Quantifying Stablecoin Stability and Decentralized Autonomous Organization (DAO) Autonomy

Kornrapat Pongmala

Electrical Engineering and Computer Sciences
University of California, Berkeley

Technical Report No. UCB/EECS-2023-247
http://www2.eecs.berkeley.edu/Pubs/TechRpts/2023/EECS-2023-247.html

December 1, 2023

Acknowledgement

I would like to express my gratitude to Professor Dawn Song for her guidance and support over the past few years, as well as to Professor Christine Parlour for serving as my second reader. I would also like to thank all of the co-authors, particularly Yujin Kwon and Tanusree Sharma, for their leadership and mentoring in the Stablecoin Stability and DAO Autonomy projects, respectively. Finally, I want to acknowledge the support of my friends, family, and teachers throughout my academic career.

Quantifying Stablecoin Stability and Decentralized Autonomous Organization (DAO) Autonomy

by Kornrapat Pongmala

Research Project

Submitted to the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, in partial satisfaction of the requirements for the degree of **Master of Science, Plan II**.

Approval for the Report and Comprehensive Examination:

Committee:

Dawn Song

Professor Dawn Song
Research Advisor

4/25/23

(Date)

* * * * * * *

Professor Christine Parlour
Second Reader

April 27/2023

(Date)

Abstract

Quantifying Stablecoin Stability and Decentralized Autonomous Organization (DAO) Autonomy

by

Kornrapat Pongmala

Master's of Science in Electrical Engineering and Computer Sciences

University of California, Berkeley

Professor Dawn Song, Chair

Stablecoin Stability

In May 2022, an apparent speculative attack, followed by market panic, led to the precipitous downfall of UST, one of the most popular stablecoins at that time. However, UST is not the only stablecoin to have depegged in the past. Designing resilient and long-term stable coins, therefore, appears to present a hard challenge. To further scrutinize existing stablecoin designs, and ultimately leading to more robust systems, we need to understand where volatility emerges. Our work provides a game-theoretical model aiming to help identify why stablecoins suffer from a depeg. This game-theoretical model reveals that stablecoins have different price equilibria depending on the coin's architecture and mechanism to minimize volatility. Moreover, our theory is supported by extensive empirical data, spanning 1 year. To that end, we collect daily prices for 22 stablecoins and on-chain data from five blockchains including the Ethereum and the Terra blockchain.

DAO Autonomy

Decentralized Autonomous Organizations (DAOs) have emerged as a novel way to coordinate a group of (pseudonymous) entities towards a shared vision (e.g., promoting sustainability), utilizing self-executing smart contracts on blockchains to support decentralized governance and decision-making. In just a few years, over 4,000 DAOs have been launched in various domains, such as investment, education, health, and research. Despite such rapid growth and diversity, it is unclear how these DAOs actually work in practice and to what extent they are effective in achieving their goals. Given this, we aim to unpack how (well) DAOs work in practice. We conducted an in-depth analysis of a diverse set of 10 DAOs of various categories and smart contracts, leveraging on-chain (e.g., voting results) and off-chain data (e.g., community discussions) as well as our interviews with DAO organizers/members. Specifically, we defined metrics to characterize key aspects of DAOs, such as the degrees of autonomy. The degree of autonomy varies among DAOs, with some (e.g., Compound and Krausehouse) relying more on third parties than others. We offer a set of design implications for future DAO systems based on our findings.

Contents

List of Figures

List of Tables

Acknowledgments

I would like to express my gratitude to Professor Dawn Song for her guidance and support over the past few years, as well as to Professor Christine Parlour for serving as my second reader. I would also like to thank all of the co-authors, particularly Yujin Kwon and Tanusree Sharma, for their leadership and mentoring in the Stablecoin Stability and DAO Autonomy projects, respectively. Finally, I want to acknowledge the support of my friends, family, and teachers throughout my academic career.

Chapter 1

Stablecoin Stability

1.1 Acknowledgement

This chapter in the thesis outlines the joint research work led by Yujin Kwon. The research work is on the stablecoin risks modeling from a discrepancy of redemption values between users and protocol. The work aims to provide a general risks framework, allowing theoretical comparison between different stablecoin designs.

1.2 Introduction

1.2.1 Stablecoin Roles in Decentralized Finance

In the past few years, we have seen an increase in the adoption of cryptocurrencies, with a market capitalization exceeding 2 trillion US dollars in 2021. This growth can be credited to the increasing popularity of Web3 and decentralized finance, which has attracted many innovators to develop diverse designs of decentralized applications aimed at addressing various existing hurdles in the decentralized finance landscape. Of the many areas of development, stablecoins have been one of the most innovative fields where a variety of designs coexist without a clear winner.

Similar to how fixed foreign exchange rate works between countries, stablecoins are cryptocurrencies designed to be 'pegged' or closely follow the price of another currency. One of the most common types of currency to which stablecoins are pegged is fiat currencies such as US dollars.

Stablecoins have played an integral role in onboarding new users and funds to the web3 space as they allow users to transact and store value knowing that their money is between traditional finance and decentralized finance worlds, knowing that it will not be affected by the price volatility of other currencies. Without stablecoins, many decentralized applications would be less useful as users are exposed to undesirable price volatility risks of cryptocurrencies such as ETH or Bitcoin.

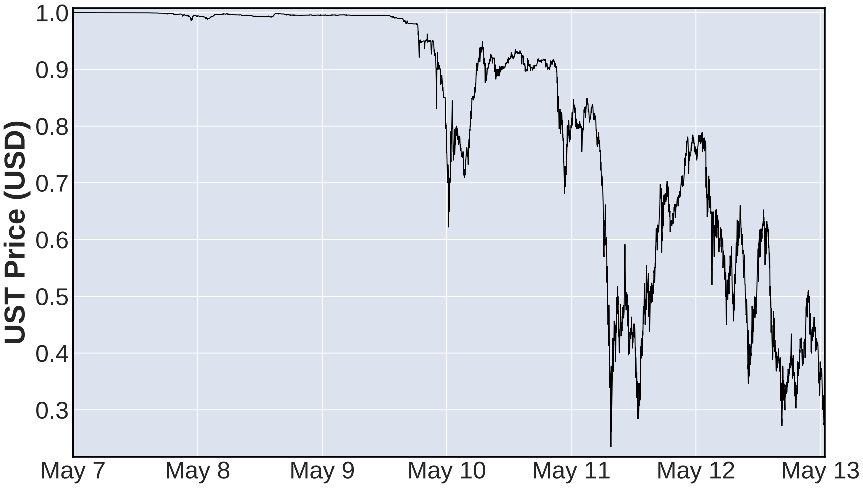


Figure 1.1: UST spot price (UST/USDT market) on Binance (May 7 – May 13, 2022).

1.2.2 Not-So-Stable Stablecoins

Given the integral part that stablecoins play in decentralized finance, risks associated with stablecoins pose a major threat to the entire web3 ecosystem. To provide further context on the importance of stablecoin stability on the cryptocurrency market, as of February 18th 2023, stablecoin's total market capitalization is over 137 billion US dollars, over 10 percent of the total cryptocurrency market capitalization. However, perhaps the most obvious incident illustrating the importance of stablecoin stability to the cryptocurrency market is the downfall of the Terra ecosystem on May 12, 2022, where USTC (formerly UST), a stablecoin pegged to US dollars, lost its value, liquidating billions of dollars worth of its cryptocurrency collateral and affecting the entire market on its way down [13].

Terra's UST was not the only stablecoin that had depegged from its intended value. Prior to UST, we have seen IRON from Iron Finance losing its peg of 1 USD [24]. A more recent example is USDN on the Waves blockchain that depegged down to 0.3 USD and eventually rebranded into XTN token that is no longer a stablecoin [18, 45].

While UST, IRON, and USDN never recovered to 1 USD, there are other stablecoins that have suffered temporary instability and still were able to recover to their intended value. USDT is a centralized stablecoin where its value is backed by a combination of fiat and other real world assets [44]. Due to its centralized nature, many people have expressed concerns over the actual value of the collateral backing USDT value. Whenever there is a significant news article that USDT may not be fully backed, its price may deviated from the peg. However, the price would always recover to 1 USD in a few days.

The diverse designs of stablecoins and the differences in their stability and ability to recover the peg beg the question of how the design differences of stablecoins affect their stability in various market conditions.

1.3 Background

1.3.1 Types of Stablecoins

Most of the existing stablecoins rely on arbitration to manage the supply and maintain the target price. The arbitration is done between trades on the secondary market, such as Binance and Uniswap, and the primary market, issuance and redemption in the stablecoin protocol. Based on the reserve type and redemption mechanism, stablecoins can be categorized into one or a combination of the following categories: Fiat-Collateralized, Crypto-Collateralized, Over-Collateralized, and Algorithmic. Here, a detailed definition of each category of stablecoins is provided below.

Fiat-Collateralized

Fiat-collateralized stablecoins are stablecoins that hold their reserves in the target fiat currency of its equivalent, such as treasury bills and loans. In fiat-collateralized designs, users can redeem their stablecoins directly into fiat currency against the reserves. To bridge between cryptocurrencies and government-issued fiat, users rely on a centralized organization that manages the issuance and redemption of stablecoins. Examples of fiat-collateralized stablecoins are USDT, USDC, BUSD, and TUSD.

Crypto-Collateralized

Crypto-collateralized stablecoins is a broad term generally used to refer to any stablecoin whose reserves are composed of a basket of cryptocurrencies. In this study, however, the term is used to refer to stablecoins whose reserves are composed of a basket of cryptocurrencies and *not associated with a lending protocol.* Redemption of a crypto-collateralized stablecoin yields cryptocurrencies at the target value. Specifically, the redemption of crypto-collateralized stablecoin with a target value of 1 USD gives 1 USD worth of a combination of cryptocurrencies. Unlike fiat-collateralized stablecoins, however, crypto-collateralized stablecoins' reserves have a risk of the reserves value falling lower than the stablecoins supply, making the stablecoins only partially backed. For this reason, the crypto-collateralized design is often used in combination with another design to ensure that users can always redeem their stablecoins at target value even while the reserves depreciate. An alternate solution is to find a way to expand the reserves, which could be done by imposing fees in various places in the protocol [28]. Some of the most well-known crypto-collateralized stablecoins are USDN, CUSD, and FEI.

Over-Collateralized

In this study, over-collateralized stablecoins refer to stablecoins whose issuance and redemption processes are derived from a decentralized lending protocol. In over-collateralized stablecoin designs, users deposit cryptocurrencies as collateral to mint the stablecoin, representing the debt owed to the protocol. Redemption, in general, can only be done by the debtors who would have to pay the stablecoin loan to unlock their collateral. The term 'over-collateralized' means that the value of the collateral is higher than the stablecoin debts at all times. The over-collateralization is supported by the collateral ratio and the liquidation process. The collateral ratio indicates the ratio between the collateral value and the stablecoin value, and is assigned to be higher than 1, meaning users have to deposit a higher value of collateral than the stablecoin loan. Moreover, each type of collateral cryptocurrencies can have a different collateral ratio depending on its price volatility. The liquidation process, on another hand, is a special case of redemption where a debt position is open up for anyone to repay in return for the collateral once the position is at risk of having a collateral ratio of less than 1 and becoming bad debt. One of the most prominent examples of over-collateralized stablecoins is DAI from the MakerDAO protocol.

