Electronics and Computer Science

Dissertation

# Stablecoins with an analysis of MakerDAO and Dai

Samir Farhat Dominguez

s1746788

Supervised by Dr. Aggelos Kiayias

December 3, 2020

# Contents

**Abstract** **2**

**1 Background and Motivation** **2**

1.1 Cryptocurrency . . . 2

1.2 History and Rationale Behind Cryptocurrencies . . . 2

**2 Introduction** **3**

2.1 Stablecoins . . . 3

2.1.1 The Notion of Stability . . . 3

2.1.2 Stability Mechanisms . . . 4

2.2 MakerDAO, Maker Protocol and Dai(Waiting on interview on the 7th of Dec to finalize this section) . . . 5

2.2.1 Maker Vaults . . . 6

2.2.2 Governance . . . 6

2.2.3 Maintainers . . . 6

2.2.4 Maker Protocol Future . . . 7

2.3 Proposal and Objectives . . . 8

2.3.1 Objectives . . . 8

2.3.2 The Basket of Goods . . . 8

**3 Implementation** **8**

**4 Analysis** **8**

**Bibliography** **9**

# Abstract

**With the rise in adoption and coverage of cryptocurrencies, a mainstream market still finds itself hesitant to participate, much preferring the storied, highly regulated and centralized currencies controlled by the central banking system. This is due in no small part to the quick and dramatic shifts in price for even some of the most widely adopted cryptocurrencies, most notably Bitcoin. As such, their have been numerous promising developments around blockchains and cryptocurrencies solely focused and designed on the ethos of stability. But what is stability? And how do we attain it?**

# 1 Background and Motivation

In order to contextualize this this work, it is first imperative to discuss the definition and history of cryptocurrencies as well as stablecoins.

## 1.1 Cryptocurrency

A cryptocurrency is properly understood as a digital asset that works as a medium of exchange for goods, services, and other currencies. Records of ownership, transaction, and distribution of these currencies are stored in highly cryptographically secure databases known as blockchains. They have the marked characteristic of only existing in digital form, being decentralized, and are not to be confused with highly regulated, centralized, government-issued digital currencies, which are typically under the prerogative of central banking systems.

Blockchains are fundamental to the construction of cryptocurrencies, as they represent a distributed ledger which holds all records of movement and ownership of the cryptocurrency they pertain to. A blockchain, as the name entails, is a sequence of blocks linked cryptographically, usually by hashing the timestamp associated with each transaction. These blocks each contain information on each individual transaction or production of the cryptocurrency they maintain. They use separate computers which function as nodes that record, share and synchronize the transactions in their respective electronic ledgers. This is what allows cryptocurrencies to maintain their decentralized characteristic, as multiple devices across a network which verify and check against each other to ensure the blockchain has not been modified or tampered with by an outside entity. This characteristic, alongside strong cryptographic protocols, make blockchains almost completely resistant to modification, which is inimical to ensuring the security and reliability of the blockchain. Users and programs can interact with a blockchain through a construct called a smart contract.

In the context of blockchains, smart contracts represent programs that delineate transaction protocols. Essentially, they are highly secure algorithms that control the distribution and ownership of a cryptocurrency. The network of nodes that maintain the blockchain verify that the smart contracts have not been tampered with. A simple example of a smart contract process would be when a fee payment is made to the Ethereum blockchain. When a user completes a payment, a program sends the record of this transaction to a smart contract, which updates the blockchain to include this movement of funds and issues the corresponding Ethereum to the cryptocurrency wallet associated with the user. This transaction record is then synchronized with all the nodes in the blockchain.

## 1.2 History and Rationale Behind Cryptocurrencies

Although cryptocurrencies are a contemporary construction they still have a more extensive history than the average person may be privy to. In the 1980s there was the so called 'first wave of crypto' where there was an attempt to digitize government issued currency. This venture was ultimately unsuccessful as the centralized nature of fiat currencies did not allow for a digital asset existing without a physical store of money to back it. However, these digital currencies would not fall under the definition of cryptocurrency delineated at the beginning of this subsection. This early period was valuable in defining some of the computational and engineering practices in the construction of modern cryptocurrencies. Some examples of this would be the creation of the first digital ledgers, the first coin mining operations, and the first successful transactions of completely digital assets(not backed by physical money in banks and reserves).

