ShiftCTRL: A Decentralised Stablecoin Protocol anchored to Bitcoin, and guided by Austrian economic sound money principles

Rich Saunder
rich.saunder@gmx.com
www.shiftctrl.money

Abstract. Money stands fractured, a system tainted by the manipulation of central banks, governments, and commercial banks. The absolute authority wielded by these entities in the creation of currency perpetuates an unjust advantage for the privileged, thereby exacerbating income and wealth inequality and hindering upward social mobility.

In response to this broken monetary landscape, Bitcoin emerged as a beacon of change, introducing blockchain technology and embodying virtuous ideals such as decentralization, permissionless-ness, censorship resistance, and financial sovereignty. As the trailblazing pioneer, Bitcoin has successfully laid the groundwork for newer, more efficient, and scalable blockchain technologies prevalent today, unfortunately, this in turn has highlighted some limitations that it faces as a new form of money.

The advent of stablecoins in 2014 aimed to address the issue of price volatility that impeded the widespread adoption of cryptocurrencies in real-world applications. Tether (USDT), the largest stablecoin, has surpassed the combined transaction volume of Bitcoin and all non-stablecoin cryptocurrencies. As the adoption of stablecoins grows, it is frequently overlooked that the majority of stablecoin protocols operate in a centralized manner whilst relying on fiat currencies or government securities as reserves. Essentially, these stablecoins are just crypto forms of fiat currencies or government-issued money.

The rise of Central Bank Digital Currencies (CBDCs) further blurs the line between crypto and traditional finance. Will the crypto community adopt these CBDCs just like the have with centralised, fiat-backed stablecoins? Which begs the question: Why the move to crypto? Why not just stick with traditional finance?

Our objective is to realign the trajectory by constructing a monetary system anchored to Bitcoin, firmly rooted in its ethos, and guided by the sound money principles advocated by Austrian economics. Modelled after the classical gold standard (1870s - 1914), our system has addressed the shortcomings of the original model by making a few significant enhancements:

- Gold is replaced by Bitcoin.
- paper money gives way to stablecoins.
- Central bank mandates are supplanted by community governance (decentralized governance).
- Centralized settlement yields to blockchain settlement.

Illustrating the classical gold standard's operation, governments were required to possess gold reserves to authorize the printing of money, typically adhering to a common cover ratio of 40%. This meant that for every 100 dollars printed, central banks were obligated to hold 40 dollars' worth of gold reserves. The redeemability of printed currency in gold placed a constraint on the quantity of money central banks could circulate.

ShiftCTRL adopts a similar mechanism, allowing users to mint stablecoins, termed Tabs, pegged to any of the 155 national currencies globally, by depositing reserves in the form of Bitcoin. Reserves must meet the minimum reserve ratio of 180%. Falling below this threshold results in penalties and breaching the liquidation ratio of 120% triggers automated auctions to liquidate reserves. The main piece to our model lies in its decentralisation, with all parameters configurable through decentralized governance.

In a world where traditional finance and crypto converge, ShiftCTRL strives to create a monetary paradigm centred around Bitcoin that is rooted in transparency, decentralization, and economic fairness.

1. Introduction

Money. Is. Broken.

Why? Well, the short answer is that money as we know it in the 21st century, is just debt created by central banks alongside world governments, and it is imposed upon the world via a fiat currency system that we did not exclusively choose. Then again, that’s what ‘fiat’ is – from the Latin word that means “let it be done”. In other words, an order or decree.

The contemporary global monetary system took its current form when President Richard Nixon of the United States reneged on the nation's commitment, terminating the convertibility of the Dollar to gold in 1971. This historic event, known as the Nixon Shock, marked the conclusive demise of the once-prosperous Gold Standard.

In just one broadcast, he single-handedly removed the last remnants of any restriction on the Federal Reserve's (Fed) ability to create money out of thin air. Since that fateful day, there has been a deluge of this mysterious money magically floating throughout the world economy.

What’s worse is that we – the true owners and risk-bearers of this medium of exchange, have virtually no say in money’s creation, circulation, and valuation.

While Nixon’s advisors cited neoclassical and mainstream economic concepts behind the 1971 decision, they completely ignored the philosophical economic principles of maverick Austrian economists such as Carl Menger, Eugen von Böhm-Bawerk, Ludwig von Mises and F.A. Hayek who came before them.

Since the 19th century, these great thinkers had spent their lives advocating for a free market in money, and as an extension, in the economy. Through scores of diligent research, literature, and debate, they theorized that individuals should be free to use any commodity they choose as a medium of exchange, which was precisely the case with precious metals, especially gold for centuries.

These Austrian economists concretely argued that the value of money should always be determined by natural market forces rather than government policy.

In hindsight, the brokenness of money was already apparent prior to the Nixon Shock. Five decades earlier, The Great Depression also laid bare the structural defects that arise from unsound monetary policies via interventionism.

While the causes of the calamity are complex and multifaceted, many from the Austrian school of economics saw it coming a mile away. With the Wall Street Crash of 1929, the so-called secured banking system experienced widespread bank runs of epic proportions. Panicked depositors rushed to withdraw their savings, causing further bank failures and a contraction of credit. To Austrians, it was a mere case of I-told-you-so.

The Fed’s tightening of monetary policy by raising interest rates and reducing the money supply only compounded the nosediving economy and led to a drastic decrease in investment and consumption.

In fact, it was Austrian economist F.A. Hayek who famously quipped that the Great Depression was more a failure of government rather than the market. He cited that the deliberate lengthening of the boom and slow adjustment process created the epic chaos that had rippling effects around the developed world.