Algorithmic

Algorithmic stablecoins differ from the three others as algorithmic stablecoins do not hold reserves. Instead, algorithmic stablecoins work by expanding and contracting their supply based on the demand. This is done by allowing users to mint or redeem the stablecoins with the protocol from and to another cryptocurrency endogenous to the protocol. For example, Terra USTC allowed users to mint or redeem 1 USTC from and to 1 USD worth of LUNC. LUNC is minted during USTC redemption and burned during the issuance of USTC. In this case, the price volatility of USTC is offloaded into LUNC from arbitraging the secondary market with the protocol. Since the collapse of USTC, many existing algorithmic stablecoins transitioned to other peg defense mechanisms. Prior to the collapse, some other popular algorithmic stablecoins included USDD in the Tron ecosystem.

1.3.2 Risks

Stablecoin risk and instability is a topic widely discussed both in peer-reviewed academic journals and web3 community. In addition to those, many existing studies on risks in traditional finance also translate well into stablecoins. This section goes over relevant studies regarding risks in stablecoin designs.

Many works [32, 15, 34, 37, 33] have analyzed the systematic risks of different stablecoin designs. As discussed in [32], traditional models of bank runs [20], runs on currency pegs [38], and pegged redemption money market funds [40] can be applied to understand the risks of various stablecoins; it is possible to reinterpret the pegging mechanism as the central bank, and so basic results about bank and currency runs can translate to many stablecoin settings. Given this, [41] investigates a way to avoid speculative attacks [38] in partially backed stablecoins, and shows that optimal exchange rate policies rate can help avoid the risk. [35] also studies the optimal strategy of collateralized stablecoin systems to investigate whether stablecoins are sustainable given the risks.

On the other hand, models explaining the (in)stability of stablecoins are relatively sparse. [30, 29] model stablecoins like DAI, where issuance is based on a market for leverage. In this context, they characterize deleveraging spirals that caused instability in DAI on "Black Thursday" in March 2020. [36] models how stablecoins backed by 100% reserves, such as USDC, maintain stability through arbitrage with minting and redemption. [31] explains a shape of redemption curves of several stablecoins and then designs a redemption curve that attains properties informed by currency peg models.

Beyond few attempts to elucidate the price (in)stability of stablecoins, existing models are difficult to generalize due to the heterogeneity of the stablecoin design space. Moreover, various distinctions about stablecoin models are not as developed, such as modeling the fact that reserve assets are not the currency target (e.g., USD is not an on-chain asset).

1.4 Redemption Value Discrepancy as Stability Risk

While the risks specific to some of the existing stablecoin designs have been well studied, the field lacks theoretical tools for stability comparisons across stablecoin designs. In this work, we propose a generalized game-theoretical model for ranking stability among the four broad stablecoin design categories mentioned earlier. This model is built on the concept of redemption value discrepancy between the protocol and users. As users cash out their stablecoin to the protocol, the actual value they receive may not be equal to the target value the stablecoin is designed to match. Some possible causes of the difference are discrete price oracle updates and reserves' price volatility. We show the actual value users realized during redemption gets translated into the price (in)stability on secondary markets.

Price oracle is one of the core components of all stablecoin designs. An inaccurate price oracle or discrete price oracle updates can be very problematic, in the issuance and redemption process, as it dictates the value of collateral so that the protocol could calculate the appropriate exchange rate between the stablecoin and collateral. Delayed price oracles can cause deficit to one of the parties and create undesirable market pressure.

Besides price oracle, the volatility of the collateral cryptocurrencies affects the actual value users realized. This is partly due to price oracles not being able to update fast enough to capture the volatility, but also the time it takes for users to realize the collateral cryptocurrencies into the target offchain fiat currency is non-zero, during which the value of the redeemed collateral could change.

1.5 Proposed Model

Here, we provide a description of the one-shot game model with many players. The model focuses on downward price instability as the upward price instability has never happened in practice as it can be easily corrected from users minting stablecoins from the system and selling to secondary markets for profit. Because we are only considering the downward price instability, it is sufficient to consider redemption as the user's only interaction with the protocol.

On the supply side, stablecoin holders can choose between 3 actions: 1) selling their stablecoins to the secondary market at price $p(M)$, 2) redeeming their stablecoins to the protocol at price v, and 3) holding on to their stablecoins for some future returns of $max\{i(p'(M')), i(v')\}$. Here, p denotes the current price function of the stablecoin, taking into account the slippage, where it depends on the liquidity depth and the amount of supply sold to the secondary market at that moment (M). v denotes the price offered by the protocol during redemption. i is an incentive function unique to each protocol, where users are rewarded for simply holding the stablecoin. This could be in a form of interest rate, additional token drops, or perks. Of course if the player decides to hold on to their stablecoins, their reward will be the max between selling their stablecoins in the future $i(p'(M'))$ and redeeming their stablecoins in the future $i(v')$, where p' is the price function at a specific moment in the future, M' is the amount of supply sold to the secondary market at a specific moment in the future, and v' is the offered redemption value by the protocol at a specific moment in the future.

On the demand side, players can choose between 1) joining the market by buying stablecoins from secondary market and redeeming them to the system, 2) joining the market and holding the stablecoins for future returns, and 3) not joining the market at all. These 3 actions could be viewed as identical to the supply side actions, but with the payoffs being $p(M)$ (cost to enter the market) less than the supply side actions. As the payoffs are identical, it is sufficient to analyze a rational agent behaviour on the supply side.

To put formally, the supply side payoff are defined as follows:

$$\text{payoff} = \begin{cases} p(M)(= p^s) & \text{if they sell coins to the market,} \\ v & \text{if they redeem coins to the system,} \\ \max\{i(p(M')), i(v')\} & \text{if they keep holding coins} \end{cases} \tag{1.1}$$

Without loss of generality, we assume that the intended target peg of the stablecoin is 1. Intuitively, to make the state $p(M) = 1$(secondary market price equals to intended target price) reachable and the state $p(M) < 1$ not an equilibrium, when $p(M) < 1$, the rational action should either be 1) redeeming the stablecoins to the protocol or 2) holding on to the stablecoins, preventing additional selling pressure on secondary markets. Additionally, to make the state $p(M) = 1$ the unique equilibrium, either redeeming the stablecoins or holding on to them should at least be as good of an option compared to selling to the market when $p(M) = 1$. This is to prevent the secondary market price to deviate below 1.

Theorem 1. *$max(v, i(v'), i(p'(M'))) > p(M)$ if $p(M) < 1$ and $max(v, i(v'), i(p'(M'))) \geq 1$ if $p(M) = 1$ are sufficient conditions to guarantee a reachable unique equilibrium at pegging state.*

This analysis of the game model can be applied to all types of stablecoins with the only modification of the redemption value v.

1.6 Stablecoin Equilibrium

In this section, we provide descriptions of redemption value v of each stablecoin design and qualitatively compare the theoretical stability of the four stablecoin designs by examining the equilibrium of each on various economic fundamental state θ as defined in [38]. Higher θ corresponds to stronger economic fundamental. The fundamental state is important to our analysis as it is one of the key factors affecting the redemption value discrepancy if users redeem into intermediary cryptocurrencies as defined in section 1.4. Incentive function can be used in conjunction with any of the four stablecoin designs, but is assumed to be identity in our study as it focuses on redemption mechanisms. Moreover, $v' = v$ is assumed as the redemption mechanism is independent of time.

1.6.1 Fiat-Collateralized

Let V^f be the value of fiat collateral in the reserves, T^s be the total supply of the stablecoins Q be the amount of the stablecoins users want to redeem to the protocol. In the case where the stablecoins are fully-backed by their reserves, $T^s \leq V^f$, redemption value v is guaranteed to be 1 as the reserves have enough balance to pay redemption and users redeem directly into fiat currency, circumventing any intermediary currency volatility risks. By Theorem 1, $v \geq 1$ is sufficient to guarantee a reachable unique equilibrium at the pegging state.

On the other hand, if the fiat-collateralized stablecoin is partially-backed, that is $T^s > V^f$, redemption value depends on the quantity of stablecoins being redeemed. If $Q \leq V^f$, then v is 1. Otherwise, v is $\frac{V^f}{Q}$. Depending on users' belief on the magnitude of Q, many equilibria exist. If the users believe that $Q \leq T^s$, they would feel safe holding on to the coin in the short term, maintaining the peg. If the users believe that Q can potentially be more than T^s, then they would rush to redeem to fiat or sell to secondary markets, eventually depegging the stablecoin.

1.6.2 Crypto-Collateralized

As redemption is paid in cryptocurrencies, redemption value discrepancy between the protocol and users matters. Depending on the fundamental state θ, the total value of the reserve $V^c(\theta)$ changes, where V^c is an increasing function of θ. With the value of stablecoin to redeem not exceeding the value of the reserves, $Q \leq V^c(\theta)$, for each stablecoin redeemed to the protocol, users would get $\frac{1}{p^c_s}$ collateral, where p^c_s is the collateral price in unit of fiat the system refers to. It is only when users sell those collateral cryptocurrencies into fiat that they realized the stablecoins into the pegged currency. Selling the collateral would give them $\frac{p^c_u}{p^c_s}$ fiat per stablecoin when p^c_u is the collateral price in the unit of fiat user refers to at the time they realized into target fiat. Let $v = r^c(Q, \theta) = \frac{p^c_u}{p^c_s}$ be the ratio of the price discrepancy between user and system. This ratio depends on the amount of stablecoins user redeems to the system and the fundamental state since the process of realizing the collateral to fiat depends on the market liquidity and often requires non-zero time. Similar to fiat-collateralized stablecoins, when $Q > V^c(\theta)$, $v = \frac{V^c(\theta)}{Q} r^c(Q,\theta)$

Assuming that the fundamental state θ is always strong enough for $V^c(\theta) \geq T^s$, the equilibria can still vary depending on $r^c(Q,\theta)$. For a stablecoin price to have a reachable unique equilibrium at 1, $v = r^c(Q,\theta) \geq 1$ is required. Let $r^c(T^s,\bar{\theta}) = 1$ at $\bar{\theta}$. $r^c(Q,\bar{\theta}) \geq 1$ for all Q as r^c is an decreasing function of Q. Thus, for $\theta \geq \bar{\theta}$, the stablecoin price has a reachable unique equilibrium at 1. However, if $\theta \leq \underline{\theta}$ where $r^c(0,\underline{\theta}) = 1$, the only price equilibria are the depegging states. Since when $p(M) \geq 1$, the rational action of some users would be to sell the coin to secondary market as redeeming the stablecoins would give less payoff and they do not believe that $p'(M') \geq 1$. This drives $p(M)$ to be lower than 1 and as $r^c(Q,\theta) < 1$ for $\theta \leq \underline{\theta}$ and $Q > 0$, the price could not return to the peg.

