Economics of Dynemix

Dynemix is a blockchain platform of the next generation designed to become the first worldwide-adopted cryptocurrency capable of competing with conventional consumer-level payment infrastructure on equal footing and substituting it entirely eventually.

The economic model of Dynemix features a breakthrough design of a decentralized algorithmic central bank capable of simultaneously balancing the value of native coins against fiat currencies and directly maintaining a targeted interest rate, which allows to indirectly target an optimal level of inflation and output growth.

The following paper contains an informal description of the project. The provided specifications are not final and are subject to amendments, if necessary, up to the mainnet launch. Any updates to this paper can be made without prior notice.

The following paper does not contain any coin purchase offerings or any other information on the initial coin distribution.

www.liberdyne.com

version 1.0 © Dmitriy Petryakov 2024

Contents

I. Introduction

In 2009, the first decentralized cryptocurrency, Bitcoin, was introduced.

Bitcoin can be considered a response to the modern monetary policy, which tends to favor minor elite groups. Although the proclaimed intentions of banking systems led by central banks are focused on stabilizing the economy, facilitating continuous growth, and helping overcome crises, it often happens that gains are consumed by elites, and losses are shared among the middle class. E.g. according to the Bank of England, its own QE measures during 2008 recession increased the wealth of the richest 5% of households by 40%.

Bitcoin introduced a groundbreaking concept of an algorithmically controlled currency with a fixed hardcoded monetary policy that was supposed to prevent elite groups from gaining the ability to control the coin supply. Satoshi's invention could have changed the entire financial framework, but unfortunately, Bitcoin featured too many shortcomings that didn't allow it to reach the stated goal. Even though it was introduced by its creator as a decentralized payment system (literally "a peer-to-peer electronic cash system"), Bitcoin did not turn out to meet that definition and became a speculative asset or an inflation hedging tool instead.

If we leave technical issues aside and focus on the economic model of Bitcoin, we can state that there are two main issues in Bitcoin's design that impede the ability of the platform to perform the money function:

- Scarce supply and a primitive issuance model.
- An inappropriate model of the coin distribution.

It is impossible to solve these issues without changing the fundamentals of Bitcoin, which is why we need a new system that can finally embody the initial ideas of Satoshi and become a true cryptocurrency.

To create a true decentralized cryptocurrency, we need to solve the following issues:

a) **Technical.** The platform should be capable of providing the level of user experience at least not inferior to conventional fiat payment infrastructure. As far as this paper is devoted to the economic model, we will only address technical solutions that are required to implement the described features.

Inserts describing technical solutions will be marked with green background. If you are not interested in technical details, you can skip those parts.

b) **Economic.** We need to solve the issues of Bitcoin described above and create a currency that will be perceived as a medium of exchange instead of a value-storing asset.

c) **Political.** The system should stay substantially decentralized, which means that we cannot use economic models that heavily rely on external sources and/or governance. We can admit that the model will require corrections, which can be applied via forks, but we assume that this shouldn't grow to the extent of systemic manual control.

In the following paper, we present an economic model of cryptocurrency Dynemix, which is capable of conducting a monetary policy in a similar manner as the conventional policies of central banks are executed, at the same time being completely decentralized and independent, thus becoming the first true cryptocurrency.

II. Simple Model

1. Naïve Implementation

The scarcity of the money supply eliminates incentives for economic development. If the economy grows much faster than the money supply, it leads to deflation, which in turn gives a start to deflationary cycles that create permanent instability.

If we want to create an asset that will be used as a medium of exchange, this asset should be perceived as something spendable. This can be achieved by raising the expectations of perpetual devaluation, and an obvious solution is to apply a high issuance rate.

According to the naïve concept, we need to find the optimal ratio of the attractiveness of our coin to consumers and its unattractiveness to speculators. Simply put, if the issuance rate is set too low, it may turn the coins into an investment and inflation-hedging asset like Bitcoin; if the rate is too high, we may inhibit the growth of the platform for a rapidly depreciating asset becomes unattractive for any purpose. This idea can be interpreted as a sort of Friedman's k-percent rule.

At the early stage, the emission rate could be set higher since the platform will more likely experience an influx of investors expecting an increase in value. In time, as the potential investment attractiveness drops, the issuance rate should be decreased and stabilized at some point providing the level of the supply inflation optimal for the further economic growth.

Suppose we apply 10% annual emission during the first year after the mainnet launch with a gradual reduction of the monetary issuance to the level of 5% within the following five years.

This solution engenders two issues:

- We cannot reliably estimate the optimal issuance rate. We are unable to forecast even an approximate course of the economic development, which is why any chosen rate is just a shot in the dark.
- This approach can work with a Proof-of-Work (PoW) system, but being applied to a Proof-of-Stake (PoS) system it can produce the opposite effect.

The problem is that PoW concept is obsolete and cannot provide technical features that allow the platform to compete with conventional centralized payments systems, which is why we need to use a PoS model.

Suppose we have a typical PoS blockchain, in which coin holders can deposit coins in their possession to participate in block production (minting). We also have a fair random sampling algorithm that provides a chance to create a block proportional to the size of the deposit S_n expressed as a share of the total coin supply, and an issuance model with the amount of reward for each block that maintains a constant annual issuance rate k_i. In our model, we will neglect minimal stake requirements as well as other obstacles for the participation in minting (hardware, bandwidth etc.) and assume that each coin holder can participate on equal terms regardless of the number of coins in his possession.

Suppose we have an array of n stakeholders each of which placed a stake of an arbitrary value. The stake pool S will consist of the sum of all currently placed stakes

$$S = \sum_{i=1}^{n} S_i$$

Alternatively, we can define S as a share of the total supply of coins being staked at a given moment.

In the long run, each stakeholder will receive a number of coins corresponding to the size of his stake S_n, the size of the stake pool S and the issuance rate of the blockchain k_i. Typically, stakeholders are also allowed to restake after a certain Δt, and they can compound interest by adding the newly acquired coins to S_n. Under such conditions, the annual nominal income of stakeholders can be expressed as

$$\frac{S_n k_i}{S} < \text{nominal income } < \frac{S_n(e^{k_i} - 1)}{S}$$

We can also compound the issuance rate by recalculating each subsequent $k_i(B_n)$ in the row $\{B_n\}_{n\in\mathbb{N}}$ according to $k_i(B_{n-1})$ to offset additional income gained by restaking, but since potential deviations are low enough to be negligible for our purpose in any case, we will approximate the result to

$$\frac{S_n k_i}{S}$$

The equation above, however, doesn't account for the growth of the coin supply that occurred via k_i.

Assume that coins of our blockchain hold stable value. Inflation i can then be expressed through inflation of the coin supply or, in other words, the issuance rate ($i = k_i$). Under such an assumption, we can adapt the Fischer equation to calculate the real income for stakeholders in the following way:

$$\text{real income } = \frac{S_n k_i / S + S_n}{1 + k_i} - S_n$$

We can derive two important observations from this equation:

a) **Under $S = 1$, $real\ income = 0$ regardless of k_i.** If all coins in the system are staked, minters gain no real income, and the relative share of the total supply in their possession stays static at any issuance rate we set. The assumption of all coins being staked, however, is unrealistic and meaningless. Coins are supposed to be transacted, which is why only a fraction will be deposited simultaneously.

b) **Under $S < 1$, $real\ income > 0$ and is positively correlated with k_i and inversely with S.** The less the stake pool is, and the higher issuance rate we set, the more real income the stakeholders start to receive, which means that by adopting the model described above we create incentives for hoarding instead of spending, thus achieving a result opposite to our intentions.

To make the model work, we need to adjust the setup and create an inverse relation between the issuance rate and real income. At this point, we introduce our contribution to the crypto economics: helicopter coins.

2. Helicopter Coins

In Bitcoin and other PoW systems, newly issued coins are granted to miners to create economic incentives for keeping the system secure. In PoS implementations, issued coins are distributed in a similar way among stakeholders (minters). As shown above, this approach allows to increase the relative share in possession and thereby makes the rich richer and the poor poorer. In fact, the economic models of current PoS implementations don't differ much from the conventional elitist policy of monetary authorities and have little to do with the initial ideas behind Bitcoin and decentralized currencies in general.

However, what if we start distributing issued coins among all users? The concept named helicopter money was proposed by Milton Friedman. The current understanding of the concept implies the transfer of newly "printed" money directly to individuals bypassing commercial banks (or applying variations, such as tax cuts, which can produce a similar effect) as an alternative to quantitative easing and other expansionary measures.

Although there are no banks that create credit money within blockchains, minters (miners) can be considered similar oligopolistic actors who have strong influence on the distribution of wealth. Bypassing minters and giving coins to users significantly alters the entire economic model.

Permissionless blockchains are vulnerable to Sybil attacks, which is why a non-trivial technical solution is required to implement helicopter coins. We cannot simply grant coins to all IDs (accounts, keys etc.), because users can create multiple representations to gain more coins (unless the setting is permissioned).

In Dynemix, the solution for distributing helicopter coins is based on the capabilities of the Liberdyne messenger. The system features a transport protocol for offline message delivery that involves a band of users as delivery relays. One of the key properties of the protocol is extremely low overhead, which allows for participation via mobile devices. As the protocol will be activated for all Liberdyne users, it will serve as a distribution channel for helicopter dynes. You can read more information on the solution in the Dynemix and Liberdyne whitepapers.

Now let us see what happens if we introduce helicopter coins into the model described above.

Assume we set a minters' share k_s. For example, we set $k_s = 0.2$, which means that out of all issued coins only 20% go to minters and 80% are dropped from the helicopter.

