The Second Coming of Money

A Discussion on Reviving the Ideals Surrounding the Bitcoin Revolution

K. Kayra Banak

October 2024

Abstract

Bitcoin, originally envisioned as a decentralized alternative to fiat currency, has largely failed to fulfill its promise due to issues like speculative volatility, mining centralization, and deflation. While stablecoins were introduced to counter volatility, most rely on fiat backing or centralized systems, compromising decentralization. This paper explores the shortcomings of Bitcoin and stablecoins, proposing a new model for a truly decentralized stablecoin. The proposed coin would balance stability, privacy, and eco-friendliness without pegging to external assets. By implementing a novel consensus mechanism, flexible supply management, and democratized decision-making, this stablecoin could offer a sustainable and accessible alternative to existing cryptocurrencies, designed for daily transactions.

1 Introduction

Bitcoin was supposed to change the world. Born out of the 2008 financial crisis, it promised a new era of decentralized currency, free from the grips of central banks and governments. The idea was revolutionary: money that wasn't tied to any single entity, borderless and open for anyone to use. It represented a financial system built on privacy and decentralization. As money digitized around the world, the potential future of total monetary surveillance was seeming more probable by the day (Giannakoudi 8–10). Bitcoin promised to counter that shift as a system built on privacy and true decentralization. The Second Coming of Money was afoot.

However, as time passed, Bitcoin veered away from its potential as an alternative to money. Its fixed supply and deflationary nature pushed the idea that Bitcoin was a speculative investment tool, rather than a genuine alternative to fiat money (Tut). Many cryptocoins tried to recreate their own "Bitcoin Moments", aiming for instances of sudden and radical deflation and investment rather than actually posing an alternative to fiat money.

Although stablecoins emerged as a response, attempting to offer a solution by tying digital currencies to stable assets like the US dollar, they came with their own sets of drawbacks. Most notably, they couldn't promise the same

decentralization that Bitcoin brought forth (Mita et al. 4). Many stablecoins are either backed by fiat or centralized institutions, raising concerns about their ability to truly stand apart from extant financial systems that Bitcoin sought to disrupt.

What would a truly decentralized stablecoin look like? Could there be a solution that combines the stability of stablecoins with the decentralization ideals of Bitcoin? This article explores the shortcomings of major cryptocoins including some stablecoins, and proposes a new model—a stablecoin that balances decentralization, stability, eco-friendliness, and accessibility in a way that no cryptocurrency has achieved thus far.

2 The Ideals Surrounding Bitcoin

Bitcoin emerged from a simple idea: a purely peer-to-peer electronic cash that would allow online payments to be sent directly from one party to another without going through a financial mediating institution (Nakamoto 1). What Satoshi Nakamoto aimed for with Bitcoin was quite clear: a digital cash that achieved privacy and decentralization while still being as open as possible about its mechanism and transaction history. Revisiting the ideals that shaped Bitcoin's inception and how it set out to achieve them is crucial to understanding where Bitcoin fell short in its goals.

2.1 Decentralization

:At the heart of Bitcoin's creation lies decentralization. Through the proof-of-work (PoW) system, Nakamoto managed transactions to be validated not by a central entity but by participants of the blockchain itself. This not only helped decentralize the system, but it also made sure attacks on the Bitcoin blockchain were not profitable as they required ownership of a majority of the total CPU power within the blockchain's structure.

2.2 Privacy

:Another staple of Bitcoin was the privacy it aimed to offer. Transactions in the blockchain are pseudonymous, users are only identified by their public keys. In contrast, in traditional banking the privacy cutoff is achieved through trusted third-parties (banks) not revealing information about transactions to the public. The Bitcoin public key system generates transactions that are cut off from the identities of the users, and doesn't rely on intermediaries to uphold privacy.

2.3 Offering an Alternative to Fiat Money

:The buzzword behind Bitcoin was "digital cash". As digital banking grew and money became more digitized, concerns about privacy and centralization were being raised and a digital currency as private as physical cash was understood to be necessary. Bitcoin was created with the goal of satisfying that necessity.