For $\underline{\theta} < \theta < \bar{\theta}$, there exists multiple equilibria, including $p(M) = 1$. For $\underline{\theta} < \theta < \bar{\theta}$, there exists $0 < Q^* < T^s$, such that $r^c(Q^*,\theta) = 1$. If users believe that the actual redemption would be more than Q^*, they would rush to get out of their stablecoin position by either redeeming to the protocol or selling on secondary market, inducing the stablecoin price to depeg. However, if users believe that $Q \leq Q^*$, then they have no reasons to redeem or sell their stablecoins, maintaining the state $p(M) = 1$.

1.6.3 Algorithmic

Redemption value in algorithmic stablecoin is similar to crypto-collateralized stablecoin where $v = r^c(Q,\theta)$. The only difference being algorithmic stablecoins do not need to fear its reserves running out, making $v = r^c(Q,\theta)$ no matter the economic fundamental state. Due to the similarity to the crypto-collateralized stablecoins, the analysis on price equilibrium of crypto-collateralized stablecoins applies to algorithmic stablecoins as well. For $\theta \leq \underline{\theta}$, the only equilibria are the depegging state. When $\underline{\theta} < \theta < \bar{\theta}$, there exist multiple equilibria, including the pegging state. When $\bar{\theta} \leq \theta$, the equilibrium is at the pegging state. However, as $\underline{\theta}$ and $\bar{\theta}$ are defined based on the value r^c function takes, they are dependent on the cryptocurrency being used as collateral. Algorithmic stablecoins depend on an internal cryptocurrency to be used as collateral, while crypto-collateralized stablecoins do not. Because of this, both $\underline{\theta}$ and $\bar{\theta}$ are higher for algorithmic stablecoins than for crypto-collateralized stablecoins.

1.6.4 Over-Collateralized

Redemption of over-collateralized stablecoins can be done by either a user closing their own borrowing position or a liquidation of a position open to anyone once the collateral ratio falls below a predetermined threshold. Let $D^L(\theta)$ be the amount of stablecoins to be redeemed through liquidation at a point in time and D^{u_i} be user u_i outstanding stablecoin loan not in liquidation. We assume that D^L is a decreasing function on θ, meaning more stablecoins can be redeemed through liquidation in bad economic situation.

In over-collateralized systems, users have to deposit collateral of greater value to mint stablecoins. Redemption, both through liquidation and loan payment, is to payback the stablecoins to unlock the collaterals greater in value than the stablecoins payment. We define the ratio between the value of the unlocked collateral in target currency and the unit stablecoin payment from the protocol perspective as $o^c(\theta)$, where o is a increasing function on θ. The function o varies between protocols and collateral type, but $o^c(\theta) \geq 1$ when θ is not too small. When $o^c(\theta) < 1$, the corresponding debt position is commonly referred to as bad debt, where liquidation of the position is guaranteed to incur a loss to the liquidator.

Due to the designs unique over-collateralized systems, redemption value in overcollateralized systems is $v = r^c(Q, \theta) \cdot o^c(\theta)$ when $D^L > 0$ or $\exists i D^{u_i} > 0$. Let $r^c(Q, \underline{\theta}) \cdot o^c(\underline{\theta}) = 1$. Assuming that $o^c(\underline{\theta}) \geq 1$, similar to crypto-collateralized and algorithmic stablecoins, when $\theta < \underline{\theta}$, the stablecoin only have equilibria in the depegging states as $v < 1$ for all Q. Moreover, $\underline{\theta}$ is smaller in over-collateralized system compared to crypto-collateralized and algorithmic since $o^c(\underline{\theta}) \geq 1$ from the assumption.

On another hand, when $\theta > \underline{\theta}$, there exist multiple equilibria based on users' self-fulfilling beliefs even when $r^c(Q, \theta) \cdot o^c(\theta)$ for all Q. This is because of the difference in the redemption mechanism between over-collateralized stablecoins and other types of stablecoins. In other types of stablecoins, redemption is open to anyone. With only 1 person acting in a rational way and continuously arbitraging the secondary market price and redemption value of the stablecoin, the price would converge to the peg. In over-collateralized systems, however, redemption is mainly done through closing one's own loan position, a user is limited by how much profit they can make arbitraging the price and redemption. Once they have closed the position, they are locked out from making more profit. Because of this, depending on the stablecoin debtor's belief, redemption may not be the rational decision. If the debtor believes that many other debtors will redeem and close their loan positions, they would be more inclined to close their position now and take the small profit as they would expect the price to converge back to peg in the near future. However, if they expect the other debtors to keep their position open, waiting for the stablecoin price to drop even more, they would also keep holding the stablecoin in hope for a larger profit once the price continues the decline.

1.6.5 Theoretical Ranking

Our game model yields the theoretical stability of the four types of stablecoins in various fundamental states as shown in figure 1.2.

1.7 Empirical Price Stability

In this section, we attempt to provide evidence backing the theoretical ranking from our game model by empirically evaluating the price stability of the top 22 stablecoins ranked by market capitalization on September 10, 2022. As our model relies on the economic fundamental variable θ, it is important to choose a common time frame to evaluate all of the

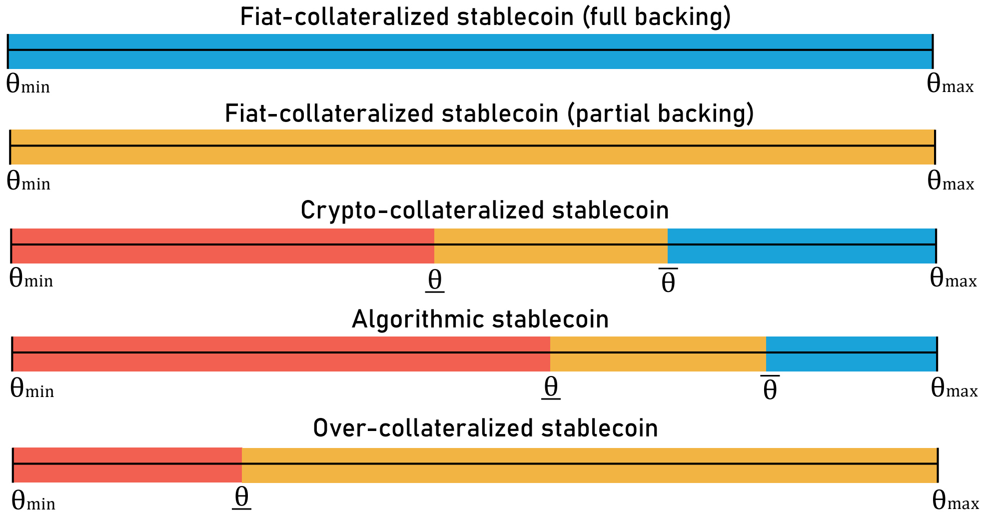


Figure 1.2: **An equilibrium state for given θ by stablecoin type.** Each color bar represents a zone of θ with a different equilibrium state. In the blue zone, a unique pegging equilibrium exists. In the yellow zone, there are multiple equilibria, including the pegging state of $p(M) = 1$. In particular, the pegging state is a self-fulfilling equilibrium. In the red zone, there is only a depegging equilibrium.

chosen stablecoins. In this study, we examine the price stability of the chosen stablecoins over a period of 1 year starting from May 13, 2021. USDD is excluded from this study as it was launched in May 2022.

The empirical analysis is done in two folds. First, we rank stablecoins downward price stability and compare them with our theoretical results. Second, we measure the correlation and causality between the actual redemption value and the price of stablecoin to quantify their relationship as suggested in Theorem 1.

1.7.1 Data Collection

In order to conduct the analysis, secondary market price data and the users' realized redemption value for each stablecoin are needed. Daily secondary market price data of all 22 stablecoins are obtained from CoinMarketCap [18]. Table 1.1 provides a categorization of the 22 stablecoins as well as price statistics during the period of study. Note that some stablecoins employ multiple defense mechanisms. Here, 'Fiat' refers to fiat-collateralized stablecoins, 'Crypto-S' refers to crypto-collateralized stablecoins that use other stablecoins as collateral, 'Crypto-NS' refers to crypto-collateralized stablecoins that use non-stable cryptocurrencies as collateral, 'Algo' refers to algorithmic stablecoins, and 'Over' refers to over-collateralized stablecoins.

On another hand, users realized redemption value data can be much more difficult to obtain due to the lack of transparency in some stablecoin designs and the missing connection when users decide to realize the collateral into fiat as this is often done through centralized exchanges. The first issue is specific to centralized fiat-collaterized stablecoins. For example, in fiat-collateralized designs, such as USDT and USDC, these data are not made available to the public. To get around this issue, we assume that the redemption value of fiat-collateralized stablecoins is $v = 1$. The second issue, however, can be circumvented if we make the assumption that users would realize the collaterals into USDT immediately through secondary market price. To this end, on-chain redemption data, the number of stablecoins redeemed, and the number of collateral tokens, are fetched for 11 of 22 stablecoins, and the secondary price of the collateral tokens to USD is fetched from CoinMarketCap. The 11 stablecoins are DAI, FRAX, FEI, OUSD, MUSD, LUSD, USDN, CUSD, USTC, sUSD, and VAI. These stablecoins are chosen prioritizing the diversity of design, diversity of platform (spanning across 5 layer-1 blockchains), high market capitalization, and ease of access to the data.

1.7.2 Downward Price Stability

The price stability of stablecoins are evaluated based on how close the current price of them are to the target value of 1 USD. We define the price deviation from the peg as $\sqrt{\frac{\sum_{i=0}^{N-1}(p_i-1)^2}{N}}$, where p_i is the closing price on the i^{th} day. Correspondingly, as the model focuses on the downward price stability, downward price deviation from the peg is defined as $\sqrt{\frac{\sum_{i=0}^{N-1}(\min(p_i-1,0))^2}{N}}$.

Unlike other stablecoins, where peg defense mechanism(redemption) is available independent of the price on the secondary market, FRAX redemption is only available when the secondary market price deviate from the range $[0.9933, 1.0033]$. To fairly evaluate the peg defense mechanism across stablecoin designs, price deviation from the peg and downward price deviation from the peg for FRAX is adjusted to be $\sqrt{\frac{\sum_{i=0}^{N-1}\min_{x\in[0.9933,1.0033]}(p_i-x)^2}{N}}$ and $\sqrt{\frac{\sum_{i=0}^{N-1}(\min(p_i-0.9933,0))^2}{N}}$, respectively.

To assign the ranking of the stablecoins based on downward price stability, we use the downward price deviation from the peg. For each pair of the stablecoin, independent t-test is used to verify if the assigned ranks are statistically meaningful. Table 1.2 shows ranking of the stablecoins based on downward price deviation from the peg. Figure 1.3a and Figure 1.3b graphically represent the price deviation from the peg and downward price deviation from the peg of each stablecoin categorized by the peg defense mechanism, respectively.