The 'second wave of crypto' led to the creation of cryptocurrency as we have defined it. The first and perhaps most significant of which was Bitcoin. This led to the creation of separate currencies operated and distributed by independent parties, thus leading to the dozens of coins on the crypto-market we see today. This also led to the development of 'gimmick' coins, which are cryptocurrencies that are designed for advertising, single use, or only usable for specific merchandise distributors. Some examples of these include E-gold, used by 'cash for gold' businesses, or 'CryptoKicks' which is a purely promotional coin used to make purchases with the footwear company Nike. The scope of this work will disregard these, as despite being registered as legitimate cryptocurrencies their functionality and usage makes them wholly irrelevant to this work's objectives.

Right now, there is a pseudonymous 'third wave'. This exists in the form of stablecoins, driven by the need to stop mitigate the extreme volatility seen in most cryptocurrencies. This volatility is exemplified in Figure 1. This depicts Bitcoin dramatically shifting in comparison to that of centralized currencies, in this case the euro, British pound and Australian dollar.

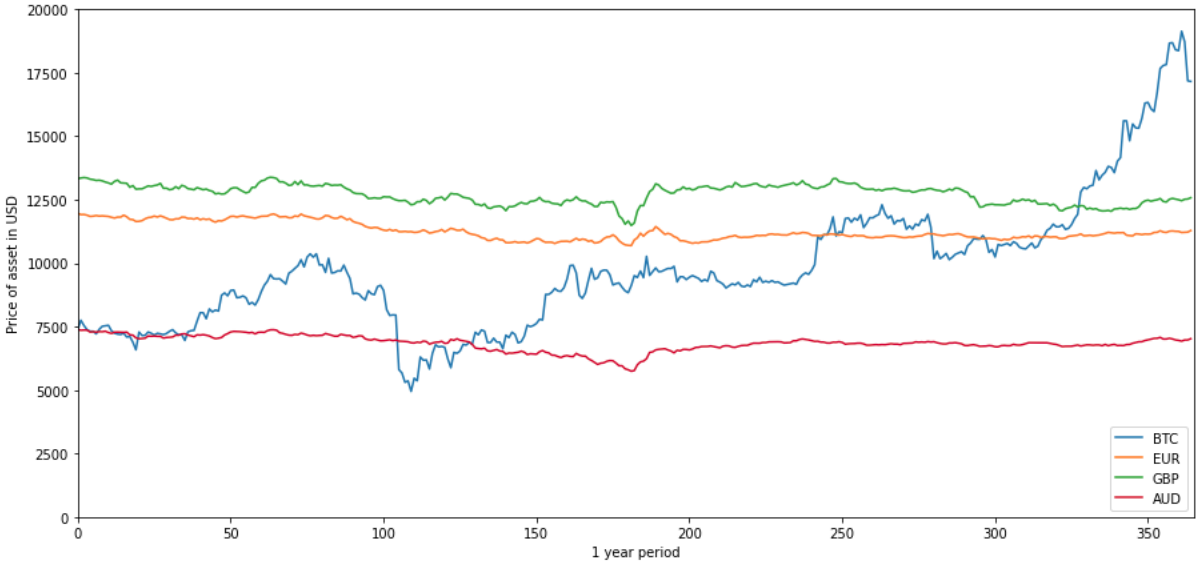


Figure 1: Bitcoin vs the USD and Fiat currencies vs 10,000 USD

# 2 Introduction

## 2.1 Stablecoins

Stablecoins are cryptocurrencies whose design and construction is primarily centered around the notion of maintaining a consistent value.

### 2.1.1 The Notion of Stability

Stability is often quantified in terms of its value relative to other fiat currencies. However, the concept of stability is a multifaceted and a somewhat vague concept. As such, their have been several different definitions of stability that can be targeted when designing a stablecoin.

The most common form of stablecoin proposals attempt to match the price of a single fiat currency. Most of the time the fiat currency selected is that of a global market hegemony. As such, stablecoins that match the price of the US dollar are the most common. Some examples of these are Tether, Dai, TrueUSD, BitUSD, and many others. The euro, British pound, and others also have stablecoin counterparts, although far and few between. Euro-STASIS and BinanceGBP are examples of these respectively.

Another conceptualization of stability that exists is that of stability with respect to a 'basket' of assets. These stablecoins select a subset of fiat currencies which are then weighted against each other to determine the value the coin should aim for. The most notable example of this type of stablecoin is that of Facebook's Libra. Libra is not currently live, but the proposal uses US treasury securities as well as the US dollar, euro, yen, British pound, and Singapore dollar in determining its target price. The weightings of these currencies on the target price is at the discretion of those who develop the coin. Weightings are often decided by examining the strengths, weaknesses, and volatility of the different currencies involved in calculations. As an example, the most recent proposal of Libra seems to weigh the USD as half of its price while the euro, yen, British pound and Singapore dollar compose the next 18, 14, 11, and 7 percent respectively.

