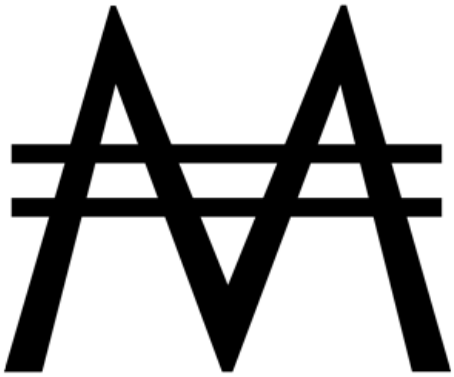

Monetary Protocol

monetarycoin@protonmail.com
www.MonetaryCoin.org

“As some of you may know, my monetary studies have led me to the conclusion that central banks could profitably be replaced by computers geared to provide a steady rate of growth in the quantity of money.” (Friedman, 1976)

Milton Friedman, 1976
Nobel Prize - Economic Sciences (1976)

“Over some periods, measures of the money supply have exhibited fairly close relationships with important economic variables such as nominal gross domestic product (GDP) and the price level. Based partly on these relationships, some economists--Milton Friedman being the most famous example--have argued that the money supply provides important information about the near-term course for the economy and determines the level of prices and inflation in the long run. Central banks, including the Federal Reserve, have at times used measures of the money supply as an important guide in the conduct of monetary policy.

Over recent decades, however, the relationships between various measures of the money supply and variables such as GDP growth and inflation in the United States have been quite unstable. As a result, the importance of the money supply as a guide for the conduct of monetary policy in the United States has diminished over time. The Federal Open Market Committee, the monetary policymaking body of the Federal Reserve System, still regularly reviews money supply data in conducting monetary policy, but money supply figures are just part of a wide array of financial and economic data that policymakers review.” (Board of the Governors of the Federal Reserve System, 2015)

Board of Governors of the Federal Reserve System
What is the money supply? Is it important? (2015)

“So it seems to me it [bitcoin] ought to be outlawed. It doesn’t serve any socially useful function. If the government says 'the reason bitcoin is being used is circumvention,' they could close it down at any moment, and then it collapses.” (Costelloe, 2017)

Joseph Stiglitz, 2017
Nobel Prize - Economic Sciences (2001)

Abstract. MonetaryCoin is compliant with ERC-20 (EIP-20) and has three key features. First, coins are forged via a Proof-of-Stake approach. Second, stakeholders may elect to add (and later delete) personal information to satisfy anti-money laundering, know-your-customer regulations. Third, once fully distributed, the rate of change in the supply of a MonetaryCoin parallels the rate of change in the GDP of a subject country (monetarism). Monetarism's limitations are well understood, and today most central bankers instead apply a variety of tools in pursuit of an inflation target, rather than the simplified money target only. **The coin serves as a simplified alternative to domestic fiat so that residents may select away from the short-run decisions of their central bank while still retaining money tethered to the long-run progress of the national economy.** Because the starting number of coins is capped at not more than 1% of the current M2 per country, MonetaryCoin is designed as a value-added companion to an existing money supply, **not** a replacement.

Table of Contents

1. **Description** 5
2. **Proof of Stake Forging** 5
3. **Endogenous Supply Governance** 8
4. **Elective AML-KYC Compliance** 9
5. **Negative GDP – Mining M5** 9
6. **Money** 10
7. **Positive and Normative Distribution** 11
8. **Currency Nomenclature** 11
9. **Conclusion** 12

Bibliography 13

1. Description

MonetaryCoin is the first cryptocurrency to implement a macro-econometric oracle feature to endogenously govern its own maximum supply once forged (i.e. mined) to an initial limit. A MonetaryCoin will exist for each country that reliably reports GDP and is intended to substitute a small fraction of global money supply so as not to disrupt the ability of central banks to target price stability. The coin functions on proof of stake forging. To satisfy anti-money laundering regulations and laws, such as Know Your Customer (KYC) stakeholders may elect to imbue their personal information into a transaction or to remain anonymous.