It can be seen from Table 1.2 and Figure 1.3b that fiat-collateralized stablecoins tend to have more price stability than other categories, followed by crypto-collateralized stablecoins using other stablecoins as collateral, then crypto-collateralized stablecoins using non-stable cryptocurrencies as collateral, algorithmic, and over-collateralized stablecoins. This result is consistent with the theoretical model as fiat-collateralized stablecoins are stable regardless

Name	Type	Market Cap.	Avg.	Min	Max
USDT	Fiat	$67.56B	1.0004	0.9959	1.0019
USDC	Fiat	$51.72B	1.0000	0.9982	1.0016
BUSD	Fiat	$19.91B	1.0001	0.9981	1.0037
DAI	Crypto-S+Over	$6.87B	1.0004	0.9878	1.0098
TUSD	Fiat	$1.62B	1.0000	0.9985	1.0024
FRAX*	Crypto-S	$1.48B	1.0003	0.9871	1.0682
USDP	Fiat	$945.18M	1.0001	0.9907	1.0060
USTC**	Algo	$637.41M	0.9977	0.4086	1.0098
USDN*	Crypto-NS	$629.60M	0.9866	0.7831	1.0157
FEI	Crypto-S	$422.23M	0.9964	0.9468	1.0127
GUSD	Fiat	$363.84M	0.9972	0.9656	1.0319
LUSD	Crypto-NS+Over	$174.97M	1.0039	0.9515	1.0415
HUSD	Fiat	$160.19M	1.0000	0.9976	1.0026
USDX	Over	$105.40M	0.9676	0.6677	1.0203
sUSD	Over	$77.24M	1.0002	0.9899	1.0276
VAI	Over	$54.92M	0.8972	0.7408	1.0963
CUSD	Crypto-NS	$51.63M	0.9991	0.9847	1.0230
OUSD	Crypto-S	$48.27M	0.9985	0.9772	1.0481
MUSD	Crypto-S	$41.92M	1.0024	0.9111	1.0578
RSV	Crypto-S	$28.84M	0.9996	0.9867	1.0196
USDK	Fiat	$28.82M	1.0013	0.9795	1.0230
EOSDT	Over	$2.17M	0.9625	0.4313	1.9084

*Although FRAX says that they are an algorithmic stablecoin, here we mark FRAX as Crypto-S, because it uses the algorithmic pegging mechanism only when the crypto-collateralized mechanism using other stablecoins does not work.

**Here, USTC means UST before May 12, 2022.

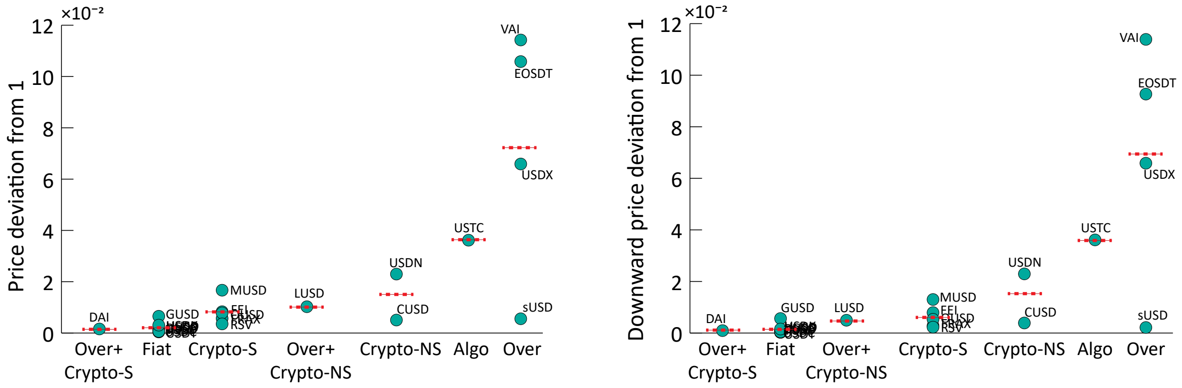
Table 1.1: Statistics of daily price data considering the time period from May 13, 2021, to May 12, 2022

Type	Name	Price deviation from 1		Downward price deviation from 1	
		Value	Ranking	Value	Ranking
Fiat	USDT	6.1961×10^{-4}	3	2.7112×10^{-4}	1
	USDC	4.1747×10^{-4}	1	2.8842×10^{-4}	2
	BUSD	6.5501×10^{-4}	5	4.1341×10^{-4}	4
	TUSD	4.8585×10^{-4}	2	2.9634×10^{-4}	3
	USDP	1.4753×10^{-3}	6	1.1181×10^{-3}	8
	GUSD	6.5357×10^{-3}	13	5.6325×10^{-3}	15
	HUSD	6.2961×10^{-4}	4	4.4792×10^{-4}	5
	USDK	3.0760×10^{-3}	8	1.5460×10^{-3}	9
Crypto-S+Over	DAI	1.5766×10^{-3}	7	9.3304×10^{-4}	7
Crypto-S	FRAX	4.1901×10^{-3}	10	7.7119×10^{-4}	6
	FEI	8.3035×10^{-3}	15	7.9128×10^{-3}	16
	OUSD	7.8163×10^{-3}	14	5.3287×10^{-3}	14
	MUSD	1.6690×10^{-2}	17	1.3002×10^{-2}	17
	RSV	3.5518×10^{-3}	9	2.2750×10^{-3}	11
Crypto-NS+Over	LUSD	1.0255×10^{-2}	16	4.9520×10^{-3}	13
Crypto-NS	USDN	2.2982×10^{-2}	18	2.2933×10^{-2}	18
	CUSD	5.0588×10^{-3}	11	3.8918×10^{-3}	12
Algo	USTC	3.6189×10^{-2}	19	3.6120×10^{-2}	19
Over	USDX	6.5899×10^{-2}	20	6.5859×10^{-2}	20
	sUSD	5.5589×10^{-3}	12	2.1421×10^{-3}	10
	VAI	1.1425×10^{-1}	22	1.1389×10^{-1}	22
	EOSDT	1.0582×10^{-1}	21	9.2677×10^{-2}	21

*When running a t-test to rank a price deviation of stablecoins, there was no statistical significance (i.e., P-value > 0.1) for the following 18 pairs out of 231 ($= {}_{22}C_2$) pairs: (USDT,BUSD), (USDT, HUSD), (HUSD, BUSD), (USDP,DAI), (DAI, FRAX), (USDK,FRAX), (USDK, RSV), (RSV, FRAX), (FRAX, sUSD), (FRAX, CUSD), (CUSD, sUSD), (OUSD, USTC), (OUSD,FEI), (FEI, USTC), (LUSD, USTC), (MUSD, USTC), (USDN, USTC), (EOSDT, VAI)

*When running a t-test to rank a downward price deviation of stablecoins, there was no statistical significance (i.e., P-value > 0.1) for the following 16 pairs out of 231 ($= {}_{22}C_2$) pairs: (USDT,USDC), (USDT,TUSD),(USDC, TUSD),(BUSD, HUSD),(FRAX,DAI), (DAI,USDP), (DAI, USDK), (USDP, USDK), (sUSD, RSV), (CUSD, LUSD), (LUSD,GUSD), (LUSD,OUSD), (OUSD, GUSD), (FEI, USTC), (MUSD, USTC), (USDN, USTC)

Table 1.2: Price volatility and downward price volatility of stablecoins given daily price data from May 13, 2021 to May 12, 2022.



(a) Price deviation from 1

(b) Downward price deviation from 1

Figure 1.3: (Downward) price deviation by stablecoin type. The x-axis is arranged in ascending order of the average values by stablecoin type. Red dot lines represent an average value by stablecoin type.

of θ if they are fully-backed. $\overline{\theta}$ and $\underline{\theta}$ for crypto-collateralized and algorithmic stablecoins are dependent on the robustness of collateral cryptocurrencies.

Downward price stability of over-collateralized stablecoins has high variance across stablecoin within the same category. This is also consistent with the theoretical model that suggests that over-collateralized stablecoins have multiple equilibria including the pegging state depending on overall sentiment of the users even when θ is large.

It is observed that stablecoins that use over-collateralization in combination with crypto-collateralization tend to have better price stability than using purely crypto-collateralization. This phenomenon can be captured by our theoretical model. Using over-collateralization with crypto-collateralization induces $\underline{\theta}$ to be lower than crypto-collateralized stablecoins, and similar to over-collateralized stablecoin, while still guarantee a unique equilibrium at the peg when $\theta \geq \overline{\theta}$. This is because the stablecoin can benefit from guaranteed over-collateralization while redemption is open to everyone.

Due to the limited number of stablecoins, these observations cannot be used as statistical evidence to our theoretical model, however, they are in agreement with the implication of it.

1.7.3 Price and Realized Redemption Value Correlation

To analyze the relationship between stablecoin price and user realized redemption value, we perform correlation and causality analysis between downward price deviation of the daily closing price and downward user realized redemption value of the last redemption transaction of the day, resulting in 365 samples of redemption values and price observations spanning from May 13 2021 to May 12 2022. This is done to ensure that the time difference between redemption and price observation is minimal and redemption happened prior to the price observation.

The realized redemption value v is calculated with the assumption that users sell the collateral to the market at the daily close price. The amount to collateral user received is fetched on-chain. This method of calculating v takes into account protocol fees that often scale linearly with the amount of stablecoin redeemed and does not take into account transaction fees that are constant relative to the amount of stablecoin redeemed.

Table 1.3 summarizes the result of Pearson correlation and Granger causality analysis.

Type	Name	Correlation		Granger causality	
		Rho	P-value	F-stats.	P-value
Crypto-S+Over	DAI	0.1499	0.0136	5.8753	0.0160
Crypto-S	FRAX	0.1833	0.2576	1.1987	0.2809
	FEI	0.1845	0.0028	5.2799	0.0224
	OUSD	0.0934	0.2097	0.9743	0.3250
	MUSD	-0.0986	0.0620	1.2057	0.2729
Crypto-NS+Over	LUSD	0.3248	<0.0001	30.1870	<0.0001
Crypto-NS	USDN	0.4914	<0.0001	76.9957	<0.0001
	CUSD	0.1341	0.0104	12.3066	0.0005
Algo	USTC	0.8366	<0.0001	88.7618	<0.0001
Over	sUSD	0.7677	<0.0001	44.1318	<0.0001
	VAI	-0.0200	0.7560	9.9877	0.0018

Table 1.3: Correlation and Granger causality between a stablecoin price and v

We can see that the significant correlation and causality between v and a price are manifested in most stablecoins. DAI, FEI, LUSD, USDN, CUSD, USTC, and sUSD showed a significant correlation and causality. Meanwhile, it was not observed for FRAX, OUSD, MUSD, and VAI. In particular, we find that stablecoins with relatively good stability of a price and v do not show a strong correlation and causality; overall, DAI and Crypto-S have a relatively high P-value in Granger causality. This could be resulted from the deviations caused by noise or other factors being more apparent in coins with good downward stability of v. Most representatively, we can think of fiat-collateralized stablecoins where v is always 1. Definitely, their price deviations do not come from v.

In addition, the existence of correlation and causality between v and a price can be inconsistent across over-collateralized stablecoins; in our data, sUSD showed a significantly positive correlation and causality, but VAI showed an insignificant correlation. As described earlier, it can be difficult to predict consequences of over-collateralized stablecoins due to their wide yellow zone.