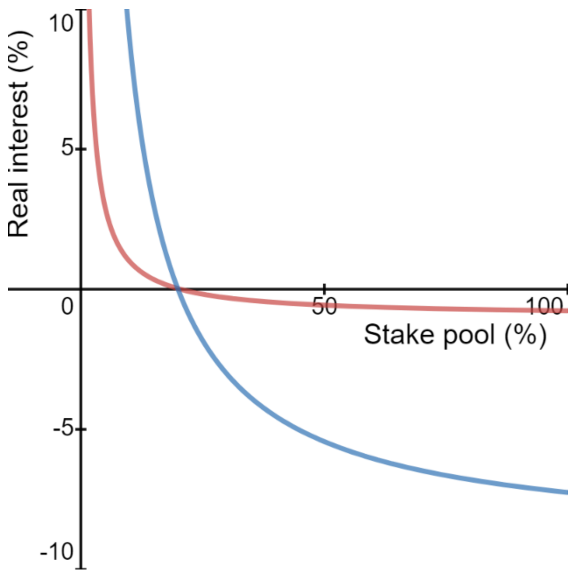
For simplicity, let us transition to the simplified version of the Fischer equation. Also, we will switch from the notion of income to the notion of interest and express all values of the variables in %. With the introduction of k_s, the equation of real interest r will look as follows:

$$r = \frac{k_s k_i}{S} - k_i$$

We can derive three important observations from this equation:

- $r < 0 | k_s < S$**.** If the stake pool exceeds the minters' share, minters start losing value in their possession, which makes hoarding not profitable.
- $r = 0 | k_s = S$**.** When the stake pool is equal to the minters' share, real income is zero, and minters maintain value in their possession.
- $r > 0 | k_s > S$**.** If the stake pool is below the minters' share, minters start gaining profit.

Suppose we have two blockchains with $k_i = 1$ in one, $k_i = 10$ in the other, and $k_s = 20$ in both. The interest rate chart will look as follows:



Axis X shows the volume of the global stake pool. Axis Y shows the real interest rate of minting at different stake pool sizes. The red and blue lines show real interest at $k_i = 1$ and $k_i = 10$ respectively.

We can see that the more we increase the issuance rate, the steeper the curve of the interest rate to the right of the neutral point $S = k_s$ becomes. If we target a stake pool size above the currently set minters' share, we can use the issuance rate to change the rate of interest for minters, thus making hoarding less profitable.

With the introduction of helicopter coins, we now have a model that can solve the issue of hoarding in PoS blockchains. By inflating the supply, we make long-term holding unprofitable, which escalates the turnover of coins and helps to stabilize the economy. In such a model, coins can become an actual medium of exchange instead of a speculative asset. At the same time, by setting a minters' share we can assure any required size of the stake pool for security.

3. From Hoarding to General Price Volatility

The described model still leaves plenty of issues unresolved. To start with, our simple model performs as a standalone ecosystem, and we didn't account its relation to external assets. The assumption of a stable real value of coins is unrealistic, and practice shows that blockchains are subject to massive value fluctuations.

Furthermore, even if we manage to solve the hoarding issue, there is still a problem of potential devaluation: we can expect drops in demand for our coins, which in worst cases can start a hyperinflation loop.

The stated problems bring us to the concept of a stablecoin. The issue of volatility in crypto economies has been addressed almost since the appearance of Bitcoin, and a number of solutions has been proposed to date.

The simplest solutions are collateralized stablecoins, which are powered by third-party's liabilities of backing coins by allegedly stable exogenous assets (such as a fiat currency, SDR, a commodity, etc.)

More sophisticated solutions use algorithmic schemes that allow the exchange rate to be determined by the market, but at the same time the supply is constantly adjusted to counter shifts in demand and keep the exchange rate stable. Known algorithmic solutions share three main fundamental flaws:

a) **They are not fully decentralized.** Seigniorage-style systems still require a "reserve bank" that stores a sufficient amount of the backing asset to counter price drops (as an alternative, it can rely on third parties performing the same functions). Managing the reserves requires a governance system, which, together with the price determination issue, inevitably brings us to a semi-centralized setting and/or significant dependence on third parties. It also brings uncertainty about the legal status of assets used in such models and about possible actions of financial regulators for said assets will be likely considered securities.

b) **They are not long-term robust.** The main economic driver of the algorithms is a short-term arbitrage opportunity. If the peg breaks, there are no long-term sustainability mechanisms, which can lead to a "bank run" of economic agents and a quick collapse of the system.

c) **They are not independent in the economic sense.** As a rule, stable coins derive their proclaimed stability from allegedly stable off-chain assets. In other words, such coins are only as stable, as assets that they are pegged to are. This concept may be acceptable if we only intend to build a sort of an auxiliary financial asset, but as we are going to create a new generation of money capable of substituting the entire fiat financial infrastructure, such an approach does not withstand criticism.

To reach our proclaimed goals, we need to create not simply a stablecoin but a completely independent model of economy that is capable to maintain stable prices intrinsically, regardless of any "foreign currencies".

Given our intentions to create a fully decentralized cryptocurrency that can substitute traditional money, we made every effort to solve the stated problems and herein we present the first model of an independent algorithmic economy capable of taming volatility and sustaining stable economic growth that relies neither on exogenous sources or assets nor on governance.

In the following section we will describe the algorithm that works as a stablecoin, i.e. an asset that maintains its exchange rate against exogenous currencies, after which we will extend the model to a fully-fledged decentralized central bank.

III. Complete Model of Stablecoin

1. Framework

The functioning of our model is based on certain premises that we need to outline before we describe the algorithm. Some of them require specific technical features, which is why the algorithm cannot be implemented into any arbitrary PoS blockchain.

a) **There is no difference between staking coins and holding them in the free form except for the opportunity cost.** We assume that the majority of users will prefer holding coins that exceed their short-term transactional demand as stakes and participate in minting because minting always brings nominal interest regardless of the state of the economy at any given time and hence is more profitable than keeping coins in the free form (unstaked). Locking and unlocking of the coins should be fast and free, and participation in the block production should be affordable for the vast majority of users. Essentially, in our economy saving means staking.

This assumption makes the volume of the stake pool highly elastic to market conditions, which allows us to use it as the main indicator of the current state of the economy at any given time, thus circumventing the involvement of exogenous oracles to retrieve data on prices, exchange rates or other indicators.

Our model assumes that coins deposited as stakes are equally (or nearly-equally) liquid to unstaked (free) coins. This doesn't seem realistic for most current PoS implementations. PoS concept suffers from a problem called nothing-at-stake. A possible solution to the named problem implies locking the deposited stakes for a long period (possibly reaching months), which turns staked coins into a long-term maturity asset. Although such a design is currently used by many PoS blockchains, it doesn't fit our economic model.

In Dynemix, we use a different approach to the nothing-at-stake problem, and deposited coins become spendable within approximately 30 seconds after an unstake transaction is processed. Although the liquidity of deposits is still formally lower than that of free coins, the difference is so minuscule that it can be neglected. For that reason, we can claim that in Dynemix liquidity preference doesn't influence the choice between holding free coins and depositing them as stakes. As we made minting extremely user-friendly via the Liberdyne messenger and secured low hardware requirements, the design of Dynemix fits the described model and allows for its full-scale implementation.

b) **We refine the notion of the real interest rate.** Previously, we assumed an autarkic ecosystem where the real interest rate was the nominal interest rate adjusted by supply inflation. Now that we switched to a more realistic setting with volatile prices, a real interest rate is the nominal interest rate adjusted to price inflation, which is a common comprehension of the notion at hand. Henceforth, the equation of the real interest rate looks as follows:

$$r = \frac{k_s k_i}{S} - i$$

c) **Users behave rationally and tend to choose a more profitable asset to hold.** The behavior of most participants is driven by the opportunity cost, risk assessment and expectations. We assume that in relation to the coins in possession that exceed the transactional demand, out of staking coins and keeping them in the free form the user will prefer the first option, whereas out of staking coins and exchanging them into other assets the user will consider the difference in the provided interest and the risk of losing liquidity along with other risks that emerge from the decision of transitioning value from a decentralized environment into a centralized one. In short, our approach is similar to the Tobin's portfolio model.

d) **The substantial part of the economy is formed by a real market with sticky prices.** The model can inherently adapt to trends but provide a worse reaction to shocks. For example, the model will not be efficient in the current economy of Bitcoin as the demand for BTC is formed

> mostly by the speculative motive, which can quickly shift the demand within a very wide band. The predominance of the transactional motive, on the other hand, allows to take the advantage of price stickiness along with time lags in the transmission scheme and hence effectively manage the expectations of economic agents.

2. Default Equilibrium

First, we need to define the default state of our economy and the targeted conditions the model will strive to maintain.

1) Stake pool

We need the stake pool to be as high as possible to provide more security. We assume that in a PoS system, the larger the global stake pool is, the more resources are required for a successful attack.

At the same time, the stake pool produces an effect similar to excessive bank reserves in a conventional economy: while being deposited, coins are withdrawn from the markets, and the velocity of circulation is reduced. The larger share we allow to be deposited, the larger fluctuations in velocity of circulation can occur as the stake pool shifts.

Given the statements above, suppose the default stake pool target is $S^* = 20$ for it provides sufficient security and produces a lesser effect on velocity. This value, however, may be not final and can be subjected to changes during further research.

2) Issuance rate

The issuance rate should be set to maintain a targeted inflation rate. If we target inflation $i^* = 2$, assuming the demand for money is static we need to apply $k_i = 2$. The demand in our stablecoin model is not static, however, which is why we need to continuously adjust the issuance rate according to the shifts in demand.