2. Proof of Stake Forging

Cryptocurrency mining has two primary functions, security, and distribution. (Spenkelink, 2014)

Security: Bitcoin and Ethereum miners, respectively, invest in specialized equipment to calculate mathematically demanding cryptographic hash functions. This so called "Proof-of-Work" mining provides a practical solution to the classic Byzantine Generals problem (Lamport, Shostak, & Pease, 1982) but comes at the expense of extraordinarily large amounts of electricity and related computing time (Batsaikhan, 2017). MonetaryCoins initially rely on the security provided by miners on the Ethereum public blockchain.

Distribution: Market participants must have a concise and transparent mechanism to calculate the expected return on an investment in pursuit of a cryptocurrency (Sas & Khairuddin, 2017). Without a distribution mechanism designed with some sense of fair-play in mind, it would be difficult to attract a broad audience of stakeholders. MonetaryCoins make use of Proof-of-Stake forging through the mechanism of a smart contract, and later, once Ethereum upgrades to PoS, will operate forging at the protocol level.

In the typical conception of proof-of-stake mining, the probability of generating a valid block is equal to the ratio of a user's balance of funds to the total amount of currency in circulation (Becker, et al., 2013). This approach encourages spending on ownership in the system rather than ownership of specialized computer hardware. The bigger one's stake, the greater one's interest to maintain a secure network. A successful attack would require one to first acquire most of the currency which would be both prohibitively expensive and hard to conceal for a popular system (Apostolaki, Zohar, & Vanbever, 2017).

On the Ethereum network, a new block is generated every 15 seconds on average (ethstats.net, 2018). For every new Ethereum block, a reward of R_{block} is distributed among all the participants of the forging process in proportion to their commitment.

The reward for a participant per block is:

$$\mathrm{R} = \frac{S}{TotalS} R_{Block}$$

Where

S - Number of tokens committed by the user (stake)

R_{Block} - Reward per block

TotalS - Number of tokens allocated by all the users (total stake)

The total stake will change over time, to calculate the exact reward, the ratio $\frac{S_i}{S_{Total}}$ needs to be calculated per block:

$$R^n = \sum_{i=1}^{n} \left(\frac{S}{TotalS_i} R_i \right)$$

Where

R^n - The reward for n blocks of forging

S - Number of tokens committed by the user (stake), constant during the whole process

$TotalS_i$ - The total stake on block i

R_i - The block reward on block i (might change as result for GDP change)

This method allows more equitable distribution of tokens to individuals over an extended period. In a system that allows the users to commit tokens for forging and withdraw every block, all the tokens will be used for mining all the time. However, PoS mandates that money designated explicitly for investment should be rewarded and not money used for daily transactions. Therefore, forging in the MonetaryCoin system will start to produce gains only after committing the stake for *c* blocks.

The adjusted reward for token dedication for n blocks of mining will be calculated by the formula:

$$R^n = \sum_{i=c}^{n} \left(\frac{S}{TotalS_i} R_i \right)$$

$$for\ n \geq c$$

Where

C - The number of blocks before mining gains. A constant to represent *the commitment of time*

Naturally, the user might decide to withdraw the stake before waiting for *c* blocks. In this case, the user will get the stake back without the additional mining reward. All coin generating mechanisms bear imperfections, our objective is to seek the most equitable normative balance between the interests of forgers and users while preserving incentives on all sides.

When implementing this scheme on a public blockchain such as Ethereum, every transaction requires a fee payment. The fee paid by the user to the miners maintains the network. The user is required to pay a fee both for commitment and withdrawal of funds from the PoS forging mechanism, this payment is marked by ϕ_1, ϕ_2 (paid in Ether) and will serve as a substitute for *the commitment of time*. Mining gains will start from the first block (as if $C = 1$).

