cost and overhead between deposit rates and lending rates required to manage loan profile risk and to maintain large, outdated organizations, like a bank. Smart contract based money markets do not have that overhead as position management is purely done by software. **This means the gap between deposit rates and lending rates can be much lower, which means higher deposit interest can be achieved at similar interest rate levels.**

Let the total value of all Cash currencies locked with Anchor be the following:

Definition III.4.1. Total Cash Value in SDR

$$\begin{aligned} TotalCashValueInSDR &= \{\mathrm{CashUSDDeposits} \cdot \mathrm{SDRtoUSD}, \mathrm{CashEURDeposits} \\ &\cdot \mathrm{SDRtoEUR}, \mathrm{CashCHFDeposits} \cdot \mathrm{SDRtoCHF}, \mathrm{CashSGDDeposits} \\ &\cdot \mathrm{SDRtoSGD}, \mathrm{CashJPYDeposits} \cdot \mathrm{SDRtoJPY}, \cdots\} \end{aligned}$$

Let the deposit interest rate of all Cash currencies on Anchor be the following:

Definition III.4.2. Global Anchor deposit interest rate

$$GlobalAnchorDepositRate = \{i_{\text{CashUSD}}, i_{\text{CashEUR}}, i_{\text{CashCHF}}, i_{\text{CashSGD}}, i_{\text{CashJPY}}, \cdots\}$$

Let the interest delta between Anchor deposit rates and real world interest rates for its corresponding currencies be the following:

Definition III.4.3. Global Anchor deposit interest rate delta

$$InterestRateDelta = \{i_{\text{CashUSD}} - i_{\text{USD}}, i_{\text{CashEUR}} - i_{\text{EUR}}, i_{\text{CashCHF}} - i_{\text{CHF}}, i_{\text{CashSGD}} - i_{\text{SGD}}, i_{\text{CashJPY}} - i_{\text{JPY}}, \cdots\}$$

The goal of Mint Cash monetary policy should be keeping $\Sigma InterestRateDelta$ – EfficiencyRates close to 0 as much as possible, where **EfficiencyRates** is the extra interest rate advantage coming from operational efficiency by operating onchain.

As Anchor under Mint Cash acts as a multi-currency basket of products rather than a single product denominated in the U.S. Dollar, **this acts as a multi-currency hedge — both in terms of value and interest rates, as different currencies have different interest rates**.

A core component of Mint Cash is the ability to borrow one currency using another currency as collateral with very low interest, explained with Section 6. Leveraging this capability, **Anchor on Mint Cash is still built as a single CashUSD deposit market** — with another foreign exchange lending market sitting on top, serving as an adapter between CashUSD and other currencies.

Therefore, effective Anchor interest rates for every currency are defined by the following two parameters:

- the **base Anchor interest rate for CashUSD**
- **borrow interest against CashUSD** with other Cash currencies as collateral

Note that the borrow interest factor is also synthetic, meaning they are levied dynamically by the protocol to adjust native Anchor rates for that currency relative against its corresponding "real world" interest rates. Thus:

- **for Cash currencies that have higher "real world" interest rates** — borrowing Cash with LSTs and native, supported tokens as collateral at staking reward subsidized, extremely low borrow rates with additional reward opportunities on top is **attractive for borrowers in that currency**

- **for Cash currencies that have lower "real world" interest rates** — depositing Cash by borrowing CashUSD on the foreign exchange lending market and depositing as CashUSD is **attractive for depositors in that currency**

With this in mind, users would likely want to *borrow* Cash currencies that have higher "real world" interest rates, and *deposit* Cash currencies that have lower "real world" interest rates, as **yield from liquid staking tokens (LSTs) subsidizes higher borrow interest without adding significant risk profiles to its underlying base token collateral** (i.e. tokens that were originally staked). This means

- the protocol should **increase** lending interest and tax rates for currencies with higher interest rates

- the protocol should **decrease** lending interest and tax rates for currencies with lower interest rates