Another form of stability is that of consistency relative to exchange-traded commodities. These exchange-traded commodities almost always take the form of precious metals such as gold and silver or natural exhaustible resources such as petroleum. Some cryptocurrencies tied to the price of drinking water have been proposed as well. These currencies can use a 'basket' model as well, where several assets are weighted to calculate a target price. These coins are more robust against crisis or inflation, since they are at the behest of tangible physical assets, rather then the more abstract prices traditional fiat currencies can take. That being said, physical assets can see changes in supply and demand, and thus run the risk of volatility in purchasing power. A strong example would be the almost inevitable depreciation of the price of petroleum, as more and more nations incentive the ownership of electric motor cars.

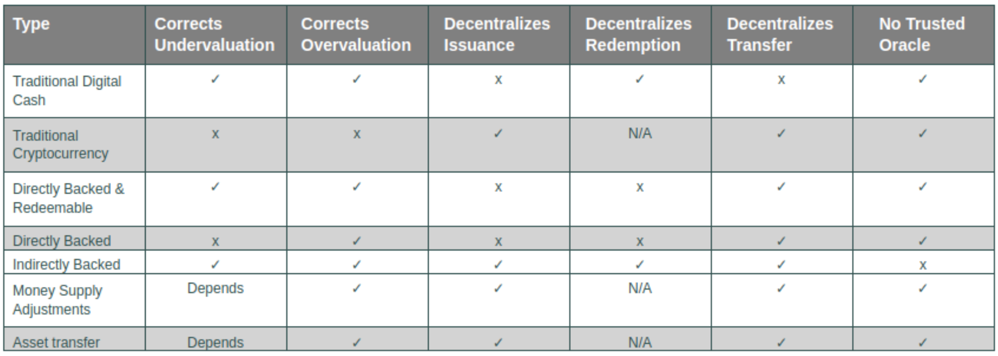
Finally there is stability with respect to inflation. This form of stability seeks to maintain constancy relative to market indicators rather than assets. The strongest example of these would be Anchor, a cryptocurrency that pegs itself to a value derived from the Monetary Measurement Unit, an economic notion derived from a series of macroeconomic inflation indicators.

### 2.1.2 Stability Mechanisms

Having discussed the concept of stability, one can move forward by elaborating on the different methodologies employed to achieve a consistent coin value. There are two principal types of Stablecoins, backed and intervention-based.

Backed stablecoins are characterized by having a reserve of money that functions as collateral to the value of the coin. That is to say a coin has assets that act act as a guarantee or security in case of a significant drop or total dissolution of the coins value. These coins come in two subsets, namely indirectly backed and directly backed. Indirectly backed coins use currencies not within their target asset or basket of assets as collateral. This can be a separate fiat currency or another cryptocurrency, commonly an Ethereum based coin. Directly backed stablecoins maintain a reserve of the target currency, often in excess of the market cap of the coin. This means that if a stablecoin pegged to say the US dollar has a market cap of 1 billion USD, then the reserves will often hold 1.3 to 2 times that value in order to ensure the robustness of their coins value. Directly backed coins can also be redeemable by the public or only the centralized entity that created the coin, which means it is important to distinguish directly backed and directly backed redeemable coins, as the former does not hold the benefit of public usability while the former does. This calls into question the legitimacy of directly backed coins being considered legitimate cryptocurrencies, but that discussion escapes the scope of this work.

Intervention-based stablecoins maintain stability through algorithmic and human intervention mechanisms. A trusted oracle will track the price of the coin and then make adjustments to ensure the constancy of the coins price relative to the asset it targets. A simple example of this would be in the blockchains releasing of the coin. If a large amount of the currency is released but the demand for the coin does not increase, then the law of supply and demand will lead to the depreciation of the coins value. At this point, the oracle might then repurchase or freeze transactions to create a scarcity, which will in turn lead to an increased price as the supply drops to meet the demand. In the following table there is a quick summary of how these stablecoins compare to other currencies in terms of decentralization and stability.