The last important point is that stablecoin systems with a popular and large incentive protocol have little correlation and causality between a price and v, which Theorem 1 points out. In fact, even though UST showed significant correlation and causality considering its collapse event, there was no significant correlation (Pearson's ρ =0.0421, P-value=0.5369) and causality (F=0.8426, P-value=0.3597) when only considering the period (Oct 01, 2021 to May 06, 2022) that an incentive protocol, Anchor, was greatly popular. Note that Anchor promises to give users nearly 20% annual percentage yield (APY), and it even held about 75% of the total UST market cap in some cases.

We recognize the limitation of empirical analysis to show the true causality because there are not only two variables, v and a price, in the real world. In fact, it is well known that deriving the true causality is really challenging. By analyzing the stablecoin price along with many variables other than v, we will be able to examine whether the true causality between v and the price exists. Nevertheless, we believe that the results of the empirical analyses confirm our theory to some extent.

1.8 Discussion

In this paper, we developed a common theory to characterize the stability properties of many stablecoins, considering reserve asset types and redemption mechanisms. A continuous price drop of the assets backing stablecoins can reduce the actual (or recognized) payoff that users get by redeeming stablecoins, which can contribute to peg stress. Stablecoin systems collateralized by volatile cryptocurrencies can often suffer from this, leading to a higher price instability level compared to fiat-collateralized systems. To avoid the depegging state, such systems may need to rely on additional incentive mechanisms, such as large interest rates that can motivate many users to keep holding their coins. As stablecoins receive newfound scrutiny, our model helps to improve understanding of design differences and establishes guidelines for future stablecoin design.

Chapter 2

DAO Autonomy

2.1 Acknowledgement

This chapter in the thesis outlines the joint research work being done in [43]. The research work aims to quantify the decentralization and autonomy level of Decentralized Autonomous Organizations(DAOs).

2.2 Introduction

2.2.1 What is a DAO?

DAO, or Decentralized Autonomous Organization, is a term that refers to a new form of organization enabled by blockchain technology. Despite its increasing popularity, the conception of the term DAO is difficult to pinpoint. Perhaps one of the first attempts to define a DAO is in an Ethereum Foundation blog post by Vitalik Buterin in 2014 [16], in which Buterin characterized DAOs using the degree of autonomy, human involvement, and internal capital. Vitalik defined DAO as an entity managing internal capital with autonomy at the center and humans at the edge in order to achieve some shared vision. Given this definition, blockchains are ideal for managing DAOs by providing transparency and programmable predefined organization rules. However, despite the provided definition, DAOs come in various forms in regard to the governance process that often do not fit nicely within the given definition due to varying degrees of human involvement and centralization.

DAOs can have a wide variety of goals and designs. Some DAOs are created to govern the distribution of digital assets, such as BitDAO [1] that enables token holders to decide and fund Web3 projects. On the other hand, a DAO could also be created to manage a decentralized prediction market, such as the Augur [2] platform which allows users to bet on the outcome of real-world events, bringing offchain data onchain. Moreover, a DAO could be used to govern a decentralized finance protocol, such as the MakerDAO [3] platform that governs the DAI stablecoin. Lastly, a DAO could be just an organization for people with a shared goal to come together and attempt to achieve it. For example, Krause House DAO [4] aims to buy an NBA team, or The Constitution DAO [5] aims to buy a copy of the US constitution. The design of a DAO can vary widely as well, with some using liquid democracy models that allow participants to delegate voting power to trusted individuals, others using token-based voting systems that give weight to each participant's stake in the network, while some abandoning the voting mechanism entirely and have centralized team to manage the funds.

2.2.2 History of DAO

One of the first examples of a DAO was The DAO, which was launched on Ethereum on April 30, 2016 [22]. The DAO was intended to be an investment DAO, comparable to venture capital, that enabled community members to vote on projects to fund while generating a return on each investment. Unfortunately, The DAO was later exploited in June of the same year, resulting in the loss of 2.6 million Ether valued at 50 million USD at the time. This event led to a hard fork of the Ethereum blockchain into Ethereum and Ethereum Classic, the prior reverting the hack and returning the funds to affected users.

Despite the controversy surrounding The DAO, interest in DAOs continued to grow. In recent years, there exists several tools to help manage and facilitate DAOs. For example, there are now DAO factory contract platforms like MolochDAO, DAOHaus, and Aragon [6, 7, 8], which allow for the creation of customizable DAO templates. There are also off-chain proposal management tools like Snapshot [9], which allows for voting on proposals without the need for on-chain transactions, saving users from the gas cost of onchain voting. Additionally, multisig wallet tools like Gnosis [10] have been developed to allow for secure management of DAO funds between trusted parties.

2.3 Background

2.3.1 Autonomy

The emergence of DAOs has the potential to disrupt various industries beyond finance, including, a range of areas such as work, arts, and governance, including the restructuring of the basis of democracy in human societies. Although these applications claim to be autonomous, human action is required to evolve them [46]. The concept of autonomy in DAOs is a topic of ongoing debate in both the technical, legal, and financial spheres [46]. Some argue that DAOs should be fully autonomous and fully automated, with no external parties involved in decision-making processes [42]. Others propose a more nuanced interpretation of autonomy, emphasizing transparency and clear decision-making processes.

In the context of human-robot interactions, autonomy is defined as the extent to which a robot can sense, plan, and act in its environment without external control [17, 14, 27]. Various researchers have addressed potential liability and ethical issues arising from autonomous agent designs [26, 21]. Pagallo provides a historical perspective on the liability issues arising from automation through to autonomous systems [39]. Different studies propose different levels of autonomy to determine where a morally salient decision belongs on the ethical scale [23]. Similarly, classifying DAOs based on autonomy metrics is challenging since existing taxonomies are often ambiguous and categorical rather than quantitative along a continuum [46]. Decision-making scope and liability are the most generalizable dimensions, with domain-specific definitions being less easily generalizable. Themes that can be applied to DAOs include the degree of human supervision, decision-making roles, liability, and ethical considerations [25]. Of these dimensions of autonomy, DAOs liability has been explored in [46]. However, DAOs' autonomy in decision making from an ethical perspective is not well explored as ethical judgment is sensitive and can be difficult to define unambiguously. On another hand, DAOs autonomy from the perspective of human supervision and their roles in decision making is more well-defined, yet not well understood empirically. Thus, in this paper, we aim to understand the level of autonomy and the degree to which DAO operates without undue external influence, potentially from corporate competitors or regulators.

2.4 Proposed Autonomy Metrics

We aim to examine autonomy within DAOs by analyzing four distinct metrics: (1) Capability of Arbitrary Transaction Execution, (2) Third-Party Dependent Proposals After Execution, (3) Canceled Proposals After Voting Ends, and (4) Execution Time Delay.

2.4.1 Capability of Arbitrary Transaction Execution

Summary Nowadays, there exist multiple methods in translating the DAO's consensus into onchain action. While the governance process can be done entirely onchain to ensure bindingness of the consensus with minimal human intervention in executing the DAO action, many existing DAOs choose to trade autonomy for simpler methods. We explore such methods for the 10 DAOs from the perspective of autonomy by investigating how and to what degree individuals can influence this process in their favor.

Limitations Despite the process being highly manual in retrieving the source code and analyzing methods DAOs use to issue onchain transactions, the results are applicable to many DAOs as DAOs tend to use existing factory contracts and pre-made methods in issuing onchain transactions.

2.4.2 Third-Party Dependent Proposals After Execution

Summary Third-party dependent proposals refer to proposals that rely on third-party actions to achieve their goals. Translating the consensus into onchain proposal execution is only half of the picture of the proposal execution process as some proposals can not be completed onchain. Some examples of such proposals could be hiring someone to host an offline event or hiring someone to write a smart contract. In this study, third-party actions refer to any action not originated from the DAO proposal pipeline. Execution refers to the timestamp for onchain conclusion of the proposal. In the case of hiring a third party to do some work, third party action refers to the work delivered by the third-party and the point of execution refers to onchain record for employment, usually comes in the form of salary payment. While interaction with third-parties is inevitable for most DAOs, the number of third-party dependent proposals after execution can serve as a proxy for the number of occurrences the DAO autonomy is being threatened. Generally, a smaller number of such proposals means a higher level of autonomy. In this section, we quantify the occurrences of such proposals in each DAO and identify strategies DAOs currently employ to mitigate the autonomy risk while still benefiting from third-party services.

Limitations In identifying whether a transaction is dependent on third-party after execution, it can be difficult for us (external researchers) to objectively make such a determination. Our proposed criteria of categorization may not be applicable to every DAO due to the diversity in the DAO proposal content. The process is also labour intensive and can be error-prone as it requires manually going through the proposal content, community discussions, and onchain transactions to understand the context of the transaction.

2.4.3 Canceled Proposals After Voting Ends

Summary One way a DAO autonomy could be hampered is through proposal censorship. Proposal censorship refers to the act of not carrying out the proposal action after the community consensus has been reached. Having a small group of people translating consensus into DAO's onchain action can be viewed as an autonomy bottleneck as that group of people have to power to censor or manipulate the community consensus result. We empirically quantify the event of proposal censorship in the 10 DAO using a combination of onchain transaction data and offchain community discussion data.

Limitations For DAOs that have their governance done onchain, calculating the number of canceled proposals after voting ends can often be done through crawling emitted smart contract events. The process for offchain DAOs, however, is much more manual as it requires a mapping between offchain proposal data and onchain transactions. Due to the vast number of proposals, not all proposals can be determined if they have been executed or canceled. This highlights the lack of proposal transparency tools in the field.

2.4.4 Execution Time Delay

Summary Part of autonomy includes the DAO's capability to promptly convert consensus into onchain action. Some DAOs rely on a small group of people to issue a transaction while some others allow anyone to issue a predetermined proposal transaction after the consensus has been reached. We collected the execution time delay data, which is the difference between actual execution time and the intended execution time, of the 5 onchain DAOs. The average execution time delay is compared across DAOs. For each DAO, we conducted a correlation analysis between network congestion and execution time delay to explore the relationship between the two variables.

Limitations Limitations for execution time delay analysis are similar to canceled proposals after voting ends analysis, where proposal timeline data can be fetched through emitted smart contract events for onchain DAOs and much more manual for offchain DAOs.

2.5 Method

2.5.1 DAO selection

We analyzed different categories of DAOs (e.g. DeFi, Investment, Entertainment, Social, Sports, Video, etc.) with 10 specific DAO projects which were formed between 2019 and 2022. We selected 10 projects, prioritizing diverse categories, popularity, and market capitalization. To add diversity for governance design, we, in particular, considered four DAOs, created with popular DAO factory contracts, including Governance Bravo, DAOhaus, and DAOStack in the governance structure aspect of smart contracts. Table 2.1 presents the key parameters of the 10 DAO projects, including the treasury size, number of DAO holders, active voters, total votes, participation rate in proposals, number of proposals, number of proposal creators, quorum voting, and proposal threshold. Despite significant growth in market capitalization, crucial information is missing from various resources for all existing DAO projects, indicating limited transparency and highlighting the need for a comprehensive service that can provide more detailed analytics for these projects.