There is no need to set the upper boundary, which makes expansionary potential practically unlimited, but the lower boundary is derived from the PoS security model, which requires economic incentives for minters to participate in block creation. We can claim that $k_i > 0$ at least.

Although we consider staked and unstaked coins equally liquid, there is still a sufficiently low value that makes the yield provided by stakes negligible for most participants. In terms of this section, we will consider $k_i = 2$ a lower boundary for illustrative purposes.

3) Natural savings

At this stage, we apply the Keynesian approach to the demand for money. We assume that most of the supply is used for transactions while a certain fraction is saved by participants. These savings consist of the natural fraction, which is formed by the long-term transactional motive (coins that are meant to be spent but with some significant delay) and the precautionary motive (coins that are saved for possible unexpected expenditures), and of the speculative fraction, which represents the opportunity to gain interest.

The natural fraction should remain approximately the same size, whereas the speculative fraction can fluctuate within a very wide band depending on the current economic setup and the expectations of future trends.

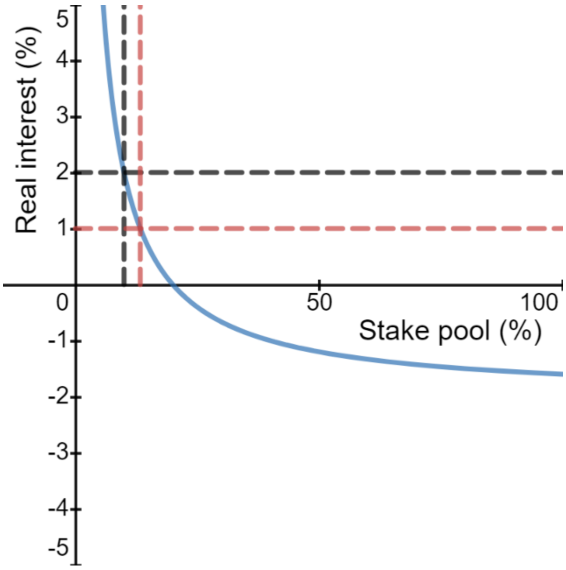
To effectively counter demand imbalances, we should estimate the natural savings rate. As in our model we assume deposited coins to be almost equally liquid to free coins, most of the natural savings will be staked anyway, regardless of the incentives at the time, which is why after we try to lower the targeted stake pool size below the natural savings boundary, the stake pool can become inelastic to market conditions, and our monetary policy will lose its effectiveness.

It is hard to predict the natural savings rate at the current stage, but we can roughly estimate that it will likely not exceed 10% of the supply. A more precise assessment can be made via empirical studies.

If we assume the natural savings to reach approximately 10%, can we then conclude that the stake pool normally should also be of that size? As we mentioned, we expect the speculative motive to have a significant influence on the total savings rate, and the actual size of the stake pool will depend on the real interest that deposited coins provide.

4) Natural interest

Suppose the economy remains stable for a certain period, prices hold at the same level and are not expected to shift. All other variables being static, if we apply $k_i = 2$, this should cause equal price inflation in the long run, and $\mathbb{E}(r)$ curve under $k_s = 20$ will look like this:



We can see that under $S = 10$ minting provides $r = 2$ (the black dashed lines).

If the current short-term real interest provided by exogenous assets r_e is also equal to 2%, it is not profitable to deposit coins further as the growth of S pushes down r, which incentivizes to convert savings into more profitable assets. If r_e drops to 1%, however, our coins become more attractive and S will grow to $S = 13.3$, at which $r = 1$ (red dashed lines). We can state that there is always a point of equilibrium to which the stake pool size tends at any given time. This point is defined exogenously by the interest rates of alternative assets combined with the exchange rate shifts and endogenously by the economic setup of our coins.

This leads to the conclusion that if we want to target a healthy size of the stake pool (say $S^* = 20$), we also need to target a healthy interest rate, which brings us to the notion of the natural interest r^*.

The natural interest rate is a Wicksellian concept and can be defined as a short-term real interest rate that provides for the output growing at its potential rate. Since it cannot be observed directly, the question of measuring the exact rate is debatable. Inasmuch as this paper doesn't purport to establish the final implementation of the model but rather to describe the basic principles, let us leave this question aside and pick a value from a well-studied conventional policy rule. Suppose the long-term $r^* = 2$ as suggested by the Taylor rule. Following the same logic, we can also set a targeted inflation rate $i^* = 2$.

5) Potential output

Now that we have established a desired i^* and r^*, the only thing we lack is the rate of expected potential economic growth ΔY^*. The exact rate is debatable, but suppose we agreed on $\Delta Y^* = 3$ as proposed by the McCallum rule.

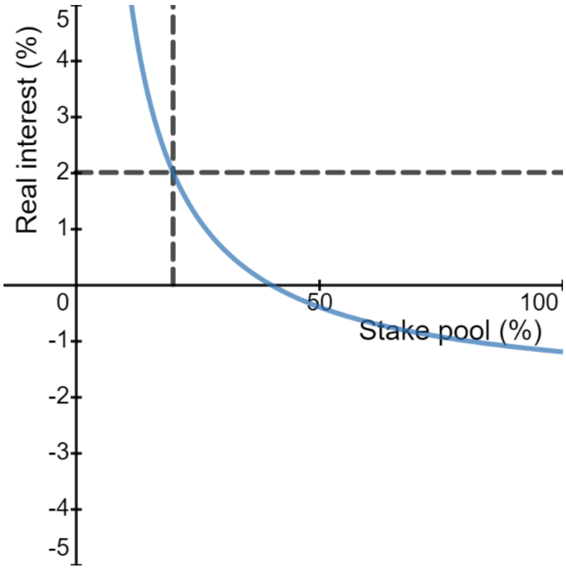
6) Equilibrium

All established variables hold fairly stable in the long run, which makes them consistent with our decentralized approach: we do not need to constantly adjust them but instead can preset values that will be relevant at least for the next 5-10 years, hence circumventing the need of a centralized governance.

Suppose we target the stake pool to $S^* = 20$ under the default conditions. To accomplish this and secure the suggested rates of interest, inflation and economic growth, we need to set $k_s = 16$. This finally brings us to the complete setting of the optimal initial equilibruim:

Under the issuance rate of 5% and the minters' share of 16%, given that the economy grows at 3% annually, the real interest rate is 2%, inflation is 2% and the stake pool is 20%.

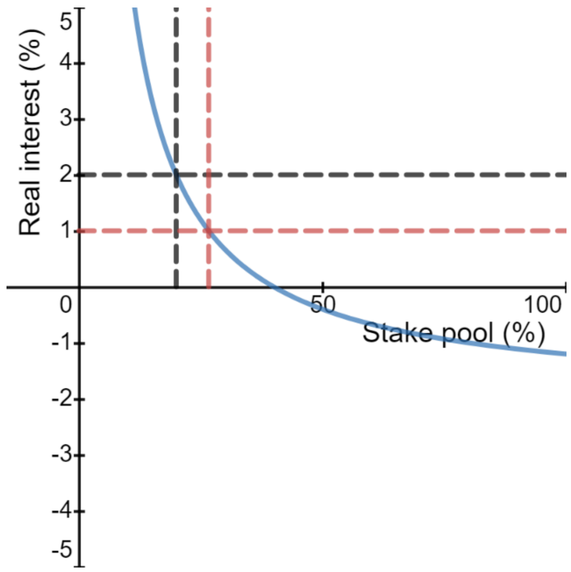
This is how the interest curve will look under the described optimal conditions:



Unfortunately, the optimal state is not a privilege we can enjoy for long, and an imbalance between the demand and the supply will emerge forcing the algorithm to conduct either expansionary or contractionary monetary policy.

3. Expansionary Policy

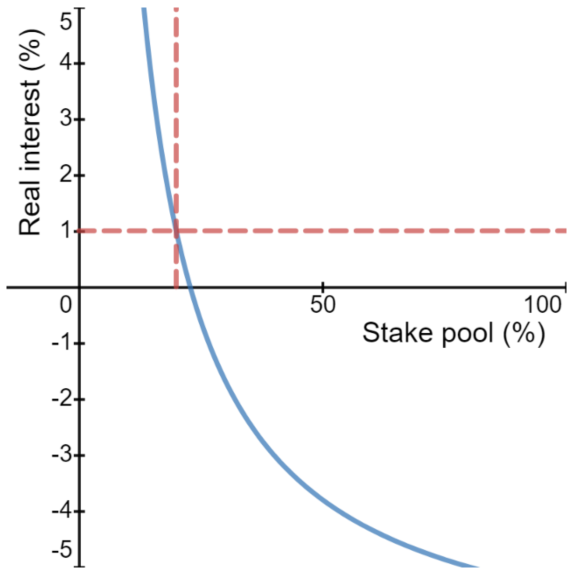
Suppose the Central Bank (CB) intends to stimulate the demand and drops the exogenous short-term real interest rate r_e to 1%. Since our stake pool is currently $S = 20$, which provides $r = 2$, this makes our coins more attractive than alternative assets nominated in the competing currency, and the speculative demand grows pushing the point of equilibrium to the right on the curve:



The black dashed lines show the initial equilibrium ($r = 2$; $S = 20$). The red dashed lines show the new equilibrium, which is now reached at $r = 1$; $S = 26.6$.

The system detects a positive shift in S (as we know, S can be observed on-chain at any time) and assumes the demand is growing. The algorithm starts increasing k_i until a new equilibrium is reached at $S = 20$. The exact rate depends on how the economy reacts to the monetary expansion.