Formally put —

Definition III.4.4: Interest rates for Cash currencies defined as an endogenous variable of $\boldsymbol{i_{\text{CashUSD}}}$ and $\boldsymbol{i_{\text{UnderlyingCurrency}}}$

$$i_{\text{CashCurrency}} = i_{\text{CashUSD}} + \text{ProtocolLeviedInterest}\left(i_{\text{UnderlyingCurrency}}, i_{\text{USD}}\right)$$

Rewriting Definition III.4.3:

Definition III.4.5: Anchor interest rate delta purely defined against i_{CashUSD}

$$\begin{aligned} &\mathit{InterestRateDelta} \\ &\quad = \{i_{\text{CashUSD}} - i_{\text{USD}}, i_{\text{CashUSD}} + \text{ProtocolLeviedInterest}(i_{\text{EUR}}, i_{\text{USD}}) - i_{\text{EUR}}, i_{\text{CashUSD}} \\ &\quad + \text{ProtocolLeviedInterest}(i_{\text{CHF}}, i_{\text{USD}}) - i_{\text{CHF}}, i_{\text{CashUSD}} + \text{ProtocolLeviedInterest}(i_{\text{SGD}}, i_{\text{USD}}) \\ &\quad - i_{\text{SGD}}, i_{\text{CashUSD}} + \text{ProtocolLeviedInterest}(i_{\text{JPY}}, i_{\text{USD}}) - i_{\text{JPY}}, \cdots\} \end{aligned}$$

$$\begin{aligned} &\Sigma \mathit{InterestRateDelta} \\ &\quad = \text{CurrencyTypes} \cdot i_{\text{CashUSD}} + \Sigma\text{ProtocolLeviedInterest}\left(i_{\text{UnderlyingCurrency}}, i_{\text{USD}}\right) \\ &\quad - \Sigma i_{\text{UnderlyingCurrency}} \end{aligned}$$

Interest rates on CashUSD — i_{CashUSD} — is also determined by the **total utilization ratio of CashUSD deposits on Anchor**, **interest given per LST collateral type**, and **how much CashUSD was borrowed per LST collateral type** (the maximum borrow cap per collateral).

Mint Cash protocol governance will determine base interest rates on CashUSD and corresponding **ProtocolLeviedInterest** values for all supported Cash currencies, while Anchor governance will determine most other factors.

5. Taxation, Treasury Fiscal Policies, and Governance

Taxation is an important factor for monetary policy decisions, as it allows for effective control of spending, market liquidity and Treasury fiscal spending capacity (in terms of interest and other government-driven policies).

Terra Core, of which Mint Cash is based on, had a built-in taxation mechanism where a predefined percentage of Terra stablecoins must be paid as taxes per transaction — with different tax rates per currency. While this is a relatively simple way of implementing taxation, wrapping them as smart contract-based tokens or bridging assets to another blockchain could easily evade this payment-based taxation policy.

Mint Cash adds the concept of **property tax** on top of transaction tax. Transaction tax is also modified to be included with gas payment logic instead of being implemented on a separate layer.

Property tax is levied on accounts that (i) do not have transaction history over a defined period (TaxationPeriod), or (ii) total paid transaction fees and taxes are less than a defined amount denominated in SDR per currency during TaxationPeriod (MinimumFeesPaid). This also applies to smart contract accounts and module accounts, excluding Anchor; Cash currencies deposited with Anchor and derivatives built on top of Anchor deposit positions are exempt from taxation. Accounts that have zero Cash balances are also exempt from any form of taxation.