DAOs often adopt existing governance protocols from predecessors. For example, BitDAO's governance token BIT uses the governance design of Compound's governance token COMP, which is built on the governance bravo contract [11]. This is done for flexibility in governance design, as it allows for delegated voting (i.e., allowing another person to vote on one's behalf) and off-chain vote aggregation with the potential for future on-chain governance. Some DAOs use factory contracts, such as dxDAO's DAOStack factory contract while others use platforms like Juicebox for treasury management and Kleros for bridging off-chain decisions to on-chain action. However, the widespread reuse of popular governance protocols can limit the diversity of the governance system. Furthermore, when DAOs reuse existing sets of smart contracts, they are relying on the security features of that codebase. This approach can have both advantages and limitations. Many DAO governance contracts developed from bigger protocols have already been audited for security issues, such as the Compound Governor Bravo Audit [12], which can be beneficial for smaller DAOs that may not have the capital or human resources to develop their own smart contracts and have them

DAO	Category	Treasury	#Holders	#Active	Avg votes	Participation %	# proposal	#votes	#Creator	Proposal Threshold	Quorum
CompoundDAO	Protocol	90.7M	205.9k	4.1k	78	1.80%	137	12750	48	25000 COMP	400,000
BitDAO	Investment	1.6B	20.4k	320	53	1.30%	19	1347	14	200,000 BIT	100,000,000
AssangeDAO	Social	242.9k	6.3k	1.1k	298	12.30%	11	3576	2	1,000 JUSTICE	867,576,97
Proof of Humanity	Social	801.7k	35.2k	3.1k	153	8.80%	104	16557	25	0 VOTE	NA
Bankless DAO	Web3 fund	1.6M	5.9k	3,375	344	43%	51	18272	7	0 BANK	NA
KrauseHouse	Sports	1.2M	1.8k	595	32	30%	131	4,484	5	1,000 KRAUSE	0
LivePeer	Video	0	NA	NA	NA	NA	7	600	7	0 LPT	1/3*27,004,976
MetaGammaDelta	Social	29.7k	NA	49	2	29.40%	79	132	30	1 DAI	0
MolochDAO	Public Good	0.1	NA	60	4	50.80%	32	83	29	1 WETH	0
dxDAO	Protocol	81M	1.4k	232	2	5.80%	864	3161	160	0 rep	0 if boosted else 50 % REP token supply

Table 2.1: DAO Projects Summary in terms of macro information

audited. On the other hand, if a vulnerability is found in a DAO using similar contracts, an attacker could easily target other DAOs that share the same codebase. Additionally, it can be more challenging for DAOs that use others' code to implement unique features that are specific to their organization. In general, while reusing existing smart contract code can be a practical solution for smaller DAOs, it is important to be aware of the potential risks and limitations involved. It is also essential to consider the unique needs and requirements of a particular DAO when deciding whether to reuse existing code or to develop custom smart contracts.

Among 10 DAO projects, five perform off-chain voting (BitDAO, AssangeDAO, Bankless, KrauseHouse, Proof of Humanity) while the rest perform on-chain. Gnosis Safe [10] Snapshot platform is often used for off-chain voting aggregation for its user-friendly interface and improved user experience. However, it does not automatically implement in blockchain and requires further action from the operation team through multi-sig. Across 10 different DAOs, the requirements vary significantly. For instance, BitDAO and CompoundDAO only allow whitelisted addresses to propose, and proposal submissions require a specific amount of tokens above a certain threshold. However, the threshold is often too high for grassroots users to propose without delegation from others, resulting in industry entities or large token holders submitting most proposals. AssangeDAO, BanklessDAO, and KrauseHouse only permit authors who are verified on snapshot to propose. In Proof of Humanity, the proposal requirement changed from allowing anyone to propose to only committee or elected members. In Livepeer, anyone with a sufficient amount of staked [1] governance tokens can propose, while in Meta Gamma Delta and MolochDAO, proposals require sponsorship[2] from a member. Lastly, dxDAO has the most flexible proposal requirement, allowing anyone to propose regardless of membership or token ownership. Each DAO also has a specific quorum voting strategy for accepting proposals, with CompoundDAO requiring 400,000 COMP, BitDAO requiring 100,000,000 BIT, AssangeDAO requiring 867,576,975 JUSTICE tokens, and Livepeer requiring 9001658.762 LPT (which is 33.33% of the LPT supply).

Each DAO has a specific voting period, ranging from a minimum of two days to seven days. After the voting period ends, DAOs have a timelock period, which can vary. Out of the 10 target DAOs, three have a timelock period, for example, CompoundDAO has a 48-hour timelock period while MolochDAO has a 7-day timelock period. Some DAOs, such as Meta Gamma Delta and MolochDAO, also have strategies to add a grace period [3] of 12 days into the timelock. On the other hand, BitDAO, AssangeDAO, Proof of Humanity, Bankless DAO, and KrauseHouse do not have any timelock period [4]. While the timelock period could

---

[1] Staked governance tokens are locked for a period of time. Those that stake their tokens often bear certain protocol risks.

[2] Sponsoring proposals in Moloch and Meta Gamma Delta DAO is an act in which a DAO shareholder moves the proposal into the voting pipeline.

[3] grace period is synonymous to timelock period here which is when a proposal is queued, but has not taken effect yet.

[4] The Timelock period refers to the time when the contract queues and executes proposals that have passed a Governance vote

be implemented in addition to a multisig, the DAOs we studied that use a multisig do not have a timelock. In particular, BitDAO, AssangeDAO, Bankless, and KrauseHouse use the multisig feature where a safe Multisig Admin manages the treasury and ensures executions. This allows organizations to fully customize how they manage their assets and protocols, with the option of requiring a predefined number of signatures to confirm transactions. Smart contracts can execute actions as long as a predefined number of trusted members agree upon them. Finally, none of the DAOs support votes from governance tokens on another chain, except for BanklessDAO.

2.5.2 Data Collection

We collected both off-chain data including DAO proposals, voting in different proposals by addresses, and token and treasury smart contracts, as well as off-chain and onchain voting smart contract modules. Furthermore, blockchains store massive amounts of heterogeneous data that grows over time.

For DAOs having readily available source code, we turned to Etherscan [5]. Etherscan has become the de-facto source for Ethereum blockchain exploration. Etherscan offers a useful feature called "verified" contracts, where contract writers can publish source code associated with blockchain contracts. Etherscan then independently verifies that the compiled source code produces exactly the bytecode available at a given address. Etherscan then makes the verified source available to the public. We scraped Etherscan for contracts as of November, 2022. We then checked contracts with the corresponding GitHub sources to determine the correct complied version for our analysis. For MolochDAO, Meta Gamma Delta and dxDAO, we aggregated factory contracts from DAOhaus and DAOstack.

Focusing on the network that DAOs are built upon, we searched for voting and proposal information sources on the blockchain (on-chain DAO) and the corresponding voting platform (i.e., snapshot for offchain DAOs). When it is necessary, we directly access records (blocks) using a unique identifier (e.g. block ID, transaction, wallet or contract address). As a result, we build scripts and data pipeline/techniques for data extraction in order to conduct analysis effectively without having to sequentially walk through all the blockchain or offchain platform data. Table 2.2 lists three main forms of data including smart contracts, on/off-chain voting, on/off-chain proposals. We collected the data in comma separated value and json files as per the needs of analysis.

2.6 Result

In this section, we evaluate the autonomy of 10 DAOs. While there exists many angles to evaluate the level of autonomy of a DAO, such as financial and legal autonomy, we aimed to explore the DAO's autonomy from the angle of operating without undue external influence. To this end, we analyze (1) whether a DAO system can execute arbitrary transactions, (2)

---

[5] Etherscan. https://etherscan.io

Smart Contract Data	DAO Proposal Data	Data Voting Data
	Proposal Author	
	Proposal Title	Voter Address
	Proposal description	Voter Organization
	Proposal Timestamp	Voter Token Weight
Ethereum smart contracts	Proposal start/end Block	Voter Average Token Weight
Factory Smart Contract	Author Token Wieght	Voter Name if available
DAOhaus	Proposal Signatures	Voting Pattern (1, -1, 0)
DAOstack	Proposal Outcome	Voting txHash
	Proposal State	Voting Gas Cost(ETH)
	Proposal Gas Cost	Voting Gas Cost(USDT)
	Execution Time delay	Voter Timestamp
	intendedExecutionTime	

Table 2.2: List of Metadata collected for off/on chain DAOs

whether it does not rely on third parties after transaction execution, (3) whether proposals have been canceled after accepting them, and (4) how long they were delayed to be executed.

2.6.1 Arbitrary Transaction Execution

```
function execTransaction(
       address to,  uint256 value, bytes calldata data, Enum.Operation
       ↪  operation, uint256 safeTxGas, uint256 baseGas, uint256 gasPrice,
       ↪  address gasToken, address payable refundReceiver,  bytes memory
       ↪  signatures
   ) public payable virtual returns (bool success) {
       bytes32 txHash;{
           bytes memory txHashData =
               encodeTransactionData(
                   to, value, data, operation, safeTxGas,
                   baseGas, gasPrice, gasToken,refundReceiver,
                   nonce );
           nonce++;
           txHash = keccak256(txHashData);
           checkSignatures(txHash, txHashData, signatures)  }
```

Figure 2.1: Multi-sig: Arbitrary txn execution achieves in GnosisSafe Multisig Wallet

The ability to execute arbitrary transactions is a crucial aspect of DAOs [19]. Here, arbitrary transaction execution refers to the capability of a DAO to fulfill a wide range of proposals, regardless of their specific requirements. Without this capability, a DAO's functionality would be limited, and it would require additional intervention to execute certain transactions on-chain, such as transferring funds to an EOA[6] to carry out proposal execution. This would decrease the autonomy level of the DAO. To achieve arbitrary transaction execution, DAOs must be able to interact with any contract on the same blockchain, as well as other entities on the chain. This is typically done by passing call data through the call function in Solidity [19].