3 Bitcoin Fails

Over the years, Bitcoin encountered countless challenges that hindered its ability to hold onto its revolutionary promise. Centralization slowly started to take place in the mining process, companies and algorithms against Bitcoin's private nature gained power, and most significantly, Bitcoin's sudden deflation damaged cryptocoins' perception for years to come, with most people seeing them as a "cheat code into riches". This affected the future intentions and outcomes of all cryptocoins post-Bitcoin.

3.1 Mining Centralization

While Bitcoin's PoW system was designed to be decentralized, over time the mining process has become increasingly centralized. Large mining pools and specialized mining hardware (ASICs) have made it difficult for average users to participate in the validation process. As of today, the majority of Bitcoin's total hash rate is controlled by a few large mining pools (Adeniyi). Centralization of the mining process threatens Bitcoin to the core, as a 51% attack becomes more feasible with fewer entities controlling validation power.

3.2 Blockchain Analysis Systems Against Privacy

Despite Bitcoin being pseudonymous, the transparency of the blockchain allows for transaction tracking, and companies have developed tools to link public addresses with real-world identities (Kuzuno and Karam). The rise of blockchain forensics firms like Chainalysis has allowed law enforcement agencies to trace activities and identify users.

3.3 Bitcoin Creation Cap and Deflation

One of the most unique features of Bitcoin is its creation cap. The creation of Bitcoin is linked to the amount of blocks validated, and the rewards given out for block validation. Every time the amount of Bitcoins needed to reach 21 million is halved, the rewards are halved with them. This approximately corresponds to rewards being halved every 4 years. With Bitcoin creation exponentially slowing down, there will never be more than 21 million Bitcoin. This simulated scarcity increased demand, and made Bitcoin into "digital gold". Bitcoin's price skyrocketed, and it became a store of value currency, rather than one to use for daily transactions.

As Bitcoin's value as an investment tool rose, its vulnerability and instability became noticeable. In less than fifteen years, Bitcoin experienced seven crashes that each caused an over 50% drop in value. Some of these shocks were caused by nothing but a few words out of Elon Musk's Twitter account, or anti-Bitcoin measures taken by China, undeniably confirming for the entire world that Bitcoin had become a speculative currency (Lisa).

Bitcoin's demise was not necessarily seen as a failure by cryptocoin enthusiasts, in fact, as Bitcoin became a speculative investment tool and morphed into a buzzword in mainstream media, other cryptocoins arose to achieve similar "success". The primary goal of the cryptocurrency movement shifted from creating digital cash to chasing sudden deflationary movements and generating price bubbles that drew investment and popularized the new coin. Nonetheless, for both commercial and idealistic reasons, stability in the crypto landscape was still needed, which birthed the rise of stablecoins.

4 Stablecoins

Stablecoins are cryptocoins that aim to counter the volatility of classic cryptocoins. Some of them offer easier daily transactions, while some offer to be a bridge between volatile cryptocoins and fiat money. They achieve their stable prices by three different measures. Pegging the coin to fiat money or any other material asset, pegging it to another cryptocoin, or using algorithms that aim to keep the coin's price stable.

4.1 Fiat-Backed Stablecoins

Fiat-backed stablecoins are pegged to fiat money, or baskets of different fiat currencies. These coins, while still blockchains, lack the decentralization of other cryptocoins, since they are technically tied to real life monetary entities such as governments or banks. USDT, for instance, is linked to the US dollar, meaning it's vulnerable to US monetary policy and regulatory changes, making true decentralization impossible. These coins usually function as transactional middle-men between fiat money and cryptocurrencies (Hampl and Gyönyörová 235). Over time, different governments or companies have created their fiat-backed stablecoins which are often used as tools for mass surveillance, collecting and centralizing transaction data, undermining privacy.

4.2 Crypto-Backed Stablecoins

Instead of fiat money, some stablecoins are pegged to other cryptocoins. These coins usually require over-collateralization in order to counter the volatility of their pegged cryptocoins. This makes them harder to use for daily transactions, and less popular in the market.