On chain calculations:

In order to distribute the mining gains in a trustless manner, the reward calculation should be done on-chain. However, the calculation of an exact result will require the storage of the entire history of commitments and withdraw of all users on chain, and writing to storage is the most expensive blockchain operation. So, we reduce the need for an on chain-storage by smoothing the result using linear approximation:

Instead of calculating

$$R^n = \sum_{i=1}^{n} \left(\frac{S}{TotalS_i} R_i \right)$$

We will substitute the per-block stake calculation with:

$$\overline{S} \equiv (S_1 + S_n) / 2$$

And block reward per-block calculation with:

$$\overline{R} \equiv (R_1 + R_n) / 2$$

During withdraw, the reward will be calculated using:

$$R^n = \frac{n \times S}{\overline{S}} \overline{R}$$

$$For\ \overline{R} > 0$$

Where

R^n - The reward for n blocks of forging

This substitute maintains all the key properties of the original formula while drastically decreasing storage requirements and user fees.

3. Endogenous Supply Governance

Once fully mined, the rate of change in the available forging supply of a MonetaryCoin parallels the rate of change in the GDP of a subject country. Monetarism is widely recognized as a vital but incomplete guide to central bank policy (Williamson, 2012). However, a simple central bank rule-based companion currency may offer normative benefits for domestic residents – provided that companion currency exists in the shadow of a dominant fiat currency managed for price stability. MonetaryCoins are therefore limited to 1% of M2 (or equivalent[1]) in each country, before programmatic GDP based adjustments to the supply of coins available for forging.

Where the maximum number of coins available for forging is adjusted quarterly such that

$$\Delta S_n = S_{n-1}\left(\frac{GDP_n}{GDP_{n-1}} - 1\right)$$

Where

GDP - quarterly revised GDP for the period

S - The cap on the total number of coins in the subject country MonetaryCoin system (supply)

The initial implementation of MonetaryCoin will peg the quarterly growth rate of GDP to the trailing twelve-month average of GDP; we expect to then introduce the oracle feature in an upgrade performed in advance of the first system-wide quarterly update (i.e. within 90 days of launch).

Money Supply Oracles:

Country	**Ticker**	**Oracle***	**Source**
USA	MUSA	M2	Federal Reserve
Eurozone	MERO	ECMSM2	European Central Bank
Japan	MJPN	JMNSM2	Bank of Japan
UK	MUK	UKMSVQWU	Bank of England
Australia	MAUS	AUM3	Reserve Bank of Australia
New Zealand	MNZ	NZMSNAM1	Reserve Bank of New Zealand
Canada	MCAN	MSCAM2	Bank of Canada
Switzerland	MSWI	SZMSM2	Swiss National Bank
China	MCHI	CNMSM2	The People's Bank of China
Hong Kong	MHK	HKM3TL	HK Monetary Authority
Norway	MNOR	NOMSM3	Statistics Norway
Sweden	MSWE	SWMSM2	Sveriges Riksbank
Denmark	MDK	DKMOM3	Danish Central Bank
South Korea	MKW	KOMSM2	Bank of Korea
UK	MUK	UKMSVQWU	Bank of Japan
Australia	MAUS	AUM3	Reserve Bank of Australia
New Zealand	MNZ	NZMSM3	Reserve Bank of New Zealand

[1] Oracle tickers drawn from Bloomberg LP. For example, Australia reports M1 and M3, with M3 closer to the M2 measure we apply for other countries. The UK reports M0 through M4, and so in this case M3 is the relevant metric.