For the purpose of this section, assume static ΔY: regardless of the actions of the algorithm, $\Delta Y = 3$. Then we can assume that any change in the issuance rate will shift the expectations of inflation $\mathbb{E}(i)$ by the equal margin. Under such conditions, a new equilibrium can be found at $k_i = 10$. r curve will look as follows:



On the curve above, 20% stake pool provides 8% nominal interest, and, given 10% issuance rate and 3% economic growth, expected inflation reaches 7%, which secures 1% real interest for stakeholders.

One can notice that a jump from $i_1 = 2$ to $i_2 = 7$ seems excessive for a scenario in which the real interest rate drops only by 1%. This observation leads us to the next issue: a faster devaluating currency becomes less attractive.

Suppose the exogenous inflation level $i_{e2} = 4$. In such a case, our currency with $i_2 = 7$, other factors being equal, becomes less attractive to hold, which shifts the demand in favor of the alternative currency. The disproportion in demand affects the exchange rate making our coins devaluate against the fiat currency. In this case, the exchange rate channel of the monetary policy activates.

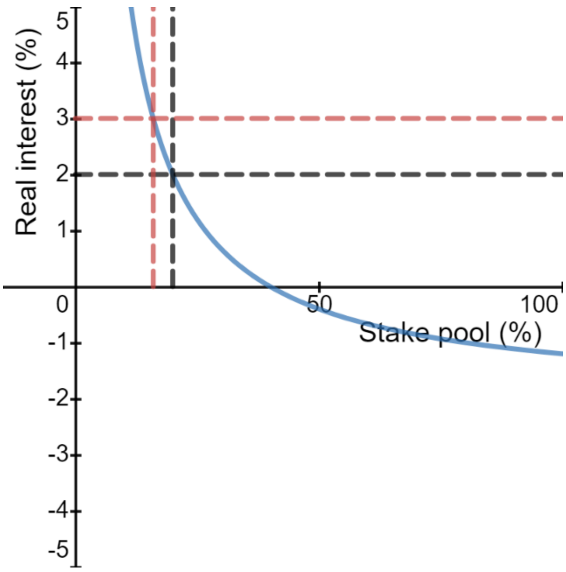
If we assume both currencies being interchangeable, under the assumption of perfect capital mobility, the exchange rate can directly affect preferences: more nominal interest will be demanded from a devaluating currency to be preferred for the speculative purpose, and hence an equilibrium will be actually found at a lower issuance rate, somewhere in the band $5 < k_{i2} < 10$. Conversely, if the alternative currency faces faster devaluation, it can push $k_{i2} > 10$.

The algorithm also response in a similar way to the pressure that comes directly from the exchange rate channel. If the exchange rate shifts in favor of our currency for the reasons irrelevant to the macroeconomic setup, this makes our coins preferable to hold even under $i < i_e$, which attracts more stakeholders and pushes the stake pool up. The algorithm escalates expansion, which causes a downward pressure on the exchange rate until an equilibrium is reached at S^*.

In any case, under the assumption of interest rate parity, an equilibrium will be found, and the algorithm will be capable to adjust the supply to the growing demand and balance the economy against alternative assets to keep the exchange rate relatively stable.

4. Contractionary Policy

Suppose the CB intends to cool down the economy and raises the exogenous short-term real interest rate r_e to 3%. Since our stake pool is currently $S = 20$, which, under the initial economic setup, provides $r = 2$ for stakeholders, this makes our coins less attractive than alternative assets nominated in the competing currency, and the speculative demand drops pushing the point of equilibrium to the left on the curve:



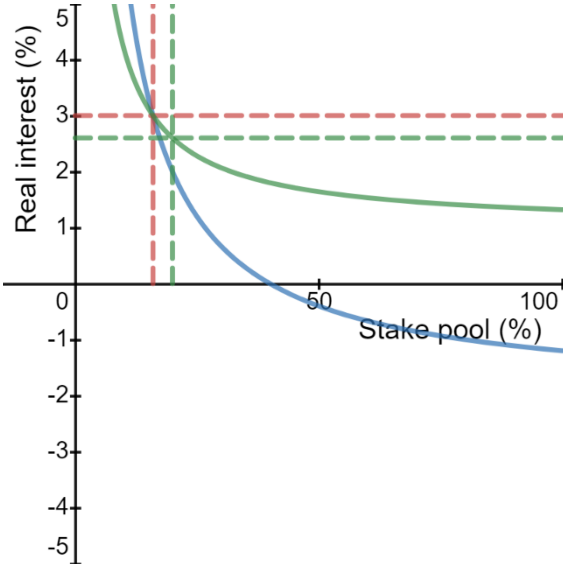
The black dashed lines show the initial equilibrium ($r = 2$ at $S = 20$). The red dashed lines show the new equilibrium, which is now reached at $r = 2$ at $S = 16$.

The system detects a negative shift in S and assumes the demand is falling, therefore it needs to adjust the supply to the falling demand.

1) Decreasing issuance rate

Suppose ΔY stays static. If we target $r = 3$ under such conditions, the model fails finding an appropriate k_i to return to S^*. The reason is that we set $k_s = 16$ previously, which means that it's impossible to provide a real interest equal to the rate of economic growth under $S > 16$.

In such a case, the system will decrease k_i to the lower boundary (which we previously set to 2%):



The blue line shows the r_1 curve. The green line shows the r_2 curve at $k_i = 2$. The red dashed lines show an equilibrium at $S = 16$ and $r = 3$. The green dashed lines show an equilibrium at $S = 20$ and $r = 2.6$.

We can see that even after k_i drops to the lower boundary, $r = 3$ is still acquired at $S = 16$. Under the assumed conditions ($\Delta Y = 3$), our current version of the algorithm can counter the increase of the interest rate only up to $r = 2.6$ (green dashed lines on the chart).

According to the equation of exchange, other variables being static, with $k_i = 2$ and $\Delta Y = 3$, our model should provide $i = -1\%$ in the long run. If the CB manages to increase r_e, at the same time keeping $i_e \geq 0$, our deflating currency becomes more attractive, which will result in a positive shift in the exchange rate against the competing currency. Under such conditions and under the assumption of interest rate parity, it can become possible to find an equilibrium by adjusting only k_i but suppose that $i_e = i = -1$.

2) Increasing minters' share.

Suppose the algorithm set $k_i = 2$, but the stake pool is still below 20%. We cannot go below the lower boundary of k_i for it can jeopardize the security model of the blockchain, and hence we need to use other tools.

As we remember, the equation of r in our system contains two arbitrarily adjustable variables. So far, we used only k_i, but since it no longer suffices for our goals, we should turn our attention to k_s. Earlier, we set $k_s = 16$ and haven't been touching that setting ever since, but now we need to adjust it to create a proper contractionary algorithm.

First, we need to set the boundaries that we can work within.

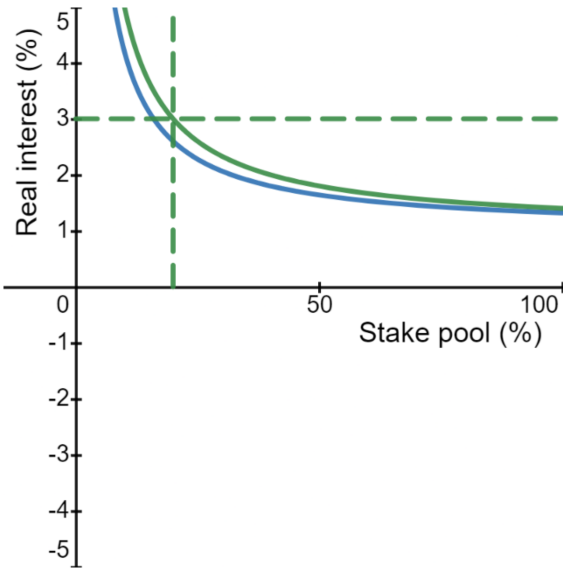
a) **Lower boundary.** $k_s = 16$ allows to target $S^* = 20$ under normal conditions, which were described earlier. If we decrease it while keeping k_i intact, this will decrease r, and S will shrink to compensate for that effect, hence forcing us to set a lower S^*.

   The size of S directly determines the security level of the blockchain, which is why keeping it reasonably high is one of the top priorities. For that reason, we assume that we shouldn't set k_s that targets $S^* < 20$. We should also keep in mind the issue of the natural savings rate and keep S sufficiently above that rate.

b) **Upper boundary.** Theoretically we can go up to $k_s = 100$, but that depends on the particular implementation of helicopter coins. Since permissionless blockchains are vulnerable to Sybil attacks, a Sybil-proof solution is required, which in most cases rely on certain resources being spent or put at stake. Under such conditions, we should keep a sufficient level of economic incentives for resources to be shared, hence a minimal helicopter share should be set.

In Dynemix, we use helicopter coins as a reward for delivering messages to offline users. This activity consumes only a tiny amount of resources, which is why we do not need much of incentives. We can assume that 5% share should suffice and set the upper boundary $k_s = 95$ for now.

Now let us see how adjusting k_s affects our economic setup. As we remember, our initial setting changed to the following: $k_i = 2$, $\Delta Y = 3$ and $i = -1$.



The blue line shows r_2 curve from the previous chart at $k_i = 2$ and $k_s = 16$. The green line shows r_3 curve at $k_i = 2$ and $k_s = 20$. The green dashed lines show an equilibrium at $S = 20$ and $r = 3$.

After we set $k_s = 20$, the equilibrium at $r = 3$ shifted to $S = 20$, which was exactly what we wanted, but does it help us with our goal of balancing the economy? To answer this question, let's take a look at how the contractionary policy is executed by CBs in conventional economies.

When a CB raises r_e, the effect of that transitions to other market interest rates, which raise accordingly. As borrowing becomes more expensive, individuals start cutting consumption while business cuts investments in the expansion of production and research. This causes a drop in the aggregate demand and employment, which further contributes to a decrease in the demand.