To determine the capability of a DAO to execute arbitrary transactions, and the methods by which it does so, we first conducted a thorough examination of the smart contracts listed on the DAO's website or Github repository. Specifically, we searched for code snippets that enable arbitrary transaction execution. We then identified the treasury address of the DAO through the information available on their website and their voting platform (such as Snapshot, DAOHaus, etc.). Subsequently, we traced transactions from the treasury address to proposals through the voting platform and located the address of the code snippet we had previously identified, thus validating the DAO's use of a contract with arbitrary transaction execution capability. We also analyzed the smart contract codes of the DAOs and how they interact with other entities on the blockchain. Figures 2.1 and 2.2 provide examples of

---

[6] Externally Owned Account (EOA) refers to addresses that are managed by a private key and not a smart contract code.

```
function execute(bytes32 _proposalId) external {
      MultiCallProposal storage proposal = proposals[_proposalId];
      require(proposal.exist, "must be a live proposal");
      require(proposal.passed, "proposal must passed by voting machine");
      if (schemeConstraints != SchemeConstraints(0)) {
          require(
          schemeConstraints.isAllowedToCall(
          proposal.contractsToCall,
          proposal.callsData,
          proposal.values,
          avatar),
          "call is not allowed");
      }
```

Figure 2.2: On-chain DAOs: dxDAO Arbitrary txn execution achieved by the MultiCallScheme

DAO	Arbitrary Txn Execution
CompoundDAO	On-chain
LivePeer	2 of 3 Multisig
MetaGammaDelta	On-chain
dxDAO	On-chain
MolochDAO	On-chain
AssangeDAO	3 of 7 Multisig
BitDAO	3 of 6 Multisig
Bankless	4 of 7 Multisig
ProofOfHumanity	Kleros Governor
KrauseHouse	4 of 7 Multisig

Table 2.3: A table summarizing the arbitrary transaction execution of each DAO. Rows are DAOs. Columns are Arbitrary Transaction Execution Capability and Context note of why that DAO do/doesn't need it.

different types of arbitrary transactions, including on-chain[7], multisig[8], and Kleros Governor contract[9]

Our study of 10 DAOs revealed that all of them have some protocols for executing arbitrary transactions, although the protocols vary in terms of autonomy. The majority of DAOs that have an on-chain voting system have the entire pipeline for voting, reaching consensus, and execution on-chain. Due to this, we can consider DAOs that use on-chain arbitrary transaction execution to be the most autonomous, as the transaction sequence is immediately defined at proposal submission and no one can make changes to it afterward. Conversely, DAOs that have an off-chain voting system require a mechanism to bring the consensus reached off-chain to on-chain. Most of these DAOs use a multisig wallet to issue on-chain transactions. This limits the degree of decentralization and autonomy, as a small group of people controls the on-chain actions that should be executed. However, using multisig wallets is mainly for ease of implementation and maintenance.

Another method to bring transactions on-chain is to allow anyone to propose a list of transactions to fulfill passed proposals, and after a period of time, those transactions will be executed. If anyone submits a competing list of transactions, a community dispute is opened, and the winning transaction list gets rewarded from the losing list stake. This approach is observed in the Kleros Governor contract. Currently, Proof of Humanity adopts this method. Although this method is more decentralized than a multisig wallet, it still has limitations

---

[7] The transaction list is crafted at proposal submission and queued in timelock or executed right after voting, all processes are done on-chain, and no one can stop this (except the proposer in some cases).

[8] Core members craft a list of transactions for a particular proposal and execute them on the chain with a multisig

[9] Anyone can craft a list of transactions satisfying the proposals, and community member double check on the crafted list and can challenge the list.

in terms of autonomy, as multiple parties have to be involved in ensuring that the proposed list of transactions is valid, which can result in a delay in execution.

The approach to achieve arbitrary transaction execution varies among the DAOs, with having the transaction data included at proposal submission on-chain being the most autonomous. The multisig approach trades autonomy for simplicity. While Kleros Governor contract ensures decentralization in bringing off-chain consensus on-chain, the approach still lacks autonomy.

2.6.2 Cancelled Proposals After Voting Period

We then examined proposals that were canceled after the voting period ended. These are proposals that were accepted but ultimately not implemented. This statistic serves as a proxy for evaluating whether community consensus is respected and whether a DAO is truly autonomous, in the sense that a small group of individuals cannot prevent a DAO action from being carried out. To determine the percentage of proposals that were canceled without execution, we analyzed events from the smart contracts of on-chain DAOs, except for LivePeer, by crawling them. For off-chain DAOs and LivePeer, we manually examined data from Snapshot and Discourse to determine if the proposals have been successfully implemented.

Most of the analyzed on-chain DAOs (i.e., three out of five DAOs) have a "binding" consensus, which means that proposals will be executed after accepting them. This is often done through a smart contract, so they do not have a cancellation mechanism after the proposal

```
function cancel(uint proposalId) external {
        require(state(proposalId) != ProposalState.Executed,
        ↪  "GovernorBravo::cancel: cannot cancel executed proposal");
        Proposal storage proposal = proposals[proposalId];
        if(msg.sender != proposal.proposer) {

            } else {
                 }    }
        proposal.canceled = true;
        for (uint i = 0; i < proposal.targets.length; i++) {
            timelock.cancelTransaction(proposal.
            targets[i], proposal.values[i], proposal.signatures[i],
            proposal.calldatas[i], proposal.eta);
        }   emit ProposalCanceled(proposalId);   }
```

Figure 2.3: CompoundDAO: smart contract method for proposal cancellation.

DAOs	Binding	Total Prop	Total Prop Passed	Proposal Passed but Did Not Get Executed	Total Unknown Status
CompoundDAO	Proposer can cancel	137	110	6	0
dxDAO	Binding	789	678	0	0
LivePeer	Not binding	7	7	0	0
MolochDAO	Binding	25	25	0	0
MetaGammaDelta	Binding	75	69	0	0
AssangeDAO	Not binding	11	10	0	0
BitDAO	Not binding	18	16	0	2
BanklessDAO	Not binding	51	48	0	2
ProofOfHumanity	Not binding	104	87	9	5
KrauseHouse	Not binding	131	113	14	44

Table 2.4: Proposal decisions in each DAO where rows are the DAOs and columns are whether the consensus is binding through: smart contract timelock that cant be canceled, smart contract timelock that can be canceled by proposer, multisig, or single wallet. The number of proposals that were canceled before execution. Rows are each DAOs. Columns are the number of proposals that were canceled before the execution

has passed. Only on-chain DAOs with a formal cancellation mechanism after the proposal has passed are CompoundDAO and LivePeer. In CompoundDAO, proposal cancellation can be done by the proposal author at any moment or by anyone in the case that the author's governance token balance drops below the proposal threshold. The proposals that were canceled after the voting period ends in CompoundDAO are mostly ones that were overwritten by another proposal because of parameter/transaction issues[10] and ones for a temporary bug fix that were overwritten by another proposal[11]. The cancellation in the case of LivePeer is because the DAO requires a multisig to issue the transaction, and not everything is done on-chain. Thus, after the consensus has been reached, multisig still can "cancel" the proposal if they wish. For the remaining off-chain DAOs, proposals can technically be censored as off-chain consensus is not guaranteed to be brought on-chain. However, some off-chain DAOs still hold a binding consensus ideology and have not yet censored any proposals. While the percentage of proposals canceled is an important metric for autonomy, difficulty arises when empirically calculating this metric due to the limited transparency of the proposal status after consensus is reached in many off-chain DAOs.

---

[10] https://compound.finance/governance/proposals/99

[11] https://compound.finance/governance/proposals/63

Name	1 (not reliance)	0 (reliance)
AssangeDAO	81.81%	18.18%
CompoundDAO	83.94%	16.06%
BitDAO	72.22%	28.78%
Proof of Humanity	86.54%	13.46%
Bankless DAO	70.59%	29.41%
KrauseHouse	25.19%	74.81%
LivePeer	85.71%	14.29%
Meta Gamma Delta	100%	0%
MolochDAO	84.84%	15.15%

Table 2.5: Percentage of proposals that relies on third-party services after execution. Rows are each DAOs where 0 means relying on a third party and 1 is not reliance

Our data on the number of proposals canceled after voting ends suggests that DAOs tend to follow proposal binding ideology even if it is not guaranteed programmatically. A high number of unknown status proposals suggests that there is a need for proposal transparency tools.

2.6.3 Third-Party Dependent Proposals

In DAOs, third-party dependencies refer to the reliance on external entities to fulfill a portion of a proposal after it has passed the voting period. This dependence on third-party services can be a sign of lower autonomy for the DAO, as it introduces uncontrollable external factors that can potentially intervene with the intention of the DAOs action. It is also important to investigate how current DAOs utilizing third-party services handle and minimize associated risks. Our analysis of the relationship between DAOs and third parties can not only aid in evaluating autonomy, but also provide insight into how DAOs currently benefit from third-party services while minimizing risk exposure. For example, actions in a DAO like CompoundDAO or BitDAO would be considered third-party dependent if they are not proposed through the DAO's governance or executed through its designated contract (e.g. Timelock contract or Multisig). According to our investigation, such proposals can be payment for future services or delegation of decision-making power to a small group. These proposals rely on third-party services after their execution as the DAO is delegating trust to a third party to fulfill promises made in the proposal.

We sought to investigate the utilization of third-party services following the execution of proposals within DAOs. To accomplish this, we analyzed both the content of the proposals and the associated execution data. Our evaluation process involved assessing the primary objectives of each proposal to determine whether post-execution intervention or deviation from the proposal's promises could potentially negate the proposal's effectiveness or have a detrimental effect on the DAO.

Table 2.5 presents the percentage of proposals that rely on third-party services for nine different DAOs. dxDAO is left out of the analysis due to the large number of proposals making it infeasible to conduct the manual analysis. Of the 9 DAOs examined, only proposals from the Meta Gamma Delta DAO do not rely on third-party services following execution. This is because proposals within the Meta Gamma Delta DAO are either requests for membership or funding, with no promise of returns made in the proposal. The DAO with the highest percentage of proposals relying on third-party services following execution is the KrauseHouse DAO at 74.81%. Many of the KrauseHouse proposals involve funding requests from third parties, with promises of future returns in the form of working hours, contributed to the DAO. While third-party reliance following proposal execution can be beneficial in allowing a DAO to achieve various goals, particularly those that are off-chain or related to real-world works, DAOs should take measures to minimize the risks associated with third-party services. By inspecting the proposals that rely on third-party services following execution, some strategies that DAOs use to minimize these risks were identified, including (a) using stream payments instead of upfront lump sum payments, (b) using milestone-based payments where funds are paid based on completed tasks, and (c) assigning a committee with a multisig wallet to manage funds allocated for third-party services.

Most DAOs require services from a third party to operate. One of the most common cases of third-party reliance is employment for some future services. DAOs that have complicated offchain goals, such as KrauseHouse buying an NBA team, can have more reliance on the third party. Despite the such necessity of the third party in DAOs, there are many strategies to minimize the risk of third-party reliance.

2.6.4 Execution Delay

Part of being autonomous is the ability of a DAO to promptly translate consensus into actions. We look into the execution time delay defined as the time between a transaction being executable to the actual execution time. For the execution time delay analysis, we collected proposal timeline data, including Timestamps of proposal execution and proposal voting ends. We plot the execution time delay over time to see the trend and analyze whether the proposal time delay is correlated with a gas cost. For all on-chain DAOs, we did not find a significant correlation between gas cost and execution delay.

The average execution time delay is summarized in table 2.6. The average execution time delay of CompoundDAO is the lowest with 4h 58 min. This is expected as CompoundDAO is one of the most popular DAO , has its proposal pipeline done entirely on-chain, and their proposals are more urgent in general (e.g., updating parameters, new token support, new functionality) than a proposal on other DAOs (e.g., membership, grant request, etc.) On the other hand, MetaGammaDelta has the highest execution time delay with 5d 15h 23 min on average. Some possible explanations for this could be due to the fact that the number of active participators in Meta Gamma Delta is lower than in other DAOs and most proposals are on membership approval, which is not an urgent matter.

