Scientific Research Publishing

Theoretical Economics Letters, 2022, 12, 1559-1565
https://www.scirp.org/journal/tel
ISSN Online: 2162-2086
ISSN Print: 2162-2078

# Trustless, Permissionless, Non-Custodial Stablecoins in Decentralized Autonomous Organizations (DAO)

**Alessio Castello, Gregory Gadzinski**

International University of Monaco, Omnes Education, Monaco
Email: acastello@monaco.edu

**How to cite this paper:** Castello, A. and Gadzinski, G. (2022). Trustless, Permissionless, Non-Custodial Stablecoins in Decentralized Autonomous Organizations (DAO). *Theoretical Economics Letters, 12,* 1559-1565.
https://doi.org/10.4236/tel.2022.126085

**Received:** October 5, 2022
**Accepted:** November 8, 2022
**Published:** November 11, 2022



## Abstract

The benefits offered by cryptocurrencies are a great many: transaction cost and speed, security and transparency, to name a few. Yet, there is also a major drawback represented by their extremely high volatility. Stablecoins offer an ideal solution since they preserve all the advantages of blockchain-based currencies, while reducing considerably the volatility issue. Currently, stablecoins are almost exclusively pegged to the US Dollar and secured by non-crypto assets held in account at custodial institutions. In this article, we present the design of a decentralized organization aimed at issuing stablecoins backed by crypto-assets stored on-chain and pegged to assets different from fiat money. Our model offers several advantages, in particular, it allows the issuance of stablecoins in a trustless, permission-less and non-custodial environment.

## Keywords

Blockchain, Cryptocurrencies, Stablecoins, Decentralized Autonomous Organizations

## 1. Introduction

Among the many questions surrounding cryptocurrencies, valuation emerged very early as one of the most difficult to solve (Cong et al., 2021). Volatility, in particular, has been widely explored in the literature (Ardia et al., 2019; Baur et al., 2018; Corbet & Katsiampa, 2020; Katsiampa, 2017; Phillip et al., 2018) since it constitutes real obstacles to cryptocurrency adoption (Miraz et al., 2022). On the other hand, the benefits offered by cryptocurrencies are undiscussed: transaction cost and speed, accessibility, security and transparency (Schlichting & Pe-

trini, 2019), as well as accelerating the unbundling of payments, credit and banking services (Catalini & Massari, 2021), are all factors that make cryptocurrencies a valuable tool to deliver financial services and increase financial inclusion (Choi, 2021).

Stablecoins represent a solution to mitigate cryptocurrency's volatility while preserving their many advantages (peer-to-peer or cross-border payments, on-chain trading of other digital assets, collateralized lending and other DeFi services), thus making it economically feasible to use them everywhere as "digital currency" fulfilling the usual three functions of money: medium of exchange, means of payment and store of value (Force, 2020).

Unlike cryptocurrencies such as Bitcoin and Ether, a stablecoin can be defined as: "a coin (i.e., one unit of an asset) whose value is stable relative to a reference, which may be some units of another asset or basket of assets or a more abstract reference like purchasing power" (Boltshauser & Seigneur, 2021).

Most of the time, stablecoins are cryptocurrencies that fix ("peg") their value to fiat money such as the US Dollar or the Euro. The stablecoins with the largest market capitalization are USDT, USDC and BUSD[1], which are all pegged to the US Dollar and secured by dollars or dollar-denominated assets of equivalent value held in accounts at regulated U.S. financial institutions.

Recent proposals for stablecoins pegged to assets other than fiat currencies, such as index funds, suggest that, in order to issue a certain amount of stable cryptocurrency, the same amount of the same asset should be held in custody by regulated financial institutions (Ciriello, 2021). These "tokenized" index funds can be seen then as the equivalent of physical Exchanged Traded Funds (ETF) in the blockchain world.

However stablecoins secured by fiat currencies or other financial assets incur a counterparty risk that cannot be easily edged or mitigated: all reserves are held by a third party, and there is no guarantee, except for the statements of the same third party, that these stablecoins are actually backed by enough collateral. Thus, companies issuing such stablecoins must regularly conduct independent audits to increase the level of transparency of their activities.

The need for a regulated financial institution storing the collateral assets in order to issue and redeem the corresponding stablecoins clearly requires trust. Users need to trust the issuer and its auditors to maintain the peg through sufficient collateralization and appropriate issuance and redemption of tokens. Besides requiring trust, the issuer also acts as a central entity in the whole process, thus introducing an element of centralization in contradiction with the very basic principles of blockchains.