Unfortunately, their sound theories fell on deaf ears and, today, we see the rotten fruits of this nightmare in full effect on a global level – low purchasing power, insurmountable debt, huge wealth and income inequality, staggering poverty levels… The list is both long and damning. But how did we get here?

You see, Austrian economics has always seen inflation as a form of invisible tax. As new money is introduced into the economy, each unit of currency becomes less valuable. This decrease in the purchasing power of money essentially functions as a tax on holders of currency because they can buy fewer goods and services with the same amount of money. Notably, those who benefit from this inconspicuous tax are the issuers of the new money, along with privileged segments of the population granted early access to it.

And as we’ve seen world over, this leads to injudicious government spending (larger deficit spending) while unfairly giving governments more power over its citizenry.

The reality, however, is that without the ability to print this magical money into existence, governments are solely dependent on taxation or surplus revenue from good governance of its coffers. This is why it is up to us all to hold governments to the same standards as individuals, if not higher.

The unchecked expansion of the money supply systematically distorts interest rates, a critical market signal, thereby making economic calculations totally unreliable. This distortion lies at the heart of global malinvestments, which have led to many economic recessions and crises. Additionally, the manipulation or artificial depression of interest rates by central planners ultimately favours debtors at the expense of creditors, concurrently discouraging prudence and future planning. Instead, it fosters a proclivity for instant gratification over saving and investing, a contorted process that only contributes to spiralling household debt.

Funnily enough, it was 1972's Marshmallow Experiment by Stanford University's professor and psychologist Walter Mischel, that conclusively showed the power of delayed gratification, in that individuals with the ability to delay gratification were naturally successful in life. This was already a foundational concept behind the Time Preference Theory of Interest, a core tenet of Austrian economics.

Not to mention, in a system where the expansion of money supply is dictated by central planning, it is almost laughable that this newly "minted" money is used to bail out private companies at the expense of taxpayers; it's like gambling with no risk. And where there is no risk, there is no true reward, something that was put on full display for all to see and suffer during the 2008 global financial crisis.

That being said, these glaring truths only point to one thing – this flawed financial ecosystem will continue wreaking havoc unless there's a major shift in how we understand and define sound money and take back control.

The good thing, however, is if you're reading this, it means you recognize this systemic, paralyzing flaw in our current fiat monetary system, and like us, you want to do something about it.

The way forward couldn't have been articulated better than F.A. Hayek himself: "I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take it violently out of the hands of government, all we can do is by some sly roundabout way introduce something that they can't stop."

This revolutionary workaround that was predicted by Hayek in 1984, came to full fruition in January 2009 when the pseudonymous Satoshi Nakamoto launched Bitcoin, the decentralized cryptocurrency that apprehends all the issues inherent in the crippled fiat monetary system head on.

In Bitcoin's publicly released whitepaper, Nakamoto also underlined the Austrian perspective to fiat currency: "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve."

This is why we believe that Bitcoin is an opportunity to correct an archaic system that has surely run its ruined course.

Where monetary inflation causes reckless volatility and catastrophe, Bitcoin's fixed supply of 21 million coins ensures significantly increased stability via its capability to maintain its value over time. The current inefficiency of our deformed financial system is also solved by Bitcoin, in that it allows for permission-less transactions without the reliance on centralised third parties, making it accessible to people all over the world.

And perhaps, its single most important attribute, is that Bitcoin is decentralized, and thereby shielded from interventionism and the corruption that shadows it.

Thanks to blockchain technology, no single entity has control over the network. Transactions are verified by a network of users, making it more secure and transparent than traditional financial systems. This removes the most problematic element of our current financial system – unsound monetary policies. If anything, history shows us that central planning via governments and central banks lead to a distorted version of reality.

The time has come to stop pointing fingers and being keyboard warriors, and to take full accountability for the situation at hand.

Empowered by numerous lessons of the past and with Bitcoin's unrivalled potential as the new gold of the digital era, it is up to us who believe in the ethos behind the creation of Bitcoin to arrest this imminent crash landing.

Backed by the profound philosophical approach of the Austrian school of economics – that is rooted in individual rights, free market and sound money principles, we believe that ShiftCTRL is the giant trampoline at the bottom of the pitfall, a scalable solution that can propel humanity back on its feet to reclaim its lost financial sovereignty for all in a true sense.

In other words, the best time to fix what is broken is now.

2. The Tab Protocol

Overview

The Tab Protocol is a decentralized stablecoin protocol built on Arbitrum (https://arbitrum.io/), an Ethereum Layer-2 scaling solution, that allows users to mint fiat-pegged stablecoins called 'Tabs', by depositing Bitcoin as reserves. Users may redeem their Bitcoin reserves at any time by burning Tabs corresponding to the amount that was minted using those reserves.

The design behind Tab Protocol is rooted in the sound monetary principles that underpinned the thriving Classical Gold Standard of the 1870s. This system rose to prominence as the dominant international monetary system in the late 19th and early 20th centuries, with many countries adhering to it.

However, this fluid monetary system was disrupted by the breakout of WW1 in 1914 and only some efforts were sporadically made to return to it during the interwar period. Of course, none survived past the Great Depression of the 1930s.

As part of the system's overarching parameters, a participating nation's currency was defined as a unit of weight of gold, and the paper currency issued by any government, or its central bank was redeemable in the defined weight of gold.