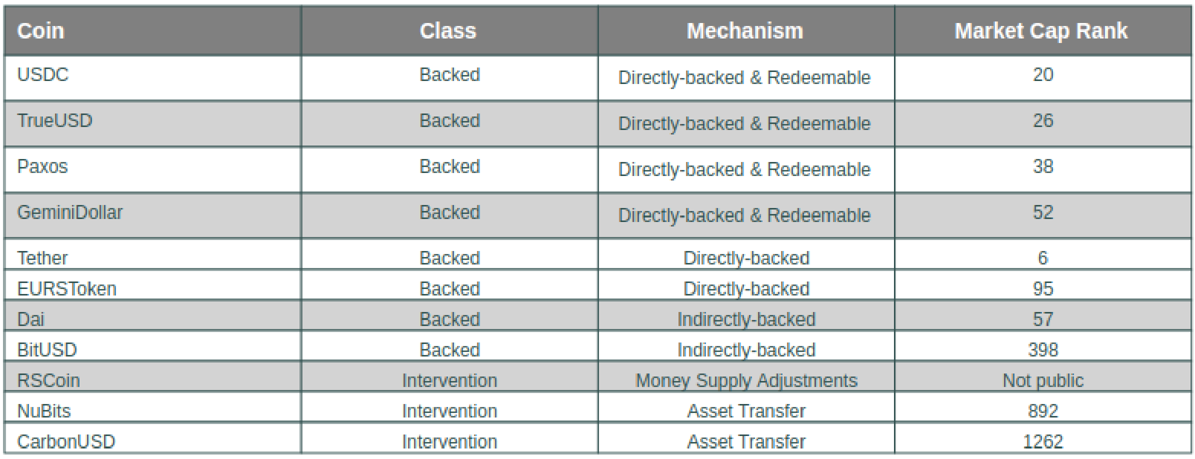


| Type | Corrects Undervaluation | Corrects Overvaluation | Decentralizes Issuance | Decentralizes Redemption | Decentralizes Transfer | No Trusted Oracle |
|---|---|---|---|---|---|---|
| Traditional Digital Cash | ✓ | ✓ | x | ✓ | x | ✓ |
| Traditional Cryptocurrency | x | x | ✓ | N/A | ✓ | ✓ |
| Directly Backed & Redeemable | ✓ | ✓ | x | x | ✓ | ✓ |
| Directly Backed | x | ✓ | x | x | ✓ | ✓ |
| Indirectly Backed | ✓ | ✓ | ✓ | ✓ | ✓ | x |
| Money Supply Adjustments | Depends | ✓ | ✓ | N/A | ✓ | ✓ |
| Asset transfer | Depends | ✓ | ✓ | N/A | ✓ | ✓ |

Table 1: Digital currencies and their characteristics

There are a myriad of mechanisms and combinations of approaches. These will be listed, followed by a brief enumeration and description of the largest stablecoins on the market.

- Correcting undervaluation: Undervaluation corrected can be done in an innumerable amount of ways. However, this is principally executed by limiting the supply of the stablecoin. Naturally, this is based on the economic principal of supply and demand.
- Correcting overvaluation: Increasing supply leads to the asset being valued at less. Once again based on the principal of supply and demand.
- Decentralizing issuance, redemption, and transfer: Spreading control of an asset amongst a large amount of people in a free market allows for a currency to stabilize. This is highly complex, but since the goal of a stablecoin is to be widely adopted, it is worth the complexity.
- Trusted oracles: Oracles are networks that set parameters for the blockchain a stablecoin is based on. These can be highly sophisticated and complex modules, or be as simple as a line of code that tracks a number.
- Arbitrage: Arbiters essentially mimic high rollers in a blockchain. They hold a high proportion of the asset, and are therefore able to control the price of a stablecoin by hoarding or dumping. This is similar to the mechanism of controlling under and overvaluation, but is more ethically suspect.



| Coin | Class | Mechanism | Market Cap Rank |
|---|---|---|---|
| USDC | Backed | Directly-backed & Redeemable | 20 |
| TrueUSD | Backed | Directly-backed & Redeemable | 26 |
| Paxos | Backed | Directly-backed & Redeemable | 38 |
| GeminiDollar | Backed | Directly-backed & Redeemable | 52 |
| Tether | Backed | Directly-backed | 6 |
| EURSToken | Backed | Directly-backed | 95 |
| Dai | Backed | Indirectly-backed | 57 |
| BitUSD | Backed | Indirectly-backed | 398 |
| RSCoin | Intervention | Money Supply Adjustments | Not public |
| NuBits | Intervention | Asset Transfer | 892 |
| CarbonUSD | Intervention | Asset Transfer | 1262 |

Table 2: Stablecoin proposals and their classification

These mechanisms allow stablecoins to maintain a consistent value relative to the asset they choose to peg themselves to. This is exemplified in the figure below, where the most widely adopted stablecoin Tether(USDT) maintains an almost perfectly consistent value of 1 USD.