With fractional reserve banking, a large portion of $M2$ money supply consists of credit money. While less loans start being issued under higher interest rates, and previously issued loans continue being repaid, the volume of credit money circulating in the economy shrinks, thus reducing the overall money supply.

We can state two main effects that are caused by the contractionary policy:

- The money supply shrinks taming inflation.
- The aggregate demand drops cooling down the output.

As we consider our currency an ancillary financial asset in this section, we will leave the issue of the aggregate demand aside for now. The effect on the money supply is what currently interests us most. If we look back at our model, we can see that adjusting k_s doesn't allow us to reach the said effect: when we increase k_s, k_i stays intact, and the money supply still inflates, whereas the redistribution of newly created coins between regular users and minters caused by our measures produces no effect on the overall money supply.

This conclusion shows us that our algorithm still lacks an efficient tool to conduct a proper contractionary policy and we need to apply further complications.

3) Reducing velocity of circulation

Since we don't have a fractional reserve system within our blockchain, and hence no credit money is issued and repaid, no control of the supply via r is available for us. We cannot use any procedures resembling open market operations to adjust the available monetary base either (as is done by CBs or proposed by the authors of Basis and several subsequent stablecoin projects) for it requires a discrete actor endowed with economic powers within the system, which is inconsistent with the concept of decentralization.

We can, however, approach the issue from another side: instead of contracting the supply directly we can create incentives for S to grow, thus locking a required share of circulating coins as deposits and granting them zero velocity. As S grows, the share of continuously transacted coins decreases, which reduces the overall velocity of circulation V. According to the equation of exchange, it produces the same effect on prices as a contraction of the supply.

Suppose each monetary unit is transacted once a year in average and $S = 0$ (no coins are deposited). This means that normally $V = 1$. As long as we maintain $S = 20$, however, 20% of the supply is continuously static. We can presume that the velocity should drop to $V = 0.8$ under such conditions, but this conclusion will unlikely hold in practice.

The reason for that is the natural savings rate, which we estimated as 10% previously. If we assume the presence of a share naturally holding near-zero velocity even without any deposits (all coins circulating freely), then under $S = 20$, V will be only 10% lower than under $S = 0$.

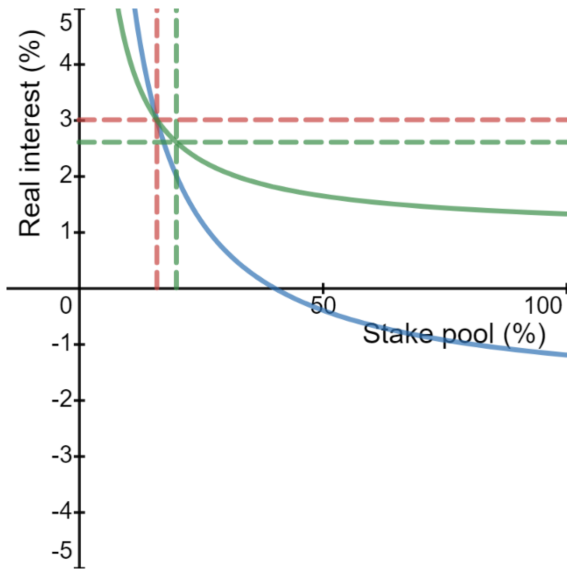
To simplify the model, let us neglect this issue and assume that the economy features $V = 0.8$ under $S = 20$. Also assume that any changes in S cause inverse changes in V, although the correlation may turn out not strictly linear in practice for there are other factors that influence V.

Since information on V at any given moment can be found on-chain (blockchains contain information on all transactions, which makes it possible to precisely assess all shifts in V), we can peg the contractionary algorithm to the actual V, i.e. the number of coins being transacted annually, but at this stage this measure seems excessive.

Assume $\Delta Y = 0$. According to the equation of exchange ($MV = PY$), ceteris paribus, shifts in the money supply M cause proportional shifts in the price level P, hence $k_i = 2$ should transition into $i = 2$ in the long run. If we adjust V, however, we can influence this effect: the decrease of V at 2% annual rate will nullify the effect produced by $k_i = 2$ and keep prices stable, whereas decreasing V at a rate exceeding 2% will cause price deflation.

Now, let us return to our framework. In our current setting, the economy grows by $\Delta Y = 3$, and since the algorithm stopped the contraction at $k_i = 2$, this leads to $i = -1$.

4) Shifting targeted stake pool size



Recall the chart for $k_i = 2$: The green line shows the r_2 curve at $k_i = 2$. The red dashed lines show an equilibrium at $S = 16$ and $r = 3$. The green dashed lines show an equilibrium at $S = 20$ and $r = 2.6$.

Since the algorithm reached the minimal k_i, but $S < S^*$, the respective contractionary measures are applied. For illustrative purposes, suppose our starting conditions are as described above.

The algorithm starts increasing k_s and at the same time adjusting S^* respectively. With the growth of k_s, r rises even under static k_i, and S grows, thus creating a deflationary pressure.

The pace at which the algorithm escalates the growth of the stake pool size and a respective decrease of the share of freely circulating coins defines $\mathbb{E}(i)$ in the economy in a similar way as k_i does, but the correlation is inverse. We can perceive $f'(1-S)$ as the contractionary rate in the system.

Although technically $f'(1-S) \neq f'(1-S^*)$, eventually the escalation of $f'(1-S^*)$ will transition into the level of deflationary pressure required to reach an equilibrium at S^*, which means that after a certain Δt, $S^* = S$. Then we can assume that within Δt, $\overline{f}'(1-S) \cong \overline{f}'(1-S^*)$. Given a proper implementation of the algorithm, Δt should be relatively short on the scale of macroeconomics, hence we can express the contractionary rate via $f'(1-S^*)$, especially considering that it will likely define $\mathbb{E}(i)$ to a much larger degree than the factual growth of S.

Let us denote the contractionary rate as $k_c = f'(1-S^*)$. $k_c = 0$ is the default value, which is used by the algorithm until stage two contraction is engaged. $k_c < 0$ creates a deflationary pressure and is used as a contractionary tool.

After the stake pool reaches the current target, the algorithm stops increasing k_c. In our case, escalating the expectations of deflation by 0.4% will allow the system reaching an equilibrium at S^* because, as mentioned above, stage two contraction started at $r = 3|S = 16; r = 2.6|S = S^* = 20$.

Suppose the algorithm escalated the growth of S^* so that the number of unstaked coins is expected to drop at the rate of 0.4% a year ($k_c = -0.4$), which has converted into 0.4% of additional deflationary pressure. Suppose to achieve that, we increased the contractionary rate exponentially using a geometric progression for k_c with the common ratio $a = 1.0001$ per block starting from $k_{c1} = -0.01$. Given 10 second block time, this would take

$$B_\omega = \frac{\ln(40)}{\ln(1.0001)} = 36891$$

blocks or approximately 102 hours.

We can compound k_c and recalculate the growth of each subsequent $S^*(B_n)$ in the row $\{B_i\}_{i=1}^{\omega}$ according to $S^*(B_{n-1})$, or we can peg the contractionary rate to the constant $S_1^* = 20$ (the size of S^* at which stage two contraction started). Let us calculate the new setting for B_ω for the latter case. S^* will grow to

$$S_\omega^* = S_1^* - \frac{k_{c1}(1-S_1^*)(a^{B_\omega}-1)}{B_y(a-1)} \cong 20{,}00098938\%$$

$k_s \propto S^*$ and will grow to

$$k_{s\omega} = \frac{S_\omega^* k_{s1}}{S_1^*} = 16{,}000791504\%$$

We can arbitrarily adjust a and k_{c1} to tune the algorithm as required and/or use a different growth function. With the values we have set, the targeted equilibrium can be reached relatively quick.

After the equilibrium is reached, the algorithm keeps increasing S^* at $k_c = -0.4$ and adjusting k_s respectively until S drops below the target or grows beyond it. If S falls short of the target again, the algorithm continues contraction. If S grows above the target, the algorithm starts to inverse the contractionary process by decreasing k_c so that $k_c(B_n) = k_c(B_{n-1})/a$ until $k_c = k_{c1}$. Once $S > S^*|k_c = k_{c1}$, the algorithm sets $k_c = 0$ and returns to stage one rule set.

We thereby created a contractionary algorithm that can counter drops in demand and balance the economy against alternative assets by expanding the stake pool and reducing the velocity of circulation of coins without changing the available supply and/or converting native coins into other assets.

IV. From Stablecoin to Stable Economy

1. Introduction

Until this point, we considered our currency an alternative monetary asset that is used along with a primary fiat currency and described our monetary policy as measures to balance the demand on our coins against exogenous stable fiat currencies to keep the exchange rate stable. Such coins are typically referred to as “stablecoins” in the crypto community. A setting in which crypto coins are used as an ancillary financial asset seems the most realistic at the early stages of crypto money adoption. Even the most optimistic enthusiasts wouldn’t argue that we can hardly count on quick mass adoption of a cryptocurrency as a legal tender all over the world no matter how well the said currency is designed.

As authorities won’t be willing to let crypto substitute fiat, the described setting will likely prevail in the near future. For this reason, it is crucial to develop an algorithm that follows the monetary policy orchestrated by centralized authorities: a task that our model copes with well, as was described.

We believe, however, that cryptocurrency technology possesses a potential to build something more than just an ancillary financial asset and that in future cryptocurrencies will eventually substitute fiat money in the same way as the latter substituted representative money in the past century.