As taxation here is only levied for currency stability purposes, determining tax rates may be greatly simplified compared to contemporary currency regimes:

- when a Cash currency requires **monetary expansion**, or lower interest rates:
    - **increase** property tax rates for that Cash currency
    - **decrease** transaction tax rates for that Cash currency
    - **increase** costs to borrow that Cash currency against other currencies (which **decreases** effective Anchor interest rates)

- when a Cash currency requires **monetary contraction**, or higher interest rates:
    - **decrease** property tax rates for that Cash currency
    - **increase** transaction tax rates for that Cash currency
    - **decrease** costs to borrow that Cash currency against other currencies (which **increases** effective Anchor interest rates)

Mint staking rewards are primarily affected by taxation as described earlier, which also serves as an important factor for expanding or contracting monetary supply.

Taxes are consisted of a **base tax**, which is a fixed amount denominated in SDR; and **premium tax**, a percentage amount levied on assets being held or transferred. These values may also be determined by protocol governance.

While protocol values and policies for Mint Cash are determined with a governance vote with the native `x/gov` module on the Cosmos SDK, certain monetary levers or parameters require faster decisions than a standard voting process, which may take up to 3 weeks. Governance may delegate decisions over some important monetary policy parameters, such as interest rates, tax rates and borrow rates, to the **Treasury Board**, which is essentially a multisig that requires a separate governance proposal to delegate power. Board members may only exercise their powers for a limited period natively enforced by the Protocol and may be kicked out at any time either through a governance proposal or a Treasury multisig vote.

6. Foreign Exchange Lending Markets

Mint Cash features a **foreign exchange lending market**, where anyone is free to borrow one Cash currency with another Cash currency as collateral. This market component is **purely synthetic**, meaning there is no requirement to provide upfront liquidity, pay actual interest, or perform collateral liquidations.

The Mint Cash forex market defines a **MinimumLiquidity** and **MaximumBorrows** parameter for all Cash currencies. The market component should hold at least **MinimumLiquidity** portion of assets in a particular Cash currency for hedging and liquidity management purposes; borrows for a particular currency also cannot exceed **MaximumBorrows**, denominated in SDR.

As a synthetic forex market, this component has three main functions: **borrow**, **repay**, and **liquidate**.

When a user wants to **borrow** Cash currency, the market internally performs a `MsgSwap` to the destination currency at a user-defined LTV lower than **MaximumCashLTV**, but maintaining sufficient liquidity defined by **MinimumLiquidity**. This position is then recorded to protocol state, which is required for performing liquidations.

When a user wants to **repay**, the exact opposite procedure is executed.

When a loan position exceeds **MaximumCashLTV** defined for each currency pair, **liquidations** may take place. Anyone may query through the list of protocol-held borrow positions and call the liquidation function for that position. Liquidated positions worth of Cash collateral are swapped back to its destination currency minus a **LiquidationsPremium**, which is mostly taken by the user that have called the liquidation function, minus a small fee taken by the protocol.

Both the Treasury Board and protocol governance has the authority to determine parameters listed above, but most importantly **borrow interest rates** for each Cash currency pair. This is important because borrow interest between Cash currencies determine its effective interest rate, as Anchor only natively supports CashUSD deposits. The borrow interest rate may be a positive or negative value determined by a currency's "real world" monetary parameters against the U.S. Dollar.

All fees collected as borrow interest and liquidation premium fees are sent to the **Protocol Treasury**, which determines how much should be burnt, sent out as staking rewards or be reserved. This balance is also managed by the Treasury Board.

7. Putting Everything Together

The goal of the mechanisms described above is to achieve monetary stability by: **(i) creating incentives to dynamically move economic parameters** of a **(ii) programmatically built currency (iii) under a model being actively utilized by modern currency regimes**.

While there have been numerous attempts — and numerous failures — of different stablecoin models, our approach of tightly integrating cash flows, taxation, staking rewards and interest rate stabilization on Cash currencies to maintain monetary stability, while also being completely backed by Bitcoin — the world's most scalable, inflation-resistant asset — is unique in the sense that **monetary policy is completely baked into the platform that developers build decentralized applications on**. DApps built on Mint Cash can build on a purely Bitcoin-backed currency while indirectly contributing back to its stability mechanisms, similar with how real-world economic policies govern fiscal policies over companies contributing back to its economy.