GDP Oracles:

Country	Ticker	Oracle	Source
USA	MUSA	GDP CUR$	Bureau of Economic Analysis
Eurozone	MERO	ENGCEMU	Eurostat
Japan	MJPN	JGDOOGDP	Economic and Social Research Institute Japan
UK	MUK	ENGCUK	Eurostat
Australia	MAUS	AUGDPCY	Australian Bureau of Statistics
New Zealand	MNZ	NZNTNOM	Statistics New Zealand
Canada	MCAN	CGEBCNGD	STCA - Statistics Canada
Switzerland	MSWI	SZGSGDP	State Secretariat for Economic Affairs
China	MCHI	CNNGPQ$	National Bureau of Statistics of China
Hong Kong	MHK	HKGCGDP	Census and Statistics Department, Hong Kong
Norway	MNOR	NOGDP	Statistics Norway
Sweden	MSWE	SWGCGDP	Statistics Sweden
Denmark	MDK	DEGDPCN	Denmark Statistics
South Korea	MKW	KOEGTOT	Bank of Korea
USA	MUSA	GDP CUR$	Bureau of Economic Analysis
Eurozone	MERO	ENGCEMU	Eurostat
Japan	MJPN	JGDOOGDP	Economic and Social Research Institute Japan
UK	MUK	ENGCUK	Eurostat
Australia	MAUS	AUGDPCY	Australian Bureau of Statistics

4. Elective AML-KYC Compliance

Stakeholders may elect to add or subtract personal information to a MonetaryCoin address to satisfy anti-money laundering, know-your-customer regulations (AML-KYC). The addition of name, address, tax or national identity number is achieved through the mechanism of a smart contract that requires minimal Ethereum gas. It then falls to the receiving party to verify the accuracy of the information. Most parties insisting on AML-KYC are regulated financial institutions with processes and resources in place to record and verify such data.
The AML-KYC data are not visible on the blockchain because they are encrypted and stored off-chain. This feature reduces the potential network drag caused by each address carrying increasing amounts of otherwise irrelevant AML-KYC data. A hash of the AML-KYC data is stored on the blockchain but only the recipient address owner can attach the hash to the off-chain data and decrypt its content. This reduces the risk of exposing sensitive information to unrelated parties. For completeness, a sender may abandon its wallet address and create a new one after the transaction.

5. Negative GDP – Mining M5

MonetaryCoins hold level their supply with the help of forgers if the economy of a subject country contracts and the currency has been otherwise fully forged. If all coins have not yet been fully forged then the cap on the total possible coin count remains constant. The features and benefits of the macroeconomic link to GDP, like many macroeconomic phenomenon, are primarily relevant only at the margin.

Once fully mined, in a down GDP year, market participants may continue mining in return for "M5" coins that are redeemable for normal coins once GDP growth recovers to permit the issuance of more money. Critically, to mine an M5 coin requires a stakeholder to temporarily cede the ability to transact a regular coin. M5 coins carry the same name as the domestic coin but with the suffixM5. M5 is treated the same as a normal coin for purposes of mining efficiency once the economy has returned to growth and new coins are available for issuance. *At the time the reward for use of an M5 coin is withdrawn, the M5 coin is then burned and its corresponding normal coin is released for spending.* This process is intended as a crude analog to what happens when market participants buy and sell government bonds instead of leaving their cash in banks to be lent and recycled through the economy.

Forgers must be provided incentive to participate in the network while at the same time not inadvertently introducing coins that otherwise decouple MonetaryCoin from its macro-econometric tether. This mechanism is designed to push the percentage expansion or contraction in money supply into line with the percentage expansion or contraction in GDP - while minimizing deviation. M5 coins are not AML KYC compliant and are tradable once per year at normal cost and at 100x the normal cost thereafter inside the trailing twelve-month period.

We expect M5 coins to price at a significant discount to domestic MonetaryCoins. That discount would reflect some implied interest rate tied (1) reduced liquidity (2) the marginal cost of mining, and (3) the market's belief about the timing and magnitude of the return to GDP growth.