2. Problem Statement

To bring our vision to life, our model should be capable of functioning not only as an ancillary currency that is pegged to fiat alternatives but also as a standalone monetary system. In the absence of a monetary authority and exogenous course to follow, the model should adjust directly to fluctuations in demand caused by shifts in macroeconomic indicators (inflation, output, employment etc.)

As we have described, even in the ancillary mode our model features wider capabilities than a typical stablecoin: whereas stablecoins adjust to shifts in the exchange rate against a particular currency, our model also engages the interest rate channel of monetary transmission and operates in conjunction with the entire global economy, which makes it act as a sort of a decentralized central bank.

However, to match the monetary capabilities of CBs, we still need to provide an optimal response directly to changes in the targeted economic variables. Modern conventional monetary policy implies discrete control of the interest rate by CBs, which assess the entire economic setup and establish an optimal interest rate for any given moment. Unfortunately, this is a privilege we cannot enjoy given our decentralized setting and the scarcity of data we can look up in the blockchain, which is why we need a non-trivial solution in the form of a feedback policy rule that can be incorporated into our algorithm.

To solve this problem, we can turn to well-known and studied solutions from the conventional economic framework and see if they are compatible with our model. The Taylor rule and the McCallum rule are, among others, the most appropriate to study in terms of our approach.

3. Taylor Rule

The equation of the rule looks as follows:

$$r = p + .5y + .5(p - 2) + 2$$

where

r is the federal funds rate,

p is the rate of inflation over the previous four quarters,

y is the percent deviation of real GDP from a target.

We can conditionally split the Taylor rule into two parts:

- **A targeted equilibrium.** The Taylor rule prescribes that when y and p are at their targeted rates, the CB should set $r = 2$.
- **Deviations from the target.** The Taylor rule prescribes to change r when y and/or p deviate from their targeted rates.

Simply put, 1993 version of the Taylor rule implies that the CB should shift the current real interest rate by 0.5% whenever inflation and/or real GDP growth shifts by 1% from the target respectively, therefore we can state that the rule incorporates the *inflation rate* and *GDP* as targeted variables and uses the *interest rate* as a policy tool.

4. McCallum Rule

The equation of the rule looks as follows:

$$\Delta m_t = \Delta x_t^* - \Delta v_t + 0.5(\Delta x_t^* - \Delta x_{t-1})$$

where

Δm_t is the growth rate of MB

Δx_t^* is the targeted growth rate of nominal GDP

Δx_t is the growth rate of nominal GDP

Δv_t is the growth rate of velocity

- **A targeted equilibrium.** The McCallum rule prescribes that when $\Delta x_t = \Delta x_t^*$, and the velocity remains constant, the CB should inflate m at the rate equal to Δx_t^*, which is suggested to be 3%.
- **Deviations from the target.** The McCallum rule prescribes to adjust m when Δx_t deviate from Δx_t^*.

Simply put, the original version of the McCallum rule implies that the CB should raise the rate of the monetary base expansion by 0.5% when the output growth falls short of the target by 1% and decrease the expansionary rate in the same proportion when the output grows faster than required. The expansionary rate should be also adjusted to the long-term growth trend of velocity. We can state that the rule incorporates *GDP* as the targeted variable and uses the *monetary base* as a policy tool.

5. Interpreting Equation of Exchange

We can see that the set of targets and policy tools in both mentioned rules doesn't allow for the direct implementation of either of them into our model. We can, however, use the underlying logic of the stated rules to create our own flexible rule that will operate with variables that can be determined within our framework.

Since the Taylor and McCallum rules are both derived from the equation of exchange, the best way to start is to take a look at the equation of exchange from the standpoint of our framework and available tools. If we assume that

$$MV = PY$$

then

$$\Delta M + \Delta V \cong \Delta P + \Delta Y$$

Within our framework, ΔM is the rate of monetary expansion, which we denoted as the issuance rate or k_i.

$$\Delta M = k_i$$

ΔV can be interpreted as a sum of exogenous shifts in velocity and the contractionary rate of the algorithm.

- **Exogenous shifts** in velocity ΔV_e occur due to economic prerequisites that are not directly controllable by the algorithm.
- **A contractionary rate** of the algorithm k_c is a rate at which the algorithm shifts S^* during the second stage of contraction.

$$\Delta V = k_c + \Delta V_e$$

Considering the above, the growth rate version of the equation of exchange now looks as follows:

$$k_i + k_c + \Delta V_e \cong \Delta P + \Delta Y$$

The right side of the equation, however, cannot be directly interpreted with the help of the tools available in our framework: we can obtain data neither on prices, nor on GDP from the blockchain, which is why we need to use proxy variables for that purpose.

6. Interest Rate as Target

According to the Fisher effect, shifts in the inflation rate cause equal shifts in the nominal interest rate. Since we can derive the current nominal interest rate I at any given time from S, we can substitute ΔP for ΔI.

$$\Delta P \cong \Delta I$$

As for GDP growth, we can choose different paths:

a) **We can express output through expenditures.** Since the information on transactions is available on chain, we can approximate aggregate expenditures and use them as a target. The precision and accuracy of the approximation, however, is highly dependent on the structure of the blockchain: if the blockchain supports only one type of general transactions, the result will likely be too loose to be used for a policy rule. Specific types of transactions, however, can help us derive a sufficiently accurate value. For example, we can conceptualize special transactions that are enforced to be used in case of a purchase of a final product or service by a customer for VAT purposes. Such transactions can allow for a more accurate assessment. As far as the path of the development of the blockchain is unclear, we would suggest a simpler approach:

b) **We can assume that changes in GDP growth rate transition into shifts of the interest rate.** In our framework, the increase in GDP growth rate will create upward pressure on the velocity of circulation and interest rate. The regression coefficient for the interest rate is not expected to be close to 1 as is in case of inflation rate shifts, and we can assume a lesser weight of GDP growth within our policy rule. An empirical study by Wang & Hausken (2022) suggests

> regression coefficients of 0.95 and 0.38 for the interest rate as the dependent variable and the deviation in the inflation rate with the deviation in real GDP as independent variables respectively in the Taylor rule framework.

Given the above, we can assume that

$$\Delta I \cong \Delta P + k_y \Delta Y$$

where k_y is positive but substantially below 1. The 1993 version of the Taylor rule implies equal weight of both Inflation and output gap ($a_\pi = 0.5; a_y = 0.5$), whereas the later modified version suggests a lower or even negligible weight of GDP for the monetary policy ($a_\pi = 0.5; a_y \geq 0$). In that regard, our policy rule follows the same logic: with GDP being less influential on the interest rate, deviations from potential GDP provoke a weaker reaction from the algorithm, and the policy rule is more focused on maintaining the inflation target. This approach also resolves the issue of the cost-push inflation, which moves GDP and prices in the opposite directions making the Taylor rule inefficient.

It is also worth noting that the output can be directly regulated by other means (such as the fiscal policy, government spending etc.) that can be complimentary to our policy rule. Given that national GDP and blockchain GDP have completely different meanings in our framework, it is advisable not to target output directly and leave its regulation to centralized authorities of the respective economic zones.

Now we have an equation that only contains variables that are obtainable from the blockchain or set by the algorithm itself:

$$k_i + k_c \cong \Delta I - \Delta V_e$$

7. Velocity of Circulation

The Taylor rule ignores the velocity of circulation, whereas the McCallum rule adjusts the rate of the monetary base expansion for the long-term velocity growth. McCallum suggests using a 4-year average rate at which the velocity of circulation grows due to the technological changes in production, which are not related to the current state of the economy and the phase of the business cycle.

We would suggest leaving the issue of the exogenous velocity aside until the economy matures, and enough empirical data is collected to make reliable assumptions. At the current stage, we see several issues that impede the development of a tenable solution:

- **The speculative motive.** On launch and presumably several years on, the demand for coins will be predominantly speculative with a slowly growing transactional fraction. In such a setting, the velocity can have unpredictable shifts.
- **Layer 2 solutions.** The development of layer 2 solutions can outsource a large chunk of transactions from the blockchain and add velocity fluctuations that are caused by transfers between layers, which will not necessarily correspond to changes in the money demand.
- **Overcomplication of the rule.** Our policy rule is driven by expectations and predictions of economic agents. A simpler rule makes expectations more consistent. Unnecessary complications, on the other hand, can add more uncertainty and discrepancy into the behavior of participants and drop the efficiency of the policy.

Furthermore, in our framework the control of V via k_c is one of the tools of the monetary policy, and S, which is a representation of V, is pegged to I. The factors that cause pressure on V will affect S and hence I, which will activate the counter measures from the algorithm, thus making the adjustments of the policy rule to the V_e redundant to a substantial degree.

For the stated reasons, we suggest excluding ΔV_e from the equation:

$$k_i + k_c \cong \Delta I$$

We should also note that although the information on the volume of transactions is typically available on blockhains, certain technical solutions can render obtaining such data difficult or even impossible.

For example, one of the potential solutions to the issue of financial privacy that may be implemented in Dynemix is an additive homomorphic cryptosystem with ZK proofs to encrypt balances and hide user interaction. Such an encryption would conceal both the volume and the number of transactions, thus rendering any information on V_e inaccessible.

In case if such technical solutions are implemented, we can only opt for neglecting the exogenous velocity entirely.