Within the context of the gold-backed system, gold was referred to as the '**money proper**', with paper currencies and token coins functioning as '**money substitutes**'. To this aim, money substitutes, oftentimes issued by central banks under the purview of governments, proved very useful as they enhanced the portability of money (gold) substantially.

A crucial element behind the stability of money during the Classical Gold Standard was down to the self-correcting nature of the monetary system. The fact that money substitutes could be converted into gold on demand, meant that there was a strict limit to how much money substitutes can be issued thereby ensuring some form of prolonged economic stability.

While paper banknotes had already been in use since the 7th century, under the Classical Gold Standard, banknotes grew in popularity because they not only reduced the risk of theft, but banknotes also reduced the cost of transportation, thus making it a more saleable form of money substitute. Likewise, token coins facilitated exchanges in smaller denominations.

However, the centralized control of the Gold Standard system, marked chiefly by government policies and unsound central bank strategies, ultimately led to its cessation.

This is why we believe that Tab Protocol's strongest feature is that it is decentralized, allowing its integrity to be collectively secured by its community of users. The Tab Protocol is governed and managed by the community who holds its governance token, CTRL, by voting on key parameters that stipulate how the protocol operates.

With this main decentralized feature in place, we are certain that the Tab Protocol will establish Bitcoin as a highly saleable money proper, and Tabs as stable money substitutes, that facilitate cheap, fast, immutable and permissionless transactions with relatively low-price volatility.

Tab Currencies (Tabs) - Fiat-pegged Stablecoins

Tabs are sound, sovereign, Bitcoin-backed stablecoins which are soft-pegged to national currencies around the world. At its inception, there will be 156 different national currencies available from the protocol, i.e., sound USD (ⓈUSD), sound GBP (ⓈGBP), sound ARS (ⓈARS), etc.

Users mint Tabs by depositing Bitcoin as reserves into Vaults (discussed below) within the protocol. This is primarily how Tabs enter into circulation, and how users can access liquidity. Users can also obtain Tabs through secondary means like buying it from on-ramps, brokers or exchanges, or by receiving it as a form of payment.

3. Reserves

Bitcoin, and only Bitcoin

From an Austrian Economics perspective, a healthy and stable economy hinges on the existence of 'sound money'. In a nutshell, sound money refers to money that is durable, scarce, divisible, portable, and fungible. These qualities ensure a money's value remains relatively stable over time, solidifying its position as a reliable medium of exchange and store of value.

Gold has stood the test of time as the most widely embraced and resilient form of sound money throughout human history, boasting an unparalleled track record as a store of value. However, we contend that Bitcoin possesses distinct qualities that position it as arguably the most advanced form of money.

Distinguished by its unparalleled scarcity, capped at 21 million units, Bitcoin surpasses gold in this aspect. Unlike gold, it is not susceptible to supply shocks resulting from the discovery of new deposits. Its ironclad monetary policy is enshrined in the Bitcoin code and is impervious to alterations without the explicit consent of the network. Furthermore, Bitcoin proves itself hardier than gold, exhibiting unparalleled resistance to inflation, with its current rate at 1.8% and projected to decrease to 0.9% by mid-2024, continuing to diminish until it reaches zero.

Beyond scarcity and resilience, Bitcoin excels in divisibility, eliminating the need for token coins to facilitate smaller denominations. Its superior portability enables effortless storage and movement, allowing Bitcoin to traverse the globe with ease. Moreover, Bitcoin's fungibility is unparalleled, as its purity and quantity remain unquestioned, negating the necessity for third parties in issuance or authentication.

A distinctive feature of Bitcoin is its immunity to manipulation, setting it apart in the financial landscape. The decentralized nature of Bitcoin ensures independence from centralized third parties, significantly lowering the risks of surveillance and coercion. Bitcoin cannot be censored or confiscated, establishing it as an unassailable asset.

The decentralized architecture of Bitcoin, coupled with its battle-tested nature, positions it as the most reliable blockchain. Boasting robust security and decentralization, Bitcoin maintains the highest number of nodes compared to other blockchains. Its consistent uptime and resistance to deep reorganizations underscore Bitcoin's remarkable track record.

In light of these factors, Bitcoin emerges as the perfect form of money proper, facilitating the role of monetary reserves that embodies both soundness and sovereignty in the realm of currency.

No Multiple Reserves

The whole overarching theme behind ShiftCTRL and thereby the Tab Protocol, is to establish a new and sound monetary system that is unburdened by the pitfalls of past monetary policies, notably bimetallism.

Bimetallism emerged during the late medieval period in Europe and one of the earliest examples of bimetallism was the use of both gold and silver as money in the Byzantine Empire during the 6th century. By the 19th century, bimetallism was well adopted by several countries, including the United States, France, and Germany; the United States, for example, adopted a bimetallic standard in 1792.

During the periods of bimetallism, the government accepted both gold and silver as a money by establishing a fixed ratio between the two metals. While it seemed a great idea at the time for reasons of divisibility and transportability, bimetallism proved to be unsustainable in the long run and ultimately failed.

One of the most well-known examples of the failure of bimetallism occurred during the 1870s and 1880s, when a flood of silver from new mines in the United States (and other countries) caused the value of silver to drop significantly.

This led to a situation where people were hoarding gold and spending silver, which caused gold to become scarce while silver flooded the market. The result was a series of financial crises and economic instability in countries that were using a bimetallic standard. In the United States, the ensuing Coinage Act of 1873 ultimately demonetized silver and effectively ended the bimetallic standard in the United States.

The failure of bimetallism is best explained by Gresham's Law which can be summarised simply as 'bad money drives out good'. That is, when the actual market values of gold and silver deviated from the legal ratio, people naturally hoarded the undervalued metal and tried to spend the overvalued metal.