In this paper, we describe a model that allows leveraging the strengths of stablecoins, while avoiding the shortcomings just mentioned. In particular, we include the possibility to handle collaterals and pegging mechanisms through smart contracts registered on the blockchain, thus allowing trustless transactions

[1]According to https://www.coingecko.com/ accessed October 15th 2022.

by removing intermediaries and external financial institutions.

Finally, pegging stablecoins to fiat currencies makes them unsuitable as a store of value and even less as investments. Such stablecoins are almost guaranteed to decline in real terms, with their purchasing power decreasing over time due to inflation. Pegging them to other asset classes, or to financial instruments that protect the purchasing power would eliminate the inflationary risk.

Also, pegging stablecoins to fiat currencies, which are managed and regulated by national central banks, contradicts the concept of decentralization promoted by the very essence of the blockchain. The trading platform remains decentralized, but the financial instrument used is not. Pegging stablecoins to securities belonging to asset classes other than fiat currencies (such as equity, commodities or real estate) would allow a greater independence from centralized financial institutions.

## 2. Model

Decentralized autonomous organization (DAO) can be defined as a corporate governance form, "incorruptible", with "publicly auditable" bylaws, running "without any human involvement" and as "open source software distributed across the computers of its stakeholders" (Hassan & De Filippi, 2021). DAO has been described by Buterin (2014), in the Ethereum white paper (Ethereum, 2014) as "an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automation itself cannot do". These members or governors "have the right to spend the entity's funds and modify its code".

We argue that a Decentralized Autonomous Organization that uses smart contracts to store collaterals in the form of cryptocurrencies and issues stablecoins pegged to financial assets belonging to classes different from fiat currencies, would be able to curtail the shortcomings described in the previous paragraph, while preserving all the advantages of more traditional stablecoins.

Figure 1 describes the key components and processes of such a DAO.

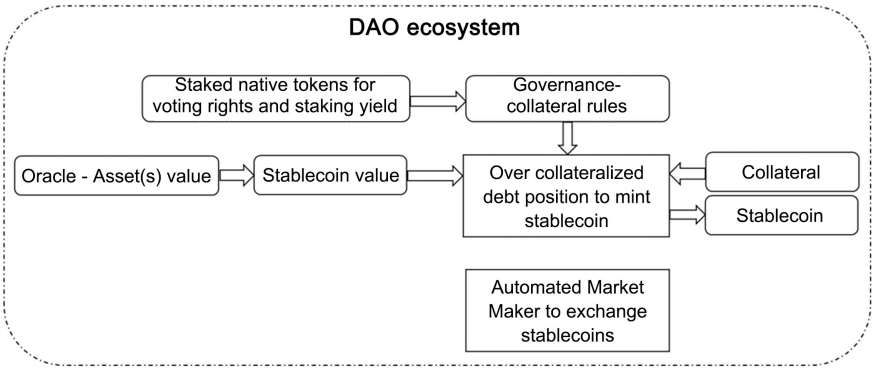


Figure 1. Main components and information flows in the DAO ecosystem (source: original from authors).

Stablecoins are issued (minted) using over-collateralized debts positions (CDP) governed by rules implemented in smart contracts executed in the blockchain. The CDPs operate autonomously and users can interact with them in a permission-less manner. There are no transaction fees for issuing stablecoins, yet users pay an interest rate (called stability fee) on the amount of stablecoin borrowed. In order to keep the stablecoin's peg, an essential function of the CDPs is to ensure that the value of the collateral deposited always exceeds the amount of stablecoin borrowed, hence the overcollateralization imposed by the protocol.

The relative value of collateral versus stablecoins changes with cryptocurrency fluctuations. The CDP's protocol must therefore include liquidation strategies triggered when the collateral value decreases below a predefined amount. Typically, there are three parameters for each collateral type:

- The minimum initial collateral ratio $r$.
- The re-collateralization ratio $rc$.
- The liquidation ratio $l$.

Where $l \leq rc \leq r$.

The CDPs operate as follows:

Consider a collateral with price pc used to mint stablecoins pegged to an asset of price pa and the collateral ratio $r$.