## 2.2 MakerDAO, Maker Protocol and Dai(Waiting on interview on the 7th of Dec to finalize this section)

The bedrock this work will build on is the MakerDAO foundation and their development of the stablecoin 'Dai'. Therefore, it would be pertinent to elaborate on and critique the systems and goals of MakerDAO.

The creation of MakerDAO and Dai was principally motivated by a distrust of biased and dysfunctional centralized financial system. As a result, it is decentralized, transparent and is managed by users all over the world. Its blockchain is built on top of a network of computers that require collective verification, meaning the blockchain cannot be altered unless every computer in the network agrees on a change. This makes it highly secure and resistant to malicious actors. Relative to other stablecoin proposals it has been immensely successful. It currently has the largest market share of any nominal stablecoin, and has a highly active and committed user base.

The Maker foundation has permitted Dai to be used as a standard currency. Allowing for the storing of money in the blockchain, which is a vital function for any stablecoin. It can also be used as a medium for exchange, a standard of deferred payment in the Maker protocol, and a unit of account in the Maker protocol. The Maker protocol allows users to generate the stablecoin Dai, a cryptocurrency that has a soft peg to the US dollar. Specifically, it seeks to be valued at exactly 1 USD.

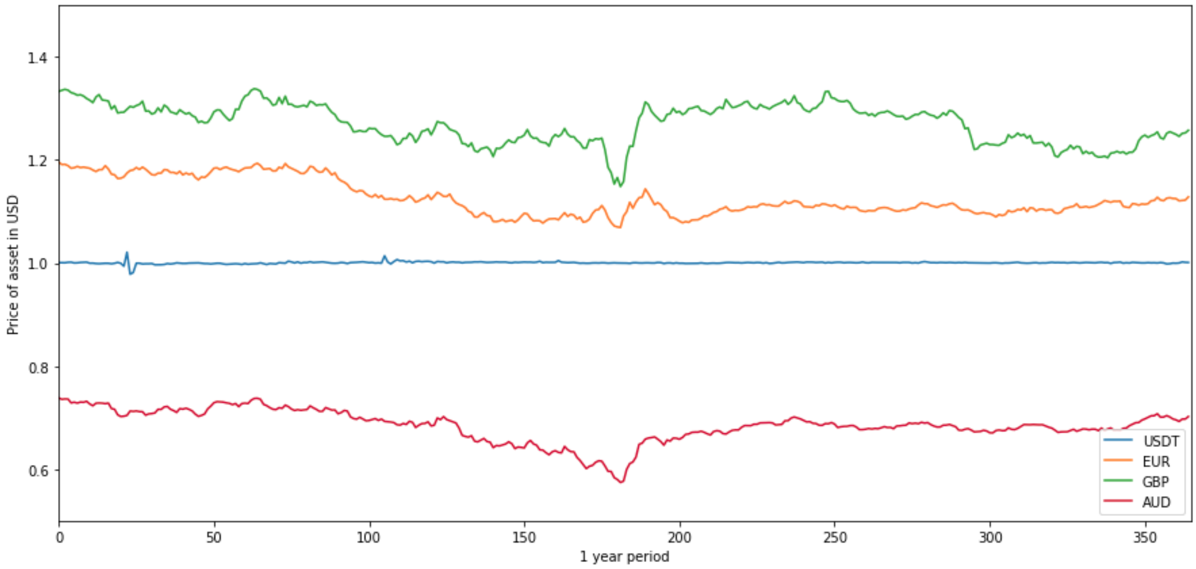


Figure 2: Depiction of the value of Tether in comparison to Fiat currency

### 2.2.1 Maker Vaults

To create Dai, a user creates and deposits Ethereum-based currencies in Maker vaults. These vaults are non-custodial, meaning that only the creator has control over the stored assets unless a liquidation occurs. Additionally, Maker vaults work through smart contracts named collateralized debt positions.

- A user creates a vault and deposits a certain amount of Ethereum-based currency to release a fixed amount of Dai. The amount of a currency required to retrieve a certain amount of Dai is determined by the Maker governance and the trusted oracles they elected.
- When the owner wishes to withdraw the deposited Ethereum-based currency, they need to pay back the generated Dai as well as a small stability fee.
- While the vault is still active, by analyzing the liquidation ratio, risk, and collateral to debt ratio of the stored asset, a trusted Maker oracle may trigger the vault to liquidate, and its assets are auctioned off internally.
- If enough is made in the auction to cover obligations of the vault, the remainder goes to the vault owner before the vault is finally closed.