Our belief is that Mint Cash will be the world's first widely adopted use case of Bitcoin by adding **monetary stability**, on top of its existing censorship resistant and inflation resistant properties.

IV. Future Work

The primary focus of this paper so far was on stability through monetary control and savings. As mentioned earlier, however, the two functions of money — **payments** and **savings** — are usually tightly integrated; payments serve a critical role in terms of monetary policy and stability, as they create native cashflow and income, predominantly through transaction fees, to bootstrap the economy and control monetary supply.

Future work would be focusing on expanding our model to include **payments** — i.e., $MX \geq 0$ — that require both the censorship resistant properties of Bitcoin *and* value stability, which would in turn power GDP to be used with our monetary policy calculations. While we will **initially be focusing on growing adoption for Mint Cash predominantly through savings**, integrating the **payments sector of money** to provide an even more **consistent value flow for all ecosystem participants** will be another area of focus that we will continue working on for the foreseeable future.

V. Conclusion

We have presented Mint Cash, a system that achieves currency value stability against various fiat currencies without relying on a centralized banking system purely with synthetic swaps, monetary policy, and Bitcoin collateral.

It should be clear for the reader that one of the missions of this project is to continue building what the Terra project have been trying to build, while avoiding reliance on a purely algorithmic mechanism to maintain peg as an attempt to address the failures the Terra system have faced 18 months ago.

A fully collateralized approach will not be able to reach levels of monetary scalability that Terra was able to achieve with infinitely printed Luna and Anchor yields; however, **we strongly believe that by taking a much more conservative approach** when it comes to controlling purchase power of the Treasury, **Mint Cash will be able to sustain itself as long as Bitcoin stands strong** and continue proving its resilience as the world's first digital native asset.

A decentralized economy still needs decentralized money, regardless of what stands in the way.

References

[1] “Bitcoin: A Peer-to-Peer Electronic Cash System”, Satoshi Nakamoto, 2008. *Paper available on the world wide web*, <“https://bitcoin.org/bitcoin.pdf”>.
[2] “Capital Mobility and Stabilization Policy under Fixed and Flexible Exchange Rates”, R. A. Mundell, 1963. *The Canadian Journal of Economics and Political Science*, Vol. 29, No. 4., pp. 475-485. doi:10.2307/139336.
[3] “"Domestic financial policies under fixed and floating exchange rates", J. M. Fleming, 1962. *International Monetary Fund (IMF) Staff Papers*, Vol. 9, No. 3., pp. 369-380. doi:10.2307/3866091.
[4] "Mr. Keynes and the 'Classics': A Suggested Interpretation", J. R. Hicks, 1932. *Econometrica*, Vol. 5, No. 2., pp. 147-159. doi:10.2307/1907242.
[5] “Terra Money: Stability and Adoption”, E. Kereiakes, D. Kwon, *et al*., 2018. *Paper archived on GitHub*, <“https://github.com/terra-money/documentation/blob/master/white-paper/terra-v1.1.pdf”>.
[6] “Uniswap v2 Core”, H. Adams, N. Zinsmeister, *et al*. 2020. *Paper available on the world wide web*, <“https://uniswap.org/whitepaper.pdf”>.
[7] “Pilgrim: An Atomic Valuation Framework for Low Liquidity Assets”, D. Hong, T. Park, *et al*. 2021. *Paper available on the world wide web*, <“https://pilgrim.money/papers/pilgrim-paper”>.
[8] “Terra Core Market Concepts”, D, Kwon, *et al.*, 2020. *Archived on GitHub*, <“https://github.com/terra-money/classic-core/blob/main/x/market/spec/01_concepts.md”>.
[9] “Anchor: Gold Standard for Passive Income on the Blockchain”, N. Platias, *et al*., 2020. *Paper available on the world wide web*, <“https://www.anchorprotocol.com/docs/anchor-v1.1.pdf”>.