Drawing parallels within the context of ShiftCTRL, envision the Tab Protocol accepting both Bitcoin and Ethereum as reserves, locked into a fixed ratio at the point of Ctrl+Alt+Delete (elaborated further below) based on their market prices, set at 60,000 ⓢUSD:3,000 ⓢUSD (20:1). Likewise, this can be construed as 1 ⓢUSD equating to 0.00001667 BTC or 0.00033333 ETH.

However, as observed in the bimetallism debacle, if the price of Bitcoin ascends to 70,000 ⓢUSD while Ethereum remains constant, users naturally gravitate towards redeeming ⓢUSD in Bitcoin and minting ⓢUSD with Ethereum. This dynamic depletes the Bitcoin reserves, subsequently replaced entirely by Ethereum.

The crucial lesson derived from the pitfalls of bimetallic legislation underscores the unsustainability of accepting two or more reserves. Aligned with ShiftCTRL's objectives, the Tab Protocol will only opt for a singular reserve, exclusively utilising Bitcoin.

What about Other Reserves?

The prevailing trend among stablecoins, including widely adopted ones like Tether, USDC, and BUSD, predominantly relies on fiat currencies, US treasuries, or other government securities as reserves. This essentially makes them fiat money in the form of cryptocurrency.

Regrettably, this reserve model fails to address the underlying challenge of money supply inflation; instead, it exacerbates the debasement of the currency. The fiat reserves that are held in the bank accounts of stablecoin operators continue to inflate the money supply through fractional or "zero" reserve banking. Compounding this issue, the money supply is inflated in the form of cryptocurrency as stablecoins.

This runs counter to the objective of ShiftCTRL and as such, Tab Protocol will not accept fiat or other government securities as reserves, both at its inception and in the foreseeable future.

Wrapped/Bridged Bitcoin

As the Tab Protocol is built on the Arbitrum network, it will utilise wrapped/bridged ERC-20 representation of BTC as reserves. The protocol is designed to accept multiple representations of BTC as that will help to mitigate potential threats, including malicious attacks and system malfunctions, to the Bitcoin wrapping operators or cross-chain bridges. The community, empowered through governance, holds the collective authority to determine which wrapped or bridged BTC variants are admitted to or removed from the protocol.

During its inception, WBTC (https://wbtc.network/) will be accepted as the ERC-20 tokenized representation of BTC. While WBTC has had a good track record and is currently the most widely used ERC-20 representation of BTC, the centralised nature of its operations where custodians are entrusted with the integrity of the system makes it less than ideal. Unfortunately, there isn't many better alternatives available at present and to that end, **ShiftCTRL will prioritise the enhancement of the protocol to accept native BTC as reserves directly on the bitcoin network in phase 2 of its development.**

4. Treasury

All Tabs pegged to 155 different national currencies can be minted by depositing Bitcoin reserves into vaults in the Tab Protocol via smart contracts that are called ‘Treasury’. Users can access the Treasury through QWERTY, ShiftCTRL’s native treasury application interface.

Minting Tabs

Step 1 : Create a Vault

Bitcoin reserves that are required for the minting of Tabs will be deposited in Vaults. Vaults are inherently non-custodial, and users will be able to interact with the Vaults and Treasury directly. Each user has complete and independent control over their reserves as long as their reserves does not fall below the liquidation ratio (discussed further below). Users will have to create a different Vault for each Tab currency they wish to mint. Multiple vaults can be created to mint the same Tab currency.

Step 2 : Deposit Reserves

Once a Vault is created, the Vault owner can specify the amount of reserves they wish to deposit.

Step 3 : Mint Tabs

Once reserves are deposited in the Vaults, a Vault owner can mint Tabs up to the Minimum Reserve Ratio (MRR). The MRR is the minimum reserve-to-Tab ratio of a vault. For example, for a Vault minting sound United States Dollar (ⓈUSD) and has 2 Bitcoins as reserves, if the price of Bitcoin is 60,000 ⓈUSD and MRR is 180%, the Treasury will allow the Vault to mint up to a maximum of 66,666.66 ⓈUSD (i.e., 2*60,000/1.8).

Withdrawing Reserves

As Vaults are inherently non-custodial, a Vault owner may withdraw reserves partially or completely, on demand, by burning the corresponding amount of Tabs, as long as reserve requirements are met. A vault remains open even if all reserves are withdrawn and is available for future deposits.

5. Managing the Treasury

Minimum Reserve Ratio (MRR)

The MRR acts as a buffer that allows the Tab protocol to absorb volatility and shocks to the value of the Bitcoin reserves anchoring the system. The Vault owner is responsible for always keeping the reserve ratio above this minimum.

Risk Penalty

Should the value of reserves in a vault fall (fall in Bitcoin prices) below the MRR, the vault will incur a *Risk Penalty*. The penalty amount is calculated by multiplying the amount required to meet the MRR (delta) with the penalty rate. The risk penalty is accrued every *penalty step duration*. Both the *Risk penalty* and *Penalty step duration* are governable parameters.