4.3 Floating Stablecoins

There are few stablecoins that function without any pegs and only through algorithms that aim to keep the coins price stable. The most influential and well-known floating stablecoin to this date was Terra(UST), which collapsed in 2022.

Terra was an ambitious project in the cryptocurrency space, aiming to create a stablecoin that maintained a peg to the USD through its sister currency,

LUNA. The Terra ecosystem sought to facilitate seamless transactions and foster economic growth by offering a decentralized and scalable stablecoin solution. However, its structure and mechanisms revealed significant flaws that ultimately led to its collapse.

While Terra positioned itself as a decentralized stablecoin, the reality was quite different. The relationship between Terra and LUNA was designed to maintain the peg through a mechanism known as "seigniorage," where LUNA could be minted or burned to balance the supply of Terra. This system relied heavily on the demand for LUNA and the ability to manage its market value effectively. However, the concentration of LUNA's holdings among a small number of wallets meant that the project was susceptible to manipulation by large stakeholders, undermining the ideal of decentralization.

Terra's collapse came to a head in May 2022, when the algorithmic mechanisms that linked Terra to LUNA failed to maintain the dollar peg. As the market began to panic and sell off Terra, the resulting drop in its value led to a cascading effect, drastically reducing the price of LUNA as well. This situation was exacerbated by the fact that the minting of new LUNA tokens did not create sufficient demand to stabilize the system, leading to an over-supply of tokens and further eroding confidence in both currencies. Ultimately, the failure of Terra marked a significant moment in the crypto landscape, highlighting the risks associated with algorithmic stablecoins and the fragility of reliance on speculative models to achieve stability.

5 An Economics Approach to a Computer Science Problem: Imagining a Truly Decentralized Stablecoin

Since the abandonment of the gold standard in 1971, money hasn't been pegged to anything but trust in governments. Governments around the globe abandoned the gold standard because it created volatility, deflation, and lots of monetary limitations. The standard was put in place to make sure countries had an objective method of being measured fiscally. A cryptocoin doesn't require a peg to justify its value, it only needs to alway be able to pay off those who exit the ecosystem. However, trying to create a stablecoin by pegging it to other assets brings forth the limitations of the gold standard, and with its increased volatility in contrast with fiat money, the coin eventually collapses. However, all that a cryptocoin needs to be used as a daily coin is trustworthiness, some level of stability without necessary pegs to fiat money, and ease of use. Instead of coming up with complex algorithms that try to account for volatility, simple economic ideas could be taken into account when creating the coin.

5.1 Decentralization and Democratization

The new digital cash should be decentralized far from any single human or group's initiative. It should be as algorithmic as possible in its functioning, acting like a living organism. Whenever human intervention is necessary, it should be as democratic as possible and include all users of the currency in the decision-making process.

In that sense, Proof of Stake is not a decentralized or democratic mode of functioning for the coin. It gives decision-making and economic power to the biggest wallet, which would in time centralize and create immense power inequality between users.

5.2 Privacy

As with any other cryptocurrency, privacy should be a main concern of a stablecoin. Its new proof and transaction systems should be private and safe.

5.3 Ease of Use and Entry

Much like cash, the stablecoin of the future should be easy to enter and easy to use. It should be made clear that the main function of this coin is daily use, and it should be completely functional even with the most basic of devices, and with little understanding of computer science. This requires that the validation process of the coin consist of light computing.

5.4 Accounting for Supply-Demand Dynamics

What causes volatility in a currency is supply and demand dynamics. Scarcity and high demand create deflation, while abundance and low demand create inflation. Bitcoin's creation cap limited its supply, and with sudden increase in demand the coin radically deflated.

Without a cap however, an algorithmic cryptocoin has more power against volatility than a government ever did considering its ability to "burn" coins. In addition, with Bitcoin and most other cryptocoins, mining rewards acted as a driving force of demand, which made the coins inherently deflationary. A coin aiming to become digital cash shouldn't tie its supply mechanism to its transactions so intrinsically and directly, as otherwise it loses its biggest asset against volatility.