8. Response Time

We can conditionally outline three flavors of the rule depending on the response time while keeping in mind that we can arbitrarily chose anything in between and apply discrete gradual response time shifts.

a) **Instant response.** Blockchain technology allows for the adjustment of the monetary policy with each newly created block. Although it still takes a certain amount of time to occur, in terms of macro economy such small time intervals are negligible, which is why we can call a response as quick as a single block time instant. An instant response means that the policy applied to block B_n is formed according to the deviation of the targeted variable in block B_{n-1}, which is the quickest response time possible.

b) **Long-term response.** We can smoothen the response by picking up a discrete time interval to calculate the average change in the targeted variable. A long-term response means that the policy applied to block B_n is formed according to the average change in the targeted variable that occurred throughout the sequence of blocks $\{B_i\}_{n-t}^{n-1}$ where t is $\frac{descrete\ time}{block\ time}$.

c) **Interval response.** We can also apply a variation of the instant response that repeats after an arbitrarily chosen time interval instead of each subsequent block. An interval response means that the policy applied to block B_{tn} is formed according to the deviation of the targeted variable in block B_{tn-1} where t is $\frac{descrete\ time}{block\ time}$.

The interval response variation is vulnerable to attacks. The security of the algorithm depends inversely on the length of the time interval, which is why the interval variation of the instant response is not advisable to implement.

Changing the response time from instant to long-term should change the main driver of the monetary policy from expectations to the combination of expectations and retrospective analysis with the influence of the latter growing more with a longer time interval chosen.

In relation to blockchains, time intervals should be substituted by a number of blocks mined prior to the block to which the calculations are applied because depending on the design of the blockchain a block time is not necessarily constant. Since Dynemix operates in a lock-step execution manner, however, the block time in our system is constant, and each discrete number of blocks corresponds to a respective discrete time interval, which allows us to operate with time periods here and henceforth in terms of this paper.

9. Rule Coefficient

The Taylor rule is based on the principle of applying a surpassive pressure on inflation through a respective change in the policy tool: if $\mathbb{E}(i)$ shifts by n from the target, the CB should shift the nominal interest rate in the same direction by $n + a$ where $a > 0$. Particularly, Taylor suggests $a =$

$0.5n$. This allows not only to balance the occurred shift in inflation but also to push inflation back to the targeted value.

We can use the same principle in our policy. If I shifts by n, we need to balance it with a respective shift of k_i and/or k_c by n and add an additional value on top of that.

Since a cryptocurrency is not supposed to be an exclusive legal tender within the economic zone but rather a mere payment option (at least during the transitional period), and hence both speculative and transactional demand can fluctuate massively, we suggest a stronger policy reaction. We can use a higher coefficient or even switch to an exponential function. Suppose we set $a = 2$ as the stage one rule coefficient.

10. Interpretation of Rule

Now that we have all the variables and coefficients established, we can write an equation of the policy rule:

$$k_i + k_c = 2(I^* - I) + k_i^*$$

Where:

k_i is the issuance rate;

k_c is the contractionary rate;

I is the current nominal interest rate;

I^* is the targeted nominal interest rate;

k_i^* is an assumed issuance rate that maintains the targeted inflation rate and potential GDP.

Suppose we agreed that the potential GDP growth rate is 3%, the targeted inflation rate is 2% and the natural real interest rate is 2%. Then we can rewrite the equation as follows:

$$k_i + k_c = 2(4 - I) + 5$$

11. Stake Pool and Velocity

Now that we established the economic interpretation of the rule, we need to solve final technical issues to complete the algorithm. One of such is the relationship between S and V during an expansion.

Shifts in I correspond to respective shifts in S, which puts pressure on V.

Suppose the system is at the targeted equilibrium ($I = 4;\ S = 20;\ k_i = 5; k_s = 16$). After an arbitrary event, $\mathbb{E}(i)$ instantly drops from 2% to 0, which means that the same real interest is now acquired at $I = 2$.

If we opt for the instant response mode, k_i will be immediately raised to $k_i = 9$, and the equilibrium will shift to $S = 72$, which means that $\Delta(1 - S) = 65$ or, in other words, the share of unlocked (continuously transacted coins) should near instantly drop by 65%.

If we opt for the long-term response mode, the adjustment of k_i will take time, during which S will increase according to the occurred changes in I. The size of S that corresponds to $I = 2$ in the targeted setup is 40%, which means that $\Delta(1 - S) = 25$ or, in other words, the share of unlocked (continuously transacted coins) should near instantly drop by 25% and continue gradually decreasing afterwards.

In both cases, such an event will make a significant impact on the overall velocity. We can assume that V_e will increase inhibiting the impact to a certain degree, which can only be assessed via empirical studies, but due to the limitations of possible V_e growth this effect will unlikely be strong.

A significant rapid drop of V will put an upward pressure on I bouncing S back. However, we expect the effect of velocity to spread much slower than the effects of the interest rate or inflation, which can create a pendulum cycle. To mitigate this issue, we need to adjust the setup to make S return to $S = S^*$ without the need to wait until the entire transmissional scheme of all respective effects completes.

We can achieve this by adjusting k_s. In the ancillary mode, we used a constant value for k_s until the second stage of the contractionary algorithm was engaged, and the equilibrium at the stake pool target was reached by gradually changing k_i. Now that we pegged k_i to I by the rule coefficient, we need to use k_s as a technical tool to control the size of the stake pool. Suppose we set

$$k_s = \frac{IS^*}{k_i}$$

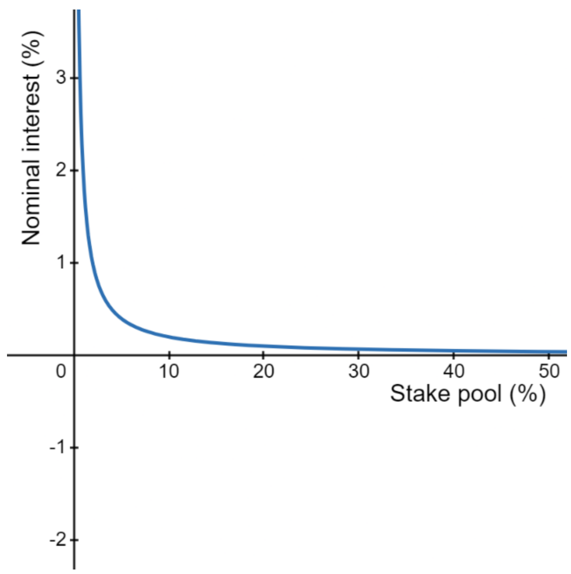
In this case, k_s will be constantly adjusted so that $S = S^*$.

12. liquidity Trap.

In our setting, I is apparently zero-bound since $I = k_s k_i / S$, and all variables on the right side of the equation can only be non-negative, which makes the policy rule technically inapplicable under $\Delta I < -4$. However, the realistic lower boundary of I is actually higher than 0.

Suppose the system is at the targeted equilibrium ($I = 4;\ S = 20;\ k_i = 5; k_s = 16$.) After an arbitrary event, $\mathbb{E}(i)$ instantly drops from 2% to -1.9%, which means that the same real interest is now acquired at $I = 0.1$.

Under the instant response, the setup will reconfigure to $I = 0.1;\ S = 20;\ k_i = 12.8; k_s = 0.15625$, and I curve will look as follows:



We can see that under $S > 10$ the curve becomes nearly flat. In fact, within the band $10 < S < 100$, I deviates only by 0.18%, which can be considered negligible by most agents. Under such conditions, S can become inelastic to further adjustments of the policy tools.

If I drops sufficiently low, we face a similar issue to the Keynesian concept of a liquidity trap, which can be overcome by measures similar to those proposed by Milton Friedman: we can still raise the rate of the monetary expansion and increase the helicopter share.

First, we should set a sufficiently high lower boundary for I at which we unpeg I from k_i and use a different rule coefficient a. We would suggest switching to an exponential function.

If $I < I_{min}$, the algorithm starts to increase k_i exponentially until $I = I_{min}$. Since k_s is inversely related to k_i during the expansion, it will decrease simultaneously thus increasing the helicopter share. These measures will continue the expansionary policy until an equilibrium is found at S^*. Once $I \geq I_{min}$, the reverse process is engaged until the system comes to an equilibrium at $S^*|I = I_{min};\ k_i = 11$, and the algorithm returns to the values established by the policy rule.

13. Algorithm in nutshell

Although the algorithm operates with S as the direct policy target since it is a value obtained from the blockchain, we will express S through I when separating stages of the algorithm to maintain compliance with the economic interpretation of the policy rule for illustrative purposes. A variable value for a particular block is denoted as $I(B_n)$, which means "I for block B_n".

By default, the algorithm is preset to the following values:

$I^* = 4$. The targeted nominal interest rate that the algorithm is designed to maintain.

$S^* = 20$. The optimal size of the stake pool under the targeted conditions.

$k_i = 5$. The issuance rate that corresponds to the targeted conditions.

$k_s = 16$. The minters' share coefficient that corresponds to the targeted conditions.

a) $I_{min} \le I < I^*$ **(stage 1 expansion)**

$$k_i(B_n) = 2(4 - I(B_{n-1})) + 5$$

$$k_s(B_n) = \frac{IS^*}{k_i(B_n)}$$

$$S^*(B_n) = 20$$

$$k_c(B_n) = 0$$

b) $I < I_{min}$ **(stage 2 expansion)**

$k_i(B_n) = ak_i(B_{n-1})$ until $I \ge I_{min}$

If $I \ge I_{min}$ and $k_i > 11$ then $k_i(B_n) = k_i(B_{n-1})/a$ until $k_i \le 11$

If $I \ge I_{min}$ and $k_i \le 11$ return to stage 1

$$k_s(B_n) = \frac{IS^*}{k_i(B_n)}$$

$$S^*(B_n) = 20$$

$$k_c(B_n) = 0$$

c) $I^* < I \le I_c$ **(stage 1 contraction)**

$$k_i(B_n) = 2(4 - I(B_{n-1})) + 5$$

$$k_s(B_n) = \frac{IS^*}{k_i(B_n)}$$

$$S^*(B_n) = 20$$

$$k_c(B_n) = 0$$

d) $I > I_c$ **(stage 2 contraction)**

$$k_i(B_n) = k_{imin}$$

$$k_c(B_n) = 2\left(4 - I(B_{n-1})\right) + 5 - k_i(B_n)$$

$$S^*(B_n) = S^*(B_{n-1}) - \frac{k_c(B_n)\left(100 - S^*(B_{n-1})\right)}{B_y}$$

$$k_s(B_n) = \frac{S^*(B_n)k_s(B_{n-1})}{S^*(B_{n-1})}$$

V. Additional features

1. Attacks and Security

So far, we do not see any potential rational attack vectors that can pose a serious threat, given a proper technical implementation. That being said, the model requires some non-trivial solutions from the underlying blockchain protocol, the effectiveness of which can determine the overall robustness of the system.