Imagine a hypothetical scenario where the price of Bitcoin drops from 60,000 ⓈUSD to 50,000 ⓈUSD and remains there. If the MRR is 180% and the *Risk Penalty* is 1.5% and the *Penalty step duration* is 24 hours, a ⓈUSD vault with 2 Bitcoin in reserves and 60,000 ⓈUSD minted will incur risk penalties as shown below:

Step duration	Outstanding Tabs (Minted Tabs + risk penalty)	Minimum Reserve Requirement	Delta	Risk Penalty
1	60,000.00	108,000.00	8,000.00	120.00
2	60,120.00	108,216.00	8,216.00	123.24
3	60,243.24	108,437.83	8,437.83	126.57
4	60,369.81	108,665.65	8,665.65	129.98
…	…	…	…	…

Users are strongly encouraged to maintain a comfortable buffer above the Minimum Reserve Ratio (MRR) to mitigate the risk of incurring a Risk Penalty. In the event that a Vault's Reserve Ratio falls below the MRR, the Vault owner has the option to rectify this by either depositing additional reserves or burning Tabs.

The primary objective of the Risk Penalty is to promote risk aversion and uphold the protocol's stability. Simultaneously, it seeks to avoid imposing an unwarranted financial burden on the Vault owner through excessively severe measures. This balanced and measured approach is envisioned to optimize the utilization of reserves, fostering a more efficient ecosystem.

To conduct various Vault operations, such as burning or minting Tabs, withdrawing Reserves, or creating a new Vault, it is necessary to settle the Risk Penalty first. When there is an outstanding penalty, any newly minted Tabs following additional reserve deposits will automatically have the penalty deducted. These collected Risk Penalties contribute to the Contingency Fund, an emergency reserve designed to mitigate risks that could destabilize the protocol, such as mismanaged Vaults. This mechanism reinforces the protocol's resilience and preparedness for unforeseen circumstances.

Liquidation Ratio
A Vault’s reserves will be subject to liquidation if its Reserve Ratio falls below the Liquidation Ratio. This is to ensure that there are always sufficient reserves to back all circulating Tabs. Liquidations are carried out through automated Tab Protocol Auctions.

6. Liquidation Auction

When a Vault is liquidated, its reserves are automatically put up for sale using a variant of the Dutch auction. Commencing at a higher price point, the auction progressively lowers the price until adequate reserves are sold to cover all Outstanding Tabs (consisting of minted Tabs and Risk Penalties) or until the price reaches its minimum threshold. Although the auction is open to all, submitted bids must be in the same Tab currency as the vault undergoing liquidation.

The auction's initial price is determined by discounting the market price of the reserve, using the *Auction start discount*. If the total liquidated reserves fail to cover the Outstanding Tabs, the reserve price undergoes further reduction through the *Auction step discount* after each *Auction step duration*. However, this reduction is capped at the Minimum Liquidation Price (MLP), representing the lowest price that allows the Liquidation Auction to cover all Outstanding Tabs for the specific vault.

For instance, if a vault possesses 2 Bitcoin in reserves, has minted 60,000 ⓢUSD, and incurred risk penalties of 2,000 ⓢUSD, the MLP is calculated as 31,000 ⓢUSD per Bitcoin (i.e., [60,000 + 2,000] / 2).

When the auction price has reached the MLP, the auction will remain active until the liquidation of all reserves held in the vault. In instances where participation in an auction is suboptimal, the community retains the option to propose, through governance, the utilization of the contingency fund to actively participate in the auction.

The following example illustrates how an auction is executed:

Reserves	: 2 Bitcoin
Reserve market price	: 60,000 ⓢUSD
Minted amount	: 60,000 ⓢUSD
Risk penalties	: 2,000 ⓢUSD
Outstanding tabs	: 62,000 ⓢUSD
Auction start discount	: 10%
Auction step discount	: 3%
Auction step duration	: 60 seconds

Step	Block	Auction price (ⓢUSD)	Reserves for sale (BTC)	Total bids (BTC)	Total bid value (ⓢUSD)
1	1	54,000.00	1.148148	0.200000	10,800.00
	2	54,000.00	0.948148	0.200000	10,800.00
2	3	52,380.00	0.771287	0.200000	10,476.00
	4	52,380.00	0.571287	0.200000	10,476.00
3	5	50,808.60	0.382770	0.200000	10,161.72
	6	50,808.60	0.182770	0.100000	5,080.86
4	7	49,284.34	0.085330	0.085330	4,205.42
				1.185330	**62,000.00**

Based on the auction's opening price of 54,000 ⓢUSD, only 1.148148 of the 2 reserves were initially put up for auction as that was all that was required to settle the vault's Outstanding Tabs. Because the reserves put up for auction were not completely sold in the first step, the auction price is reduced to 52,380 ⓢUSD. At this lowered auction price, 0.771287 reserves are put up for sale. This process continues until enough reserves are liquidated to offset the Outstanding Tabs of 62,000 ⓢUSD.

The culmination of the auction saw a total of 1.185330 reserves, equivalent to 62,000 ⓢUSD, liquidated to cover the entirety of Outstanding Tabs. From the proceeds of the auction, 2,000 ⓢUSD, representing risk penalties, were allocated to the contingency fund, while the remaining 60,000 ⓢUSD were burnt to offset all Tabs minted by the vault. The residual 0.814670 reserves remain in the Vault and is available for withdrawal by the Vault owner.

7. Ctrl+Alt+Del (Currency de-peg)

While the protocol's design to peg to fiat currencies give Tab currencies price stability relative to the mainstream economy, inadvertently, Tabs will also inherit the inflationary effects of the pegged fiat currencies.

For example, if the USD loses purchasing power as prices soar due to the expansion of the money supply, the purchasing power of ⓢUSD suffers the same fate. Over the long run, the value of Bitcoin reserves should hedge against such a loss (users can mint more Tabs as the value of Bitcoin rises against a depreciating fiat), but this would only apply to a subset of ShiftCTRL users who minted their own Tabs (we envision that part of the community would transact and access Tabs using other means).