5.5 Eco-Friendliness

The digital alternative to cash would have to be free of any caps to make sure supply can match demand at any time, but with Proof of Work as the decentralized validation method, some questions of eco-friendliness arise. As seen with Ethereum, a cap-free Proof of Work cryptocurrency uses incredible amounts of computing power to function, and incentivizes mining farms that emit gigantic

amounts of greenhouse gasses. With both Proof of Stake and Proof of Work discouraged, the currency would have to function with a unique proof system.

6 Implementation Ideas

To achieve all of its goals, the coin would need a couple of functions that are unique to its system: A new proof system, anti-volatility measures, protocols to make sure privacy isn't sacrificed, and a unique app with an easy-to-use interface.

6.1 Proof of Velocity

As an eco-friendly and decentralized proof system that supports using the coin for daily transactions, Proof of Velocity proves quite simple. Proof of Velocity would choose its validators through a weighted lottery between a group of nodes that have used over a threshold ratio of the coins they own in transactions in a set time. Different thresholds and "Reciprocal Reputation" would add to the weighting of the lottery. Even mobile devices could be validators, and in case they fail to validate in a given time their delegated full node would validate in their stead. In order to make sure even mobile devices can be validators, the system would work in a regional hierarchy.

6.1.1 Regional Blocks

To keep the number of nodes that need a constant flow of information small, local nodes (mobile devices) would only write a block of all transactions that have occurred in their "region". These regions would be defined by the "Fluid Regions Protocol". The local node, chosen through PoV, would validate the block and send it to all local and general nodes. The general nodes would then be chosen through PoV to validate the global block and cross-reference interregional transactions that are recorded in both blocks.

6.1.2 Dynamic Thresholds and Rewards

Each validation would be rewarded through the minting of a number of new coins. The number would be tied to the velocity of the coin economy. If the economy is getting too fast, which would create inflation, the PoV thresholds and validation rewards would minimize, the reward even falling to near-zero numbers. If the economy is getting too slow, validation rewards would maximize and PoV thresholds would rise. This way, the coins algorithm could better incentivize or disincentivize spending to control volatility.

6.2 Fluid Regions Protocol

In order to keep regional blocks from jeopardizing privacy, regions could shift with every validation. Regions would be pseudo-geographic, in the sense that

the protocol would generally keep regularly interacting nodes together, however the regions wouldn't be necessarily geographic and could geographically overlap with one another. Each region would have the same amount of users in it, and the "borders" of the region -the nodes in each region- would slightly shift after every validation to make sure the geographic or personal information of the users aren't at risk of being exposed.

6.3 Reciprocal Minting Framework

In another way to minimize major supply-demand shifts and decrease volatility, the coin would work in a "Reciprocal Minting Framework". This stands for the 1:1 minting and burning of coins with each entry into and exit from the coin's ecosystem. When $100 worth of coin is bought through the app, $100 worth of coin would be minted and attributed to the buyer's wallet. When $100 worth of coin is exchanged into fiat through the app, all of those coins would be burned.

These blockchains also enable DeFi, or Decentralized Finance through the use of smart contracts. By enabling globally accessible, low cost, decentralized and transparent finance, they challenge traditional banking. Blockchains draw from the ideals of peer-to-peer connections and decentralization, and their entropy challenges to drastically alter the material world.

6.3.1 Reputation of Reciprocal Mints

If reciprocal minting validations were to be rewarded, that would change the ratio of newly minted coins to fiat money from 1:1. However, validating new entries or exits along with other transactions would threaten the private nature of the coin and risk deanonymization. Therefore, reciprocal mints and burns should be validated separately, unrewarded. Instead of rewarding reciprocal transaction validations directly, the system could reward them by putting a reputation system in place that changes the odds of being chosen as validator for intracoin transactions.

In the earlier days of the coin's launch, most validations would be RMF validations, therefore some rewards would be given out until a set date through the use of an algorithmic monetary entity.