The issuance of M5 coin in a GDP downturn may offer a superior normative result compared to simply shrinking the blockchain currency outright. Issuing coin, even coin of far lower value, is nonetheless stimulatory, however small, relative to the total supply of fiat. If the proof of any pudding is in the eating, we'll know very quickly if the tradeoff between this forging mechanism and its inadvertent (likely immaterial) expansionary effect on money supply has any drawback**s.**

6. Money

MonetaryCoin meets the three standards for money: medium of exchange, unit of account, and store of value, respectively (Mankiw, 2015). The Ethereum network provides a secure medium of exchange. The unit of account is consistently expressed through a wallet and as a store of value the units of currency only increase if the size of the corresponding economy increases and forgers have incentive to participate.

Money has been Tiger Balm, cigarettes or even giant, immobile, rocks (Gillilland, 1975). Lately, money is cryptocurrency. To link a cryptocurrency to an econometric measure such as GDP encourages reduced foreign exchange volatility by tethering an otherwise hyperactive asset market to a sluggishly adjusting market for goods and services (Dornbusch, 1976).

The Monetarist's equation of exchange (Mill, 1848):

$$M \times V = P \times Y$$

Where M is the quantity of M1, V is the velocity of M1, P is the price level, and Y is the real output of the economy. Velocity is the average number of times a dollar is spent in a given year

on the purchase of final goods and services. M1 is defined as the sum of currency held by the public and transaction deposits at depository institutions (which are financial institutions that obtain their funds mainly through deposits from the public, such as commercial banks, savings and loan associations, savings banks, and credit unions) (Board of the Governors of the Federal Reserve System, 2015).

By assuming that velocity is stable, one transforms the equation of exchange into the quantity theory of money. This equation tells us that any change in M1 will impact P × Y. Changes in the money supply are the dominant forces that change nominal GDP (P × Y). It is not surprising, therefore, that monetarists view control of the money supply as the key variable in stabilizing the economy. However, monetary velocity has been unstable since the 1980s in the United States (Rasche & Williams, 2005) and primarily for this reason, Monetarism is viewed as part of the evolution of modern macroeconomic thought and not its culmination.

If a country had the same amount of cash in circulation today as it had in 1976, when Milton Friedman won the Nobel Prize, many stores would have nothing in their registers to facilitate purchases. Visualize a grocery store with rows of abandoned checkout lanes. Fortunately, if a central bank grows the supply of money with the rate of economic expansion, that economy avoids running out funds for transactions.

All else equal, even at 3% inflation a central bank claims 0.25% of the spending power of cash per month from bank depositors, unless the underlying economy that plays host to the banking system expands activity by that same 0.25% per month. Money holders fear having value stolen even if securely deposited in a bank; their time lost. That fear is so great that to rid an economy of the psychological expectation of inflation requires the central bank to undertake a set of contractionary economic policies. Like positive encouragement, adding money can boost output to a point, but after a while agents start to disbelieve its sincerity. The restoration of central bank credibility carries real costs borne by domestic residents.

It is the job of the central bank and the fiat currency to promote price stability, maximum employment and moderate long-term interests rates (The Federal Reserve System Purposes & Functions - Section 1). That means targeting price stability (i.e. low inflation) to maintain credibility. MonetaryCoin's role is to track the second order effect of these decisions, and all other factors affecting output (fiscal policy etc.) through the mechanism of the change in GDP only.

7. Positive and Normative Distribution

To prime the PoS forging pool, 10% of each of the first two 2 currencies will be available for barter in return for Ethereum at www.monetarycoin.org in 2018. Any coins allocated to a release but not otherwise distributed will be returned to the forging pool.