A CDP in which are deposited c units of collateral will be able to mint an amount s of units of stablecoin calculated in order to maintain this inequality:

$$s * pa * r \leq c * pc \text{ therefore } r \leq \frac{c * pc}{s * pa}$$

So, at issuance, the value of the stablecoin minted is over collateralized by a factor at least equal to $r$.

During the lifetime of the CDP, both $pc$ and pa will fluctuate. Should the ratio between collateral and stablecoin issued value drop to the re-collateralization value $rc$, the CDP would issue a margin call (call for re-collateralization) to bring the collateral back to at least $r$ times the value of the circulating stablecoin.

If the ratio decreases further and reaches the liquidation value $l$, the protocol retrieves and burns the stablecoins issued by the CDP. It does so by seizing the collateral and selling it to anyone willing to purchase it in exchange for stablecoins. If the collateral sells for an amount in excess of $s$, $s$ stablecoins will be burned to close the CDP and the difference credited to the wallet of the initial borrower. If the auction does not reach $s$, then the DAO protocol activates a dedicated process that consists in minting and selling the amount of native tokens necessary to repay the outstanding debt. Native tokens are cryptocurrencies tied to certain projects that are created by the DAO's protocol to accomplish the many goals described at the end of next paragraph.

Once the stablecoin is issued, there must be a market where to exchange it. Hence, the ecosystem should include or facilitate the creation of a marketplace for the newly minted coins. Automated Market Maker (AMM) serve this pur-

pose (Mohan, 2022; Wang, 2020): they are smart contracts with which users can interact in a trustless manner to perform token transactions. Each AMM creates pairs of cryptocurrencies, it "stores pooled reserves of two assets, and provides liquidity for those two assets, maintaining the invariant that the product of the reserves cannot decrease" (Wang, 2020). More generally, AMM are decentralized exchange protocols in which assets are priced according to pricing algorithms that vary from platform to platform.

To function properly, AMM require liquidity pools, i.e. smart contracts in which users deposit liquidity. In return for providing liquidity to the protocol, liquidity providers earn fees from the trades taking place in the pool. A typical fee is 0.3% of the traded amount that goes directly to liquidity providers. Considering the way in which AMMs operate, the more liquidity there is in the pool, the more efficiently they will operate, it is therefore important to attract liquidity to the pool. In order to do so, the DAO can provide an extra reward on top of the 0.3% earned from trades. It is not uncommon to see rewards in the range of 15% - 20% annual percentage rate paid in the inflationary native token of the DAO.

The last essential element required to ensure a proper functioning of the DAO is the oracle: oracles are used to provide external data to smart contracts, such as the price of a security needed to execute a certain operation. In the case of the DAO described above, the oracle is needed to input the value of the asset(s) to which the stablecoin is pegged. Oracles are critical and sensitive elements of smart contracts since they are used during the whole lifecycle of CDPs: to set the mining price, the pegging price and to initiate the eventual liquidation of CDPs. They are also the only element that bridges the blockchain to the external world, which makes them the easiest target for hackers. It is therefore recommended to deploy proper strategies to protect the system from an attacker attempting to gain control of the oracles.

## 3. Governance

In the ecosystem described so far, all regular operations can be executed in complete autonomy and transparency through smart contracts recorded in the blockchain. On the other hand, changes in the structure and processes of the DAO, require governance decisions. Topics such as collateralization ratios, assets usable as collaterals, reward rates and oracle policies require the intervention of the governing body. DAO governance is coordinated using tokens that grant voting powers (typically the native token of the DAO). Voting rights are granted to people who have a confirmed ownership of these governance tokens deposited in a cryptocurrency wallet. Governance is conducted through a series of proposals that members vote on, and ownership of more governance tokens translates to greater voting power. Incentives to promote active voting can be implemented by distributing additional DAO tokens.

Finally, it is important to mention the many roles played by the native token

of the DAO in ensuring the proper functioning of the many DAO's processes:

- The just mentioned voting rights in the DAO's governance, which allows playing a strategic role in the whole organization.
- The incentives for extra yield to reward liquidity providers to the liquidity pools.
- The important role plaid during the liquidation of CDPs: should the collateral auction for an amount of stablecoins inferior to what originally borrowed, the DAO mints enough native tokens to cover the difference.

Native token can be staked in the DAO's protocol in order to generate a return (called staking yield) for token holders; the interest paid to holders of staked coin is also decided through a governance vote.