For this reason, the pegs to each respective fiat currency only serves as a temporary solution for Tabs to promote adoption during its nascent stage. The end game, once a specific Tab has gained enough network effects, is to de-peg from its fiat currency and along with it, the inflation effects.

The process of de-pegging is referred to as Ctrl+Alt+Del. It is worth noting that, this process cannot be initiated on a Tab currency that belongs to a Vault that is undergoing a Liquidation Auction.

When Ctrl+Alt+Del is initiated on a Tab currency alongside successful approval granted through Governance (discussed below), the de-pegging Bitcoin price will underpin the value at which the Tab is anchored to, and as such, will then be defined as an amount of Bitcoin.

For example, if de-pegging price of 1 Bitcoin is 60,000 ⓢUSD, this will mean that 1 ⓢUSD will be defined as 0.00001667 BTC. Therefore, the amount of Bitcoin required as reserves for the Outstanding Tabs for each Vault is then determined based on this defined ratio.

These reserves will be consolidated under a "single" protocol Vault and amounts arising from risk penalties will be minted by the protocol vault and transferred to the contingency fund. All individual Vaults will remain open until its excess reserves are claimed by their respective Vault owners.

Subsequently, minting and burning of Tabs can no longer be performed on individual vaults but is done on the Protocol Vault instead, based on the defined ratio. The Minimum Reserve and Liquidation Ratios will no longer be applicable to the Tab currency that has been de-pegged.

From a practical perspective, this means that for every 1 ⓢUSD, the Protocol will hold in reserve 0.00001667 BTC that is readily redeemable on demand.

To illustrate the process, let's assume that the de-pegging price is 60,000 ⓢUSD; and there are 3 individual vaults, namely vault A, vault B and vault C.

Vaults	**A**	**B**	**C**	**Protocol**
Before Ctrl+Alt+Del				
Reserves Available (BTC)	2.0000	3.0000	10.0000	
Minted Tabs (ⓢUSD)	100,000	120,000	500,000	
Risk Penalty (ⓢUSD)	3,000	1,500	-	
Outstanding Tabs (ⓢUSD)	103,000	121,500	500,000	
Reserves to be consolidated (BTC)	1.7167	2.0250	8.3333	
Post Ctrl+Alt+Del				
Excess Reserves (BTC)	0.2833	0.9750	1.6667	
Tabs in Circulation				720,000
Tabs for Contingency Fund				4,500
Minted Tabs				724,500
Consolidated Reserves (BTC)				12.0750

The Ctrl+Alt+Del currency de-peg is designed on the sound money principles that were utilised during the Classical Gold Standard. Under the standard, national currencies were defined as a weight of gold and were redeemable in gold: the Great Britain pound was defined as £4.25 per ounce of gold (£1 = 0.2352 ounce of gold), while the American Dollar was defined as $20.67 per ounce of gold ($1 = 0.0484 ounce of gold), etc.

Essentially, the "Dollar',” Pound", "Franc" etc were basically different definitions of weight in gold, similar to how "Yard", "Meter", "Inch" are different definitions of length. This meant that the "exchange rates" were simply proportional gold weights of the various currency units and did not fluctuate like current day foreign exchange rates. Crucially however, this system helped foster a healthy rate of international free trade between nations for many years by reducing exchange rate volatility, increasing transparency in currency valuations, boosting confidence in currencies, and minimizing transaction costs.

8. Price Oracles

The seamless operation of the Tab Protocol relies on real-time market price information to operate its various mechanisms to ensure the Protocol's stability. To obtain this critical data, the Protocol utilizes a decentralized oracle feed structure consisting of nodes, which may be either individuals or organizations approved (whitelisted) by the community through Governance. In recognition of their vital role, nodes receive rewards in the form of CTRL tokens.

To qualify for the reward, each node will need to submit price feeds at regular 5-minute intervals. The Protocol systematically arranges these feeds in incremental order, determining the median as the definitive system price. This approach eliminates outliers that may originate from malicious intent or inaccuracies. Prices are updated either every *Oracle step duration* (1 hour) or when prices deviate by more than the *Oracle movement delta*, set at 0.5% from the established system price.

To ensure the reliability of price updates for each Tab currency, a *Minimum feed count* of 3 submissions is required. In the event that the number of feeds drops below this minimum threshold for more than the *Maximum miss count* of 3, indicating three consecutive intervals with fewer than 3 active nodes submitting price feed, the respective Tab currency will be frozen. This action results in the suspension of all vault operations, including the minting of new Tabs and the burning of Tabs. The frozen Tab currency is automatically unfrozen as soon as the Tab currency receives the minimum required number of price feeds for more than the *Maximum miss count*, reinstating the vault functionalities of the affected Tabs. This precautionary measure aims to ensure the accuracy and integrity of the price data crucial to the Tab Protocol's operations.

In the process of minting Tab currencies pegged to various fiat currencies, the Protocol necessitates the price of Bitcoin in each corresponding fiat currency. Given that these specific prices are not easily available, the Protocol adeptly derives them by utilizing the median exchange rate of these currencies against rate of ⓈUSD.

9. Governance

As articulated throughout this whitepaper, ShiftCTRL is a decentralised public protocol governed by community members. Governance is a democratic process that allows community members to submit, vote and implement proposals. The CTRL token is the governance token of ShiftCTRL, and each token represents voting rights that decide the outcomes on proposed changes.