8. Currency Nomenclature

Country	**MonetaryCoin**	**Ticker**
United States	MonetaryCoinUS	MUSA
Euro	MonetaryCoinEUR	MERO
Japan	MonetaryCoinJPN	MJPN
UK	MonetaryCoinUK	MUK

Australia	MonetaryCoinAussie	MAUS
Canada	MonetaryCoinCanada	MCAN
Swiss	MonetaryCoinSwiss	MSWI
China	MonetaryCoinChina	MCHI
Sweden	MonetaryCoinSweden	MSWE
Hong Kong	MonetaryCoinHK	MHK

9. Conclusion

Technology may be used to improve money without disrupting the ability of responsible central banks to use monetary policy to target price stability, and secondarily, full employment. If a currency ties to an econometric statistic(s), central bankers and economists ought to be able to develop predictive models that may help guide central bank policy decisions as cryptocurrency adoption rises to a responsible limit.

Bibliography

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. *arXiv: Networking and Internet Architecture*, 375-392. Retrieved 5 16, 2018, from https://arxiv.org/abs/1605.07524

Batsaikhan, U. (2017). Cryptoeconomics – the opportunities and challenges of blockchain. *Policy briefs*. Retrieved 5 16, 2018, from https://ideas.repec.org/p/bre/polbrf/21169.html

Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P., & Böhme, R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, R. Böhme, & R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 135-156). Berlin: Springer. doi:https://doi.org/10.1007/978-3-642-39498-0

Board of the Governors of the Federal Reserve System. (2015, December 16). *What is the money supply? Is it important?* Retrieved from The Fed: https://www.federalreserve.gov/faqs/money_12845.htm

Costelloe, K. (2017, November 29). *Bitcoin 'Ought to Be Outlawed,' Nobel Prize Winner Stiglitz Says*. Retrieved May 16, 2018, from Bloomberg: https://www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd

Dornbusch, R. (1976). Expectations and Exchange Rate Dynamics. *Journal of Political Economy, 84*(6), 1161–1176. Retrieved 5 16, 2018

ethstats.net. (2018, May 16). *Ethereum Network Status*. Retrieved from https://ethstats.net/: https://ethstats.net/

Friedman, M. (1976, December 10). *Milton Friedman - Banquet Speech*. Retrieved May 16, 2018, from Nobel Prize: https://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/1976/friedman-speech.html

Gillilland, C. L. (1975). *The Stone Money of Yap. A Numismatic Survey. (Smithsonian Studies in History and Technology 23).* Smithsonian Institution Press. Retrieved 5 16, 2018

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems, 4*(3), 382–401. Retrieved 5 16, 2018, from http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf

Mankiw, N. G. (2015). Macroeconomics. In N. G. Mankiw, *Macroeconomics* (9, illustrated ed., pp. 22–32). New York, New York, United States of America: Macmillan Learning.

Mill, J. S. (1848). *Principles of Political Economy.* John W. Parker Publisher. Retrieved 5 16, 2018, from http://eet.pixel-online.org/files/etranslation/original/Mill,%20Principles%20of%20Political%20Economy.pdf

Rasche, R. H., & Williams, M. M. (2005). The Effectiveness of Monetary Policy. *Canadian Parliamentary Review*, 447-490. Retrieved 5 16, 2018, from https://research.stlouisfed.org/wp/2005/2005-048.pdf

Sas, C., & Khairuddin, I. E. (2017). *Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users*. Retrieved 5 16, 2018, from https://dl.acm.org/citation.cfm?id=3025886

Spenkelink, H. (2014). *The Adoption Process of Cryptocurrencies - Identifying factors that influence the adoption of cryptocurrencies from a multiple stakeholder perspective*. Retrieved 5 16, 2018, from http://essay.utwente.nl/65677

The Federal Reserve System Purposes & Functions - Section 1. (n.d.). Federal Reserve. Retrieved 5 16, 2018, from http://www.federalreserve.gov/pf/pdf/pf_1.pdf

Williamson, S. D. (2012). Liquidity, Monetary Policy, and the Financial Crisis: A New Monetarist Approach. *The American Economic Review, 102*(6), 2570-2605. Retrieved 5 16, 2018, from http://pubs.aeaweb.org/doi/pdfplus/10.1257/aer.102.6.2570