### 2.2.2 Governance

Governance of the Maker protocol is principally handled through the use of the Maker token (MKR). MKR is a separate cryptocurrency, and can be thought of as shares in the Maker protocol. MKR holders can submit proposals for voting and participate in polling for proposed changes to the protocol. MKR token also serves as a recapitalization asset by increasing its supply if debt exceeds the surplus MKR. The price of MKR is therefore intrinsically tied to the health and security of the Maker protocol, functioning as an incentive for MKR holders to govern responsibly. MKR holders can choose emergency oracles, trigger emergency shutdowns, allocate funds, upgrade the system, activate the governance security modules in case of an attack, and other important responsibilities.

Amongst these responsibilities, MKR holders also vote on the parameters relating to debt ceilings, stability fees, liquidation ratio of vault assets, liquidation penalties, collateral auction duration, auction step sizes, and the Dai savings rate for those making interest on their Dai.

### 2.2.3 Maintainers

The Maker protocol also relies on key external actors.

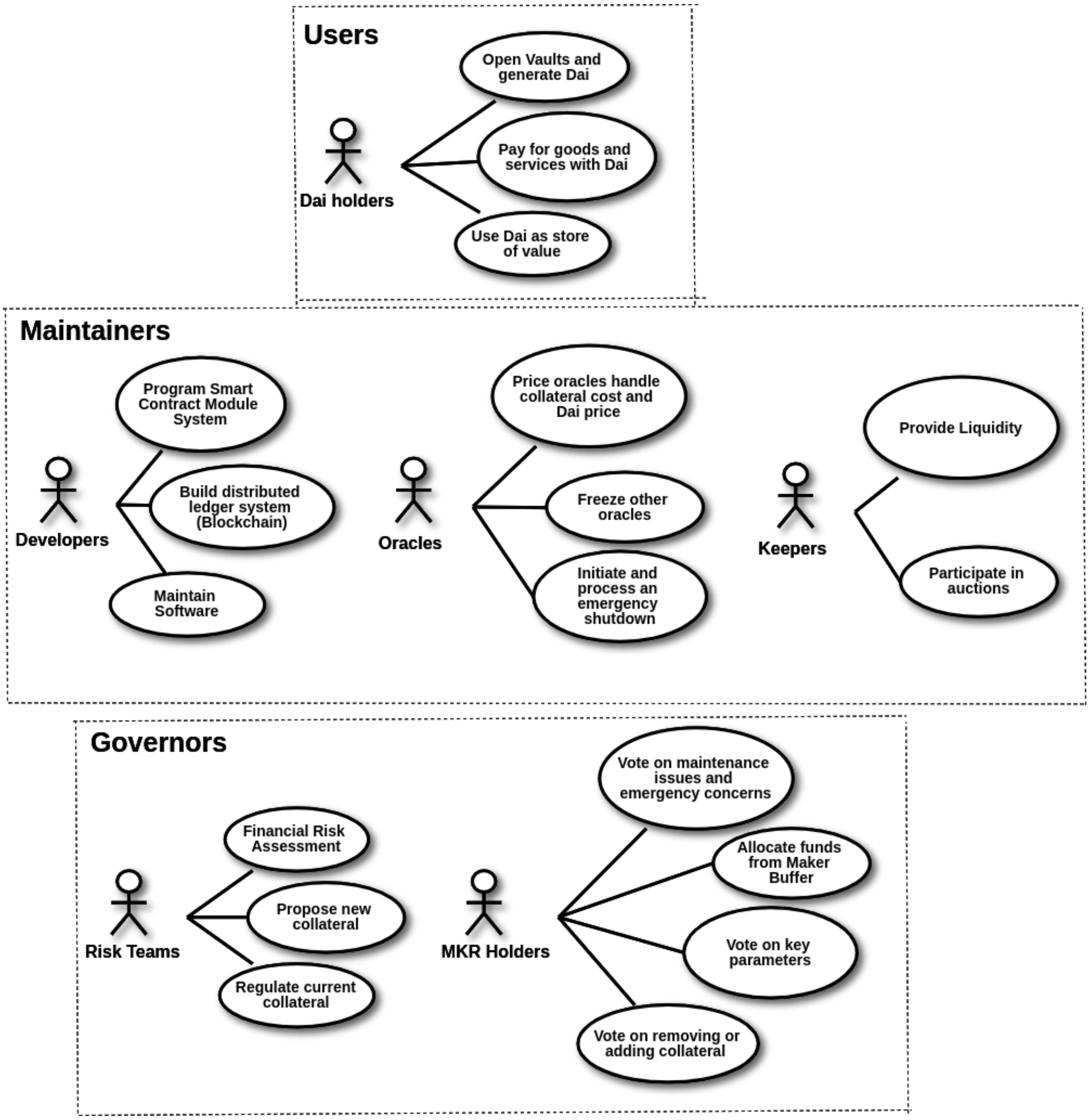

Users
Dai holders
Open Vaults and generate Dai
Pay for goods and services with Dai
Use Dai as store of value
Maintainers
Developers
Program Smart Contract Module System
Build distributed ledger system (Blockchain)
Maintain Software
Oracles
Price oracles handle collateral cost and Dai price
Freeze other oracles
Initiate and process an emergency shutdown
Keepers
Provide Liquidity
Participate in auctions
Governors
Risk Teams
Financial Risk Assessment
Propose new collateral
Regulate current collateral
MKR Holders
Vote on maintenance issues and emergency concerns
Allocate funds from Maker Buffer
Vote on key parameters
Vote on removing or adding collateral