## 4. Conclusion

This paper describes the architecture and functioning of a DAO aimed at issuing stablecoins pegged to financial assets. We argue that the design described allows full decentralization, disintermediation and permissionless transactions.

We believe that, compared to the design of most existing stablecoins, one such organization reflects more accurately the very founding principles of blockchains.

As always, like with virtually all implementation frameworks, there are drawbacks and open questions that can be addressed, entirely or partially, with further developments. In our opinion, the main ones are: the inflationist nature of the native token that may bring sharply down its value, thus depriving it of many of the functionalities described above; the governance method described requires that native token owners play an active role in the voting process, so the incentive scheme adopted must be motivating enough for participating in the voting process; finally, if the native token remains the property of only a few individuals, the ecosystem may potentially end up being more centralized than anticipated.

We believe that further refinements of the model presented in this article will help mitigate the limitations identified.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References

Ardia, D., Bluteau, K., & Rüede, M. (2019). Regime Changes in Bitcoin GARCH Volatility Dynamics. *Finance Research Letters, 29,* 266-271. https://doi.org/10.1016/j.frl.2018.08.009

Baur, D. G., Dimpfl, T., & Kuck, K. (2018). Bitcoin, Gold and the US Dollar—A Replication and Extension. *Finance Research Letters, 25,* 103-110. https://doi.org/10.1016/j.frl.2017.10.012

Boltshauser, T., & Seigneur, J. (2021). *Stablecoin DC Architecture Analysis*. International Telecommunication Union. https://archive-ouverte.unige.ch/unige:157864

Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. https://ethereum.org/en/whitepaper

Catalini, C., & Massari, J. (2021). *Stablecoins and the Future of Money*. Harvard Business Review Digital Articles.

Choi, G. (March 22, 2021). *Inner Workings of Collateral-Based Stablecoins and Its Implications*. Korea Institute of Finance Working Paper. https://doi.org/10.2139/ssrn.3809502

Ciriello, R. F. (2021). Tokenized Index Funds: A Blockchain-Based Concept and a Multidisciplinary Research Framework. *International Journal of Information Management, 61,* Article ID: 102400. https://doi.org/10.1016/j.ijinfomgt.2021.102400

Cong, L. W., Li, Y., & Wang, N. (2021). Tokenomics: Dynamic Adoption and Valuation. *The Review of Financial Studies, 34,* 1105-1155. https://doi.org/10.1093/rfs/hhaa089

Corbet, S., & Katsiampa, P. (2020). Asymmetric Mean Reversion of Bitcoin Price Returns. *International Review of Financial Analysis, 71,* Article ID: 101267. https://doi.org/10.1016/j.irfa.2018.10.004

Force, E. C. B. (2020). *Stablecoins: Implications for Monetary Policy, Financial Stability, Market Infrastructure and Payments, and Banking Supervision in the Euro Area* (No. 247). European Central Bank.

Hassan, S., & De Filippi, P. (2021). Decentralized Autonomous Organization. *Internet Policy Review, 10,* 1-10. https://doi.org/10.14763/2021.2.1556

Katsiampa, P. (2017). Volatility Estimation for Bitcoin: A Comparison of GARCH Models. *Economics Letters, 158,* 3-6. https://doi.org/10.1016/j.econlet.2017.06.023

Miraz, M. H., Hasan, M. T., Rekabder, M. S., & Akhter, R. (2022). Trust, Transaction Transparency, Volatility, Facilitating Condition, Performance Expectancy towards Cryptocurrency Adoption through Intention to Use. *Journal of Management Information and Decision Sciences, 25,* 1-20.

Mohan, V. (2022). Automated Market Makers and Decentralized Exchanges: A DeFi Primer. *Financial Innovation, 8,* Article No. 20. https://doi.org/10.1186/s40854-021-00314-5

Phillip, A., Chan, J., & Peiris, S. (2018). A New Look at Cryptocurrencies. *Economics Letters, 163,* 6-9. https://doi.org/10.1016/j.econlet.2017.11.020

Schlichting, L., & Petrini, R. D. (2019). The Qualification of Digital Assets According to Swiss Law, with Particular Reference to Stable Coins. https://doi.org/10.2139/ssrn.3424571

Wang, Y. (2020). Automated Market Makers for Decentralized Finance (DeFi). arXiv preprint arXiv:2009.01676.