6.4 Algorithmic Monetary Entity

The algorithmic monetary entity would work as a central bank. It would have complete control of the bank accounts that handle fiat-to-coin transactions, it would handle dynamic thresholds and rewards, and it would manage the initial RMF validation rewards given out during the early days of the coin. The RMF validation rewards can be backed by an initial investment in the system.

7 Conclusion

The proposed cryptocurrency builds upon Bitcoin's original vision while addressing its major shortcomings: volatility, energy consumption, and centralization risks. At its core is the Proof of Velocity (PoV) system, which balances minting with transaction volume, creating a dynamic supply that adjusts according to economic activity. This ensures stability in times of high and low activity, providing a more sustainable and adaptable alternative to traditional Proof of Work or Proof of Stake systems. Additionally, the introduction of random validator rotation enhances security and prevents manipulation, maintaining the decentralized nature of the network.

The design also incorporates a geographic validation system that decentralizes the process further by distributing responsibility across regional and global nodes. This structure not only reduces the environmental footprint but also makes the system more accessible and easy to use, promoting widespread adoption. The initial coin distribution mechanism through an algorithmic 'coin holder' helps build a fair foundation for the economy, gradually decentralizing control over time and ensuring that early rewards for validators do not lead to long-term monopolies.

In summary, this new cryptocurrency represents a step closer to the ideals of truly decentralized digital money. By addressing the key issues of volatility, centralization, and eco-friendliness, it positions itself as a viable alternative to both fiat currencies and existing cryptocurrencies, providing users with a stable, democratic, and accessible financial system.

References

[1] Adeniyi, Olowoporoku. "Data Shows 50% Of Bitcoin Hashrate Controlled By Two Mining Pools." *Bitcoinist*, 29 Jan. 2023, https://bitcoinist.com/data-shows-50-of-bitcoin-hashrate-controlled-by-two-mining-pools/.

[2] Briola, Antonio, et al. "Anatomy of a Stablecoin's Failure: The Terra-Luna Case." *Finance Research Letters*, vol. 51, Jan. 2023, p. 103358, https://doi.org/10.1016/j.frl.2022.103358.

[3] Flandreau, Marc. *Gold Standard In Theory & History*. Routledge, 2005.

[4] Giannakoudi, Sofia. "Internet Banking: The Digital Voyage of Banking and Money in Cyberspace." *Information & Communications Technology Law*, vol. 8, no. 3, Oct. 1999, pp. 205–43, https://doi.org/10.1080/13600834.1999.9965811.

[5] Hampl, Filip, and Lucie Gyönyörová. "Can Fiat-backed Stablecoins Be Considered Cash or Cash Equivalents Under International Financial Reporting Standards Rules?" *Australian Accounting Review*, vol. 31, no. 3, June 2021, pp. 233–55, https://doi.org/10.1111/auar.12344.

[6] Kuzuno, Hiroki, and Christian Karam. "Blockchain Explorer: An Analytical Process and Investigation Environment for Bitcoin." *2017 APWG Symposium on Electronic Crime Research (eCrime)*, IEEE, 2017, pp. 9–16, http://dx.doi.org/10.1109/ecrime.2017.7945049.

[7] Lisa, Andrew. "7 of the Biggest Bitcoin Crashes in History." *Yahoo Finance*, 13 Sept. 2024, https://finance.yahoo.com/news/7-biggest-bitcoin-crashes-history-180038282.html.

[8] Luther, William J. "Bitcoin and the Future of Digital Payments." *SSRN Electronic Journal*, 2015, https://doi.org/10.2139/ssrn.2631314.

[9] Mita, Makiko, et al. "What Is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems." *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI)*, IEEE, 2019, http://dx.doi.org/10.1109/iiai-aai.2019.00023.

[10] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf, 2008.

[11] Tut, Daniel. *Bitcoin, Speculative Sentiments and Crypto-Assets Valuation*. Elsevier BV, 2024, http://dx.doi.org/10.2139/ssrn.4938749.

[12] Zhu, Kaixiang. "Legal Regulation of Stablecoins." *Beijing Law Review*, vol. 14, no. 03, 2023, pp. 1142–50, https://doi.org/10.4236/blr.2023.143060.