Figure 3: Maker Protocol use-case diagram

- Keepers: Independent actors incentivized by arbitrage opportunity. They help maintain target price by dumping when above target price, and purchasing large supplies of Dai when below target price. They participate in surplus auctions, debt auctions and collateral auctions.
- Price oracles: Internal collateral value derived from decentralized oracle infrastructure. Consists of set of nodes called oracle feeds. Oracle security module also used to protect against attacks.
- Emergency oracles: The emergency oracle is chosen by MKR voters and can freeze oracles as well as trigger emergency shutdown. Emergency shutdowns are a last resort stability mechanism that protects against attacks. It works by freezing price feeds, all vault owners withdraw assets and a massive post shutdown auction process takes place to handle excess collateral. Finally, Dai holders claim the collateral in their vaults.

### 2.2.4 Maker Protocol Future

The Maker protocol has also outlined a list of its ambitions for the future.

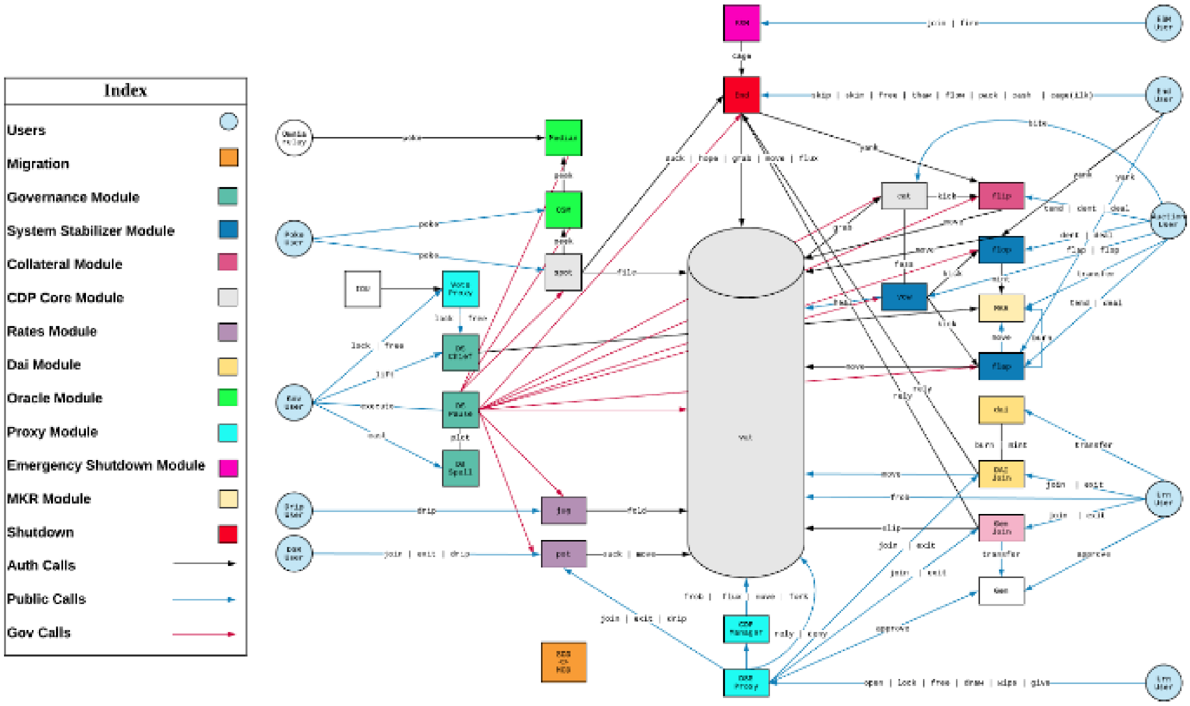


Figure 4: Placeholder for my own MakerDAO architecture diagram

- The protocol wishes to reach complete decentralization by outgrowing and gradually removing the need for the Maker Foundation in its operations.
- It wishes to extend its addressable market by turning Dai into a standard savings and exchange currency used in the technology industry. Furthermore, this would turn Dai into a capital and hedging currency.
- Another ambition is to extend its market to charities and NGOs, as the transparent and unbiased nature Maker protocol blockchain can help ensure accountability and non-profit status.
- The protocol also wishes to develop more sophisticated oracles that will be able to help MKR holders fulfill the responsibilities of the Maker Foundation.