Vote Delegation
The ShiftCTRL Governance works via delegation of votes. Holders of CTRL tokens can either self-delegate or entrust their voting power to other delegates.

Ensuring sound governance necessitates a commitment to invest effort and resources in staying well-informed and knowledgeable about the array of ideas being proposed. These concepts often span various fields of expertise such as statistics, economics, information technology, among others, presenting a potential challenge for the average community member to comprehensively grasp.

In light of this challenge, vote delegation emerges as a valuable mechanism, enabling community members to entrust their voting power to delegates who exhibit discerning judgment and clear communication of their insights. Vote delegation not only enhances overall vote participation but also in optimizing the efficiency of decentralized protocol governance, especially when dealing with a multitude of stakeholders, potentially reaching into the billions.

Furthermore, the practice of vote delegation fosters a more inclusive forum for participation in ShiftCTRL governance. This inclusivity extends to individuals who may not possess CTRL ownership, providing them with the opportunity to actively engage and contribute to the decision-making process.

Proposals
To submit a governance proposal, proposers will require at least 0.5% or more CTRL tokens delegated to them.

The most common types of proposal include:

- **Parameter Change**: to change the parameters defined in the Protocol.
- **Add Tab**: to create a new Tab currency. The new Tab currency will need to be assigned a name along with its value denominated in BTC or a fiat currency to which to peg to
- **Freeze Tab**: to temporarily disable all vault operations associated with a Tab currency. This measure is enacted strategically to safeguard the Tab currency from both potential and realized threats.
- **Unfreeze Tab**: to re-enable a frozen Tab currency once the threat has been contained.
- **Add Oracle**: to whitelist a new price oracle to the Protocol.
- **Remove Oracle**: to remove an existing price oracle from the whitelist.
- **Add Reserve**: to accept a new wrapped/bridged ERC-20 representation of BTC as reserves.
- **Remove Reserve**: to remove an existing wrapped/bridged ERC-20 representation of BTC as accepted reserves.

- **Ctrl+Alt+Del**: to de-peg a Tab from its fiat currency.

- **Software Update**: to update/upgrade protocol software.

- **Custom Proposal**: custom proposals to handle other issues or proposals requiring manual implementation.

Voting
Once a proposal is submitted, the community can utilise the 2-day *Voting delay* to review and evaluate the proposal before it transitions into a 3-day *Voting period*. During this voting window, delegates are presented with three distinct voting options:

- **Yes**: vote in favour
- **No**: vote not in favour
- **Abstain**: vote neither for or against but the vote counts towards the Quorum

For a Proposal to be accepted successfully, it must meet the following conditions:

1. Voter participation must be at least *Vote quorum.*
2. The ratio of vote in favour (yes) must be greater than the *Vote threshold.*

If a proposal is accepted, it is queued in a *Timelock* and can be implemented 2 days later.

At a technical level, smart contracts manage each type of vote. A Proposal Contract is a smart contract with one or more valid governance actions programmed into it. Once a proposal is accepted, the proposer may execute it after the timelock, and the changes described in a Governance proposal are automatically put into effect by the proposal handler.

10. Tab Protocol Parameters

Here are some example of protocol parameters configurable through governance.

Minimum Reserve Ratio (MRR) (default 180%)
The MRR is the primary safeguard against the price fluctuations (relative to fiat currency) of the Bitcoin reserves anchoring the Tab protocol. The interval between the MRR and the Liquidation Ratio serve as the buffer that absorbs any fluctuation within that magnitude. Community members need to decide on an optimum ratio that maximises both Tab liquidity and protocol integrity.

Liquidation Ratio (default 120%)
The Liquidation Ratio should have enough buffer from the market price to absorb any adverse price movement for the liquidation auction to be executed successfully. The Liquidation Ratio should also be fair and not be set too high where it becomes prohibitive to liquidity providers.

Risk Penalty (default 1.5%/day)
A well-balanced Risk Penalty not only encourages Vault Owners to behave prudently but also gives them sufficient time to raise necessary resource in the unfortunate event where their reserves have fallen below the MRR.

Risk Penalty Step Duration (default 24 hours)
The frequency at which the risk penalty will be calculated and accrued. Opting for a shorter duration offers a penalty more closely aligned with market conditions. However, it necessitates increased computational resources, consequently elevating the protocol's operational costs.

Auction Start Discount (default 10%)
The Auction Start Discount plays a pivotal role in encouraging active participation in the liquidation auction—a vital aspect of ensuring the Protocol's stability. Striking a delicate balance, the optimal discount rate is one that expedites the auction's resolution while avoiding undue penalization of the vault owner.

Auction Step Discount (default 3%)
The Auction Step Discount serves as an additional incentive to stimulate participation in the auction, particularly in cases where the initial Auction Start Discount may not accurately mirror the market's perception of the reserve's value.

Auction Step Duration (default 60 seconds)
The duration at which the price of the reserves is discounted further. Optimizing this duration is crucial for expediting the conclusion of the auction process.

Oracle step duration (default 1 hour)
The interval at which a price update is triggered within the system. Opting for a shorter duration may result in minor enhancements in price accuracy but can significantly impact operational costs.

Oracle movement delta (default 0.5%)
The magnitude of price change required to trigger a price update within the system. Choosing a smaller delta offers a more precise reflection of market price dynamics but may substantially increase operational costs.

Oracle minimum feed count (default 3)
The minimum number of feeds necessary for each interval for the feeds to be considered valid. The default value of 3 feeds represent the absolute minimum requirement, as any number below this threshold significantly heightens the risk of the oracle being compromised.