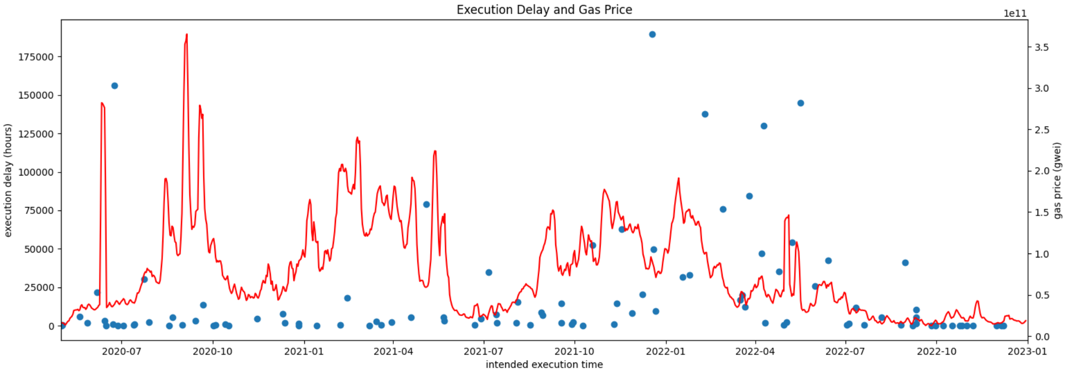


Figure 2.4: Average Execution time delay for proposal in CompoundDAO Overtime

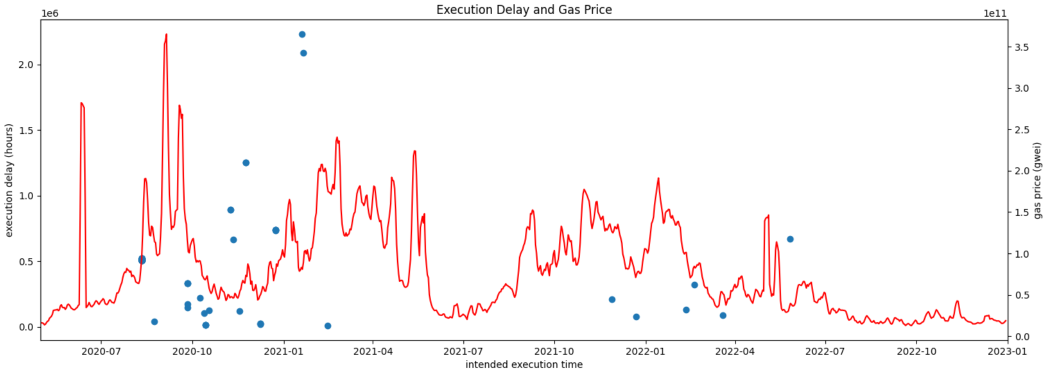


Figure 2.5: Average Execution time delay for proposal in MetaGammaDelta Overtime

DAO	Average Execution Delay (DD:HH:MM:SS)
CompoundDAO	4:58:56
dxDAO	8:53:17
LivePeer	3:09:18:57
MolochDAO	1:16:54:15
MetaGammaDelta	5:15:23:50

Table 2.6: Table containing the average time delay of proposal execution of each DAOs.

It is observed that the execution time delay varies from 4 hours up to 6 days for on-chain DAOs.

2.7 Discussion

One angle of autonomy explored in this paper is the dependency of a DAO on external entities and the degree of intervention a DAO needs to carry out its actions. One of its aspects is the method a DAO uses to translate consensus reached to onchain actions. While many onchain DAOs have their proposal pipeline done onchain to ensure decentralization and autonomy of proposal execution, many offchain DAOs use a Multisig wallet to translate the consensus reached offchain to onchain actions. This can result in poor decentralization and autonomy. Kleros Governor is an interesting alternative to ensure the decentralization of offchain DAOs, but the method can lack autonomy as it relies on multi-step checks done after consensus. Autonomy can also be explored on the proposal level as many DAO proposals rely on third-party services after execution to achieve the proposals' goal. The portion of proposals relying on third-party services after execution varies from 0-75% among the DAOs studied. Another metric calculated in this study is the number of proposals canceled after voting ends. This metric is particularly important as it shows to what degree the community consensus is respected; however, some limitations of this analysis are the limited transparency of offchain DAOs and the large number of proposals that need to be manually mapped to onchain transactions. It is observed that despite not being pragmatically guaranteed, some offchain DAOs still closely follow binding proposals ideology. Lastly, we analyzed the proposal execution delay for the five onchain DAOs. It is not found to have any correlation to the gas price data in most DAOs. However, the average delay is significantly different between the DAOs, suggesting that it might be affected by the popularity or taxonomy of the DAO.

Bibliography

[1] https://www.bitdao.io/. Accessed on 2022.

[2] https://augur.net/. Accessed on 2022.

[3] https://makerdao.com/en/. Accessed on 2022.

[4] https://www.krausehouse.club/. Accessed on 2022.

[5] https://www.constitutiondao.com/. Accessed on 2022.

[6] https://molochdao.com/. Accessed on 2022.

[7] https://app.daohaus.club/. Accessed on 2022.

[8] https://app.aragon.org/. Accessed on 2022.

[9] https://snapshot.org/. Accessed on 2022.

[10] https://docs.snapshot.org/gnosis-safe. Accessed on 2022.

[11] https://github.com/compound-finance/. Accessed on 2022.

[12] https://blog.openzeppelin.com/compound-governor-bravo-audit/. Accessed on 2022.

[13] Luna Foundation Guard (LFG). *LFG-technical audit report*. Feb. 2023. URL: https://medium.com/terra-money/lfg-technical-audit-report-ddaf3f51e7d.

[14] FEDERAL AVIATION ADMINISTRATION.(FAA). *Operation and Certification of Small Unmanned Aircraft Systems*. LULU COM, 2015.

[15] Douglas W Arner, Raphael Auer, and Jon Frost. “Stablecoins: risks, potential and regulation”. In: *Financial Stability Review* 39 (2020), pp. 95–123.

[16] Vitalik Buterin. *Daos, dacs, Das and more: An incomplete terminology guide*. URL: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide.

[17] Bruce T Clough. *Metrics, schmetrics! How the heck do you determine a UAV’s autonomy anyway*. Tech. rep. Air Force Research Lab Wright-Patterson AFB OH, 2002.

[18] *Cryptocurrency prices, charts and market capitalizations*. URL: https://coinmarketcap.com/.

[19] Poulami Das et al. “{FastKitten}: Practical Smart Contracts on Bitcoin”. In: *28th USENIX Security Symposium (USENIX Security 19)*. 2019, pp. 801–818.

[20] Douglas W Diamond and Philip H Dybvig. "Bank runs, deposit insurance, and liquidity". In: *Journal of political economy* 91.3 (1983), pp. 401–419.

[21] Carolyn Dowling. "Intelligent agents: some ethical issues and dilemmas". In: *Proc. AIC 2000* (2000), pp. 28–32.

[22] Quinn DuPont. "Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization". In: *Bitcoin and beyond*. Routledge, 2017, pp. 157–177.

[23] Sjur K Dyrkolbotn, Truls Pedersen, and Marija Slavkovik. "Classifying the Autonomy and Morality of Artificial Agents." In: *CARe-MAS@ PRIMA* 2017 (2017), pp. 67–83.

[24] Iron Finance. *Iron Finance Post-Mortem 17 June 2021*. June 2021. URL: https://ironfinance.medium.com/iron-finance-post-mortem-17-june-2021-6a4e9ccf23f5.

[25] Claudia E Haupt. "Artificial professional advice". In: *Yale JL & Tech.* 21 (2019), p. 55.

[26] Carey Heckman and Jacob O Wobbrock. "Liability for autonomous agent design". In: *Proceedings of the second international conference on Autonomous agents*. 1998, pp. 392–399.

[27] Hui-Min Huang et al. "Autonomy levels for unmanned systems (ALFUS) framework: An update". In: *Unmanned Ground Vehicle Technology VII*. Vol. 5804. SPIE. 2005, pp. 439–448.

[28] Sep Kamvar, Marek Olszewski, and Rene Reinsberg. "Celo: A multi-asset cryptographic protocol for decentralized social payments". In: *DRAFT version 0.24 https://storage. googleapis. com/celo whitepapers/Celo A Multi Asset Cryptographic Protocol for Decentralized Social Payments. pdf* (2019).

[29] Ariah Klages-Mundt and Andreea Minca. "(In) stability for the blockchain: Deleveraging spirals and stablecoin attacks". In: *Cryptoeconomic Systems* (2021).

[30] Ariah Klages-Mundt and Andreea Minca. "While stability lasts: A stochastic model of noncustodial stablecoins". In: *Mathematical Finance* (2022).

[31] Ariah Klages-Mundt and Steffen Schuldenzucker. *Designing autonomous markets for stablecoin monetary policy*. https://arxiv.org/abs/2212.12398. 2022.

[32] Ariah Klages-Mundt et al. "Stablecoins 2.0: Economic Foundations and Risk-based Models". In: *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 2020, pp. 59–79.

[33] John Paul Koning. *Algorithmic Stablecoins*. https://www.aier.org/article/algorithmic-stablecoins/. [Online; accessed 21-Jul-2022]. 2021.

[34] Yujin Kwon et al. "The trilemma of stablecoin". In: *Available at SSRN 3917430* (2021).

[35] Ye Li and Simon Mayer. "Money creation in decentralized finance: A dynamic model of stablecoin and crypto shadow banking". In: *Fisher College of Business Working Paper* 2020-03 (2022), p. 030.

[36] Richard K Lyons and Ganesh Viswanath-Natraj. "What keeps stablecoins stable?" In: *Journal of International Money and Finance* 131 (2023), p. 102777.

[37] Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. "SoK: A classification framework for stablecoin designs". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2020, pp. 174–197.

[38] Stephen Morris and Hyun Song Shin. "Unique equilibrium in a model of self-fulfilling currency attacks". In: *American Economic Review* (1998), pp. 587–597.

[39] Ugo Pagallo et al. "From automation to autonomous systems: A legal phenomenology with problems of accountability". In: *IJCAI International Joint Conference on artificial intelligence*. International Joint Conferences on Artificial Intelligence. 2017, pp. 17–23.

[40] Cecilia Parlatore. "Fragility in money market funds: Sponsor support and regulation". In: *Journal of Financial Economics* 121.3 (2016), pp. 595–623.

[41] Bryan Routledge and Ariel Zetlin-Jones. "Currency stability using blockchain technology". In: *Journal of Economic Dynamics and Control* 142 (2022), p. 104155.

[42] Carlos Santana and Laura Albareda. "Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda". In: *Technological Forecasting and Social Change* 182 (2022), p. 121806.

[43] Tanusree Sharma et al. *Unpacking How Decentralized Autonomous Organizations (DAOs) Work in Practice*. 2023. arXiv: 2304.09822 `[cs.CY]`.

[44] Tether. *Tether Balance Sheet*. URL: https://tether.to/en/transparency/.

[45] Waves-Exchange. *XTN-Neutrino Index Token*. URL: https://github.com/waves-exchange/neutrino-contract/blob/master/docs/Neutrino%202.0.%20XTN%20Litepaper.pdf.

[46] Steven A Wright. "Measuring DAO Autonomy: Lessons From Other Autonomous Systems". In: *IEEE Transactions on Technology and Society* 2.1 (2021), pp. 43–53.