Since S is the main and the only indicator that triggers shifts in our monetary policy, the adversary would be required to control S either to keep it artificially low, which triggers contractionary measures, or artificially high, which provokes expansionary measures.

1) Undue expansion

To achieve his goal, the adversary needs to make S exceed S^*. Suppose the adversary possesses a significant number of coins that are not currently staked. By the start of the attack, the system stays at equilibrium and $S = S^*$. The adversary instantly deposits all coins in his possession, which makes S grow significantly.

Since the actions of the adversary decreased I for all depositors, but the overall demand for capital in the economy didn't change, other stakeholders seeking for optimal investment opportunities will withdraw their deposits and convert them into other assets that provide a higher yield. In a short time, S will return to an equilibrium with the actual demand for coins, which renders the adversary's actions pointless.

To provoke a continuous expansion, the adversary would need to keep S oversized for a long period, which requires him to possess a number of coins exceeding the difference between S^* and the natural savings rate. Given that we have chosen a proper target, this would normally require more than 10% of the available supply. At the same time, during the attack the adversary will suffer the following negative consequences:

- his coins will devaluate due to the excessive k_i and resulting inflation caused by his actions;
- he will lose an opportunity to gain more interest by investing into higher yielding assets.

Summarizing the statements above we can conclude that such an attack is unlikely to be committed.

At this point, it is time to mention the technical requirements for the underlying blockchain that are essential for the model to be robust. One of such is a fast deposit withdrawal. Unfortunately, as known PoS blochchain implementations suffer from the nothing-at-stake problem, which is commonly solved by locking deposits for a long period, we have encountered no appropriate blockchains except Dynemix so far.

2) Undue contraction

To trigger contractionary measures, the adversary needs to shrink S below S^*.

Suppose the adversary deposited all coins in his possession, as was described above, and S settled down to S^*. Now, after the adversary instantaneously withdraws his entire deposit, S shrinks significantly below S^*. As I for stakeholders increases, some agents convert their savings into stakes and S restores its targeted size. Unlike the previous scenario, no matter how much resources the adversary possesses, he cannot keep S continuously below S^*, unless he has an opportunity to censor stake transactions on the blockchain.

This leads us to another technical requirement for the underlying blockchain: censorship resilience.

In current blockchain implementations, transactions to be added into a block are selected by the block proposer at his own discretion. Such a design opens the censorship opportunities and thus allows the adversary to control the size of the stake pool by rejecting deposits of other stakeholders, which can undermine the effectiveness of our monetary model to a various extent up to rendering it completely impotent.

In Dynemix, we developed a novel block proposal algorithm called Guess My Block, which provides sufficient censorship resilience guarantees and assures that the adversary cannot arbitrarily censor any transactions unless he controls a consensus supermajority.

2. Fractional Reserve Banking

So far, we have been operating without the consideration of credit money. Due to the properties of blockchains, we cannot endow any specific actors with the authority to issue new coins. Otherwise, the decentralized nature of the blockchain will be compromised. We can, however, conceptualize a model of a fractional reserve banking via a smart contract.

Suppose we added a smart contract that endows certain actors that can be appointed by a certain authority with the power to create tokens of a special class. Suppose we grant a CB the power to issue and void “licences” for the token issuance. Issued tokens are pegged to the native coins of the system and the CB takes on liabilities to control the exchange rate and keep it $1:1$. New tokens circulate alongside with native coins and are used as an equal legal tender within the country.

This setup creates prerequisites for credit money. With its adoption, banks can pay an interest on money deposited to their accounts and use the accumulated reserves to lend newly created tokens. The reserve requirement constrains the expansion of credit in the same way as in conventional economies.

Under such conditions, the transmission scheme will change. Since credit interest rates are related to the interest rate for minters, the expansion or contraction of credit will impact the balance between the demand for money and the available supply, which will shift the interest rate and provoke respective measures from the algorithm. A mass adoption of credit money or other derivatives may require adjustments of the algorithm, but the fundamentals will stay intact, and the system should function properly in the transformed setting.

3. Islamic-Friendly Monetary System.

Islamic religious law called Shariah prohibits any interest on money. For that reason, the conventional financial system, which is based on credit, cannot be adopted by Islamic governments on the full scale.

Fractional reserve banking allows for the circulation of credit money and thus secures endogenous control of the money supply, which contributes to price stability. The circulation of credit money allows CBs to use interest rates as the main channel of the monetary policy. In the absence of market interest rates, Islamic governments must rely on different channels, such as the Islamic banking lending channel and the exchange rate channel. Conducting an efficient monetary policy under such conditions is a challenging task, and many countries that adopted Islamic banking permanently experience economic difficulties.

The proposed solution, however, is fully compliant to Shariah principles and allows building a full-scale monetary system capable of targeting required economic indicators. The key feature of our approach is that, unlike the conventional system, we do not rely on credit money, and credit in general is factored out. Our model works in a similar way in the presence of both Islamic and conventional banking.

The interest that stakeholders receive in our system, although having been described as an interest on money for simplicity, is actually a payment for a service. Due to the design of blockchains, stakeholders do not lend their coins to third parties, and their funds stay in their sole possession regardless of being staked or free. The reward they receive is a payment dispatched by the system itself for creating blocks and assuring the system's security.

VI. Conclusions

a) **We created a model of the first decentralized algorithmic central bank.**

Since the creation of Bitcoin, there were multiple attempts to address the problem of volatility in crypto economies. Unlike previous projects, which were devoted to the development of a so-called "stablecoin", we took a step further and created an asset than can not only follow the exogenous course by being pegged to allegedly stable off-chain assets but sustain a targeted equilibrium endogenously.

We can incorporate our variation of a feedback policy rule similar to the Taylor or McCallum rules with a targeted r^* to create a functional stable economy that satisfies the needs of all participants and turns our model into a fully-fledged "decentralized algorithmic central bank".

b) **Our model is completely independent and decentralized.**

All previous attempts of creating a so-called "stablecoin" featured a common downside: no matter how sophisticated the solutions were, they always relied on external sources and were pegged to exogenous assets.

Our solution makes a major breakthrough by introducing a concept that relies exclusively on on-chain data, is fully algorithmic, and is not related to any particular off-chain asset (USD, gold, SDR etc.) Instead, our model operates in conjunction with the entire global economy.

c) **Our model doesn't require any ancillary assets unlike algorithmic stablecoins.**

Currently available algorithmic stablecoins operate with a sort of open market operations: a special asset is exchanged for native coins when a contraction is needed and repurchased back as a part of expansionary measures.

The design of such assets endows them with the properties of securities, which puts the system under the control of regulators, creates significant legal obstructions, and severely undermines decentralization.

Our algorithm operates directly with native utility coins, which allows us to avoid all the respective difficulties occurring with the introduction of ancillary assets, including sanctions from financial regulators.

d) **Our model is highly egalitarian.**

We managed to create a model that will embody the ideas of fair egalitarian wealth distribution. With the help of helicopter coins, our model impedes the concentration of power and doesn't allow strong actors to sustain their influence endlessly simply by staking all their coins and increasing the relative share in possession.

Since banks and credit are removed from our monetary model, strong financial actors can no longer take direct advantage of a monetary expansion and receive or create money out of thin air. Although governments can still create their own banking systems based on fractional reserve, they can only implement this via derivatives, whereas the underlying layer one blockchain cannot be directly affected by their actions.

e) **Our model is expected to be more efficient than the conventional discrete model.**

The effectiveness of a monetary policy is fundamentally limited by the credibility of a monetary authority. If we assume that future expectations are the main driver of behavior in a rational environment, the vector of economic trends is directed not by a set of conditions observed at any given time but mostly by expected upcoming changes.

In practice, credibility can be a weak point of a monetary policy. Despite being commonly positioned as independent actors, CBs often suffer from governmental interference, which can undermine credibility and render applied measures less effective. The governing boards of CBs can also be affiliated with commercial banks, which further aggravates the issue.

Our model is deprived of that flaw for it is completely decentralized and trustless. There can be no question of credibility or impartiality of an algorithm that is incorporated into a blockchain system, which makes the monetary policy highly efficient in terms of managing expectations and driving the behavior of participants in a desired direction. We can state that we incorporate an efficient flexible policy rule, which solves the problem of time inconsistency as long as other issues.

f) **Our model can seamlessly operate with conventional and Islamic banking.**

Most of the countries that follow Islamic financial doctrine suffer from severe economic difficulties for Islamic banking is not consistent with conventional banking, which is based on credit.

Since our algorithm doesn’t rely on credit, it us fully compliant with Islamic principles and can be adopted on the full scale by Muslim countries, thus solving the problem of seamless integration of the Islamic banking into the global financial infrastructure and allowing to overcome economic difficulties that many of Muslim countries are currently facing.