## 2.3 Proposal and Objectives

### 2.3.1 Objectives

The objective for this work will be to describe and critique the development of a new stablecoin, with the objective of achieving stability relative to inflation and purchasing power. The development of this stablecoin will employ a large number of the methods utilized by MakerDAO, and as such a critique in the MakerDAo foundation and its proposal's strengths and weaknesses will be examined throughout. This Stablecoin will be dubbed Basket(BSKT) and will be an indirectly backed stablecoin targeting the price of the UK's 2020 basket of goods. This basket of goods and the motivation behind this selected peg is described in the following subsection.

### 2.3.2 The Basket of Goods

# 3 Implementation

# 4 Analysis

# Bibliography

[1] MakerDAO. “The Maker Protocol: MakerDAO’s Multi-Collateral Dai (MCD) System.” Makerdao, Maker Foundation, makerdao.com/en/whitepaper/.

[2] Chohan, Usman W., Are Stable Coins Stable? (March 29, 2020). Notes on the 21st Century (CBRi), 2019, Available at SSRN: https://ssrn.com/abstract=3326823

[3] Bullmann, Dirk and Klemm, Jonas and Pinna, Andrea, In Search for Stability in Crypto-Assets: Are Stablecoins the Solution? (August, 2019). ECB Occasional Paper No. 230, https://ssrn.com/abstract=3444847

[4] Fatas, Antonio. “The Economics of Fintech and Digital Currencies: A New EBook.” VOX, CEPR Policy Portal, CEPR Press, Mar. 2019, voxeu.org/article/economics-fintech-and-digital-currencies-new-ebook.

[5] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 839-858, doi: 10.1109/SP.2016.55.

[6] Richard K. Lyons & Ganesh Viswanath-Natraj, 2020. "What Keeps Stablecoins Stable?," NBER Working Papers 27136, National Bureau of Economic Research, Inc.

[7] M. Mita, K. Ito, S. Ohsawa and H. Tanaka, "What is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems," 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), Toyama, Japan, 2019, pp. 60-66, doi: 10.1109/IIAI-AAI.2019.00023.

[8] Gavrielov, Yehuda. “US20200082360A1 - Systems and Methods for Implementing a Smart Stablecoin and Facilitating the Trustless Smart Swap of Cryptocurrency.” US Patents, Jointer Inc, 12 Mar. 2020, patents.google.com/patent/US20200082360A1/en.

[9] Sánchez, David Cerezo. “Truthful and Faithful Monetary Policy for a Stablecoin Conducted by a Decentralised, Encrypted Artificial Intelligence.” ArXiv.org, ArXiv Labs, 16 Sept. 2019, arxiv.org/abs/1909.07445.

[10] Dell’Erba, Marco. “Stablecoins in Cryptoeconomics. From Initial Coin Offerings (ICOs) to Central Bank Digital Currencies (CBDCs).” Banking & Insurance eJournal (2019): n. pag.

[11] Kondova, Galia and Bolliger, Christian and Thammavongsa, Erich, Stablecoins: Types and Applications (March 12, 2020). Available at SSRN: https://ssrn.com/abstract=3553296

[12] Gooding, Philip. “Consumer Price Inflation Basket of Goods and Services: 2020.” Consumer Price Inflation Basket of Goods and Services , Office for National Statistics, 16 Mar. 2020, ons.gov.uk/economy/inflationandpriceindices/articles/ukconsumerpriceinflationbasketofgoodsandservices/2020.

[13] Umar, Zaghum, and Mariya Gubareva. “A time-frequency analysis of the impact of the Covid-19 induced panic on the volatility of currency and cryptocurrency markets.” Journal of behavioral and experimental finance vol. 28 (2020): 100404. doi:10.1016/j.jbef.2020.100404

[14] Benoît Cœuré, et al. “Investigating the Impact of Global Stablecoins.” International Monetary Fund, Committee on Payments and Market Infrastructure, Oct. 2019, www.bis.org/cpmi/publ/d187.pdf.