Oracle maximum miss count (default 3)
The threshold for the maximum number of consecutive invalid feed intervals that will prompt a freeze on the affected Tab currency. As the protocol accumulates a sufficiently large pool of nodes submitting feeds, the community should consider reducing this maximum to bolster protocol resilience.

Proposal threshold (default 0.5%)
The minimum number of vote delegations required for an account to initiate a proposal within the system. This threshold serves the purpose of mitigating spam and frivolous proposals. However, setting it excessively high may inadvertently create barriers to participation in governance processes.

Voting Delay (default 2 days)
The purpose of the voting delay is to provide the community with ample time to review and thoroughly evaluate the proposal before the commencement of the voting period.

Voting Period (default 3 days)
The voting window where delegates can submit their votes.

Timelock (default 2 days)
To facilitate a smooth transition in response to the changes proposed, the voting delay allows the community adequate time to prepare and adapt.

Vote Quorum (default 30% of circulating CTRL tokens)
Vote Quorum is the minimum percentage of circulating CTRL tokens that needs to participate in the vote for a proposal to be valid.

Vote Threshold (default Yes > No)
The minimum number of Yes votes needed for a proposal to pass. Currently, more than 50% of all votes must be Yes. Abstain votes are excluded from this tally.

11. Emergency Governance

The Emergency Governance module functions akin to the regular Governance module but is tailored with distinct parameters designed for more stringent proposing criteria and swift execution timeframes, specifically geared towards emergency situations. An illustrative scenario for the Emergency Governance's application is a proposal to freeze all Tabs, triggered in response to the urgent need for protective action following the discovery of a vulnerability that threatens the reserves deposited in vaults.

The default settings for the Emergency Governance include a proposal threshold of 1% and a vote quorum of 30%. Notably, the Voting Delay and Timelock are set to 0, and the voting window is condensed to a swift 2 hours to expedite decision-making during emergency scenarios.

Just like the regular Governance module, the parameters of the Emergency Governance are configurable through governance, allowing the community to fine-tune and adjust them over time, ensuring adaptability and responsiveness to evolving emergency situations.

12. Risk and Responsibilities of Governance

CTRL holders wield the collective power to shape the trajectory of ShiftCTRL, influencing its operational dynamics to reflect the community's vision of sound money. This authority is accompanied by the responsibility to navigate and mitigate any risks or threats to the system through sagacious and prudent governance.

While the protocol incorporates various mechanisms, as outlined above, to uphold stability, protocol governors should recognize that these measures may prove insufficient in the face of a protocol-wide liquidation of Vaults. Such a scenario could potentially lead to irreversible damage and protocol failure. Consequently, there exists a crucial need to strike a delicate balance between risk and reward when establishing governance parameters.

The temptation of incorporating a "failsafe" feature, where tokens are magically minted to rescue the system, is undeniable. However, historical evidence suggests that a miraculous solution is elusive. Moreover, implementing such a feature contradicts the very sound money principles advocated by the project, resembling the practices of the current monetary system that can create money out of thin air. Hence, the conscious design choice is clear: **if the protocol experiences gross mismanagement, it is not only expected but deemed necessary for it to fail.**

13. Conclusion

All technicalities aside, at the heart of ShiftCTRL rests the pivotal belief that we as global citizens, blessed with the resources and know-how, must come together to address the broken monetary system that has left our world on the brink of financial ruin.

As recent as the last two decades, history shows enough evidence that fiat currency is plagued by unsound monetary principles. Examples include the dramatic collapse of the Zimbabwean dollar in the late 2000s, the significant devaluation of the Argentinian peso with annual inflation rates reaching 100%, and similar circumstances affecting the Turkish lira with an annual inflation rate of 85%. Additionally, the Egyptian pound suffered a loss of over 50% of its value against the Dollar, while citizens in Lebanon faced challenges accessing their own funds from banks, and the ongoing debacle that has struck the Venezuelan bolivar in the last couple of decades are all proof.

Not to mention, these calamitous events took place on either side of the 2008 global financial crisis, an epic catastrophe that was bred on poor monetary policies that continue to impact the world till today. Compounding this issue, the world now contends with the deleterious consequences of unrestrained interest rate suppression and large-scale monetary expansion undertaken by central banks globally in the lead-up to and during the Covid-19 crisis.

The fact is fiat currency is caught in a cancerous loop – it is printed into existence by the powers that be through the issuing of debt, to pay off past debts with no end in sight. The plain and simple truth is that we must stop trying to cure a sickness with more sickness. It just doesn't work.

This is the true inspiration behind ShiftCTRL, a viable cure that is formulated using the philosophical approach developed by the Austrian school of economics, champions of individual rights, free market and most importantly, sound money principles.

To achieve a self-sovereign monetary system, ShiftCTRL leverages the immense potential of Bitcoin, all while heeding the strengths and weaknesses of monetary systems past and present, especially that of the formidable Classical Gold Standard.

All that said and done, we recognize that the objective of this project is a monumental undertaking on unprecedented levels. But then again, that is to be expected to weed out the long existing systemic flaws in our global financial system.

Nonetheless, we truly believe that with the combination of a suitable platform, the right motivation and worthwhile incentives, ShiftCTRL has the capacity to bring like-minded individuals under the same banner to remedy a crippled financial system using Bitcoin as a solid anchor.

More importantly, we ask you to think about what ShiftCTRL truly stands for; a communal endeavour to create a new monetary system that not only guarantees fairness and financial sovereignty, but also reinstates the human person back as the financial